Координационный центр
национального домена сети Интернет

DiPLO
www.diplomacy.edu

Йован Курбалийя

Управление Интернетом

.ru

DiploFoundation

Координационный центр национального домена сети Интернет

Йован Курбалийя

Управление Интернетом

Москва
2010

ББК 32.973
К93

К93 **Курбалийя Й.** Управление Интернетом / Й. Курбалийя; Координационный центр национального домена сети Интернет. – М., 2010. – 208 с.

ISBN 978-5-9902170-1-0

Книга «Управление Интернетом» — это всесторонний обзор основных вопросов и действующих лиц в этой сфере. Она написана в простой и доступной форме и содержит многочисленные схемы и иллюстрации. В книге рассматриваются технические, правовые, экономические, социокультурные аспекты управления Интернетом, а также связанные с Интернетом проблемы развития. По каждому вопросу читателю предлагается краткое введение, сжатое изложение основных вопросов и трудностей и обзор различных взглядов и подходов к проблеме. Книга представляет собой практическое руководство для анализа и обсуждения вопросов управления Интернетом.

С 1997 г. обучение по программам, основанным на представленных в этой книге текстах и подходах, прошли более 700 дипломатов, специалистов по компьютерным технологиям, активистов неправительственных организаций и исследователей. Каждый раз при проведении курса материалы обновлялись и совершенствовались. Эти регулярные обновления делают книгу особенно полезной в качестве учебного материала для курсов начального уровня по управлению Интернетом.

DiploFoundation
Malta: 4th Floor, Regional Building
Regional Rd., Msida, MSD 2033, Malta
Switzerland: DiploFoundation
Rue de Lausanne 56
CH-1202 Genève 21, Switzerland
E-mail: diplo@diplomacy.edu
Веб-сайт: http://www.diplomacy.edu
Иллюстрации: Зоран Марчетич-Марча и Владимир Веляшевич
Научный редактор русского перевода: Андрей Михеев
Перевод: Андрей Михеев, Елена Зиновьева, Анна Лазуткина
Литературный редактор русского перевода: Ирина Пыжова
Корректор: Валерия Ахметьева
Верстка: Валерия Ахметьева, Николай Винник

Содержание

Обращение к читателям
АНДРЕЯ КОЛЕСНИКОВА,
директора Координационного центра национального домена сети Интернет

С книгой Йована Курбалийи «Управление Интернетом» я познакомился в 2009 году на IGF в Шарм-эш-Шейхе. Книга оказалась для меня приятным сюрпризом: прочитал буквально за день, на одном дыхании и получил удовольствие от того, насколько просто и понятно излагаются в ней не самые простые вещи.

Я много ездил на разные мероприятия IGF, и на мировые, и на региональные, но до IGF в Шарм-эш-Шейхе я не знал, что существует один источник, который в полном объеме рассказывал бы обо всем комплексе проблем под названием «управление Интернетом». Особенно приятно было то, что это книга, а не интернет-сайт: в наше время такие вещи публикуются именно на сайтах, а печатная версия — большая редкость. Конечно, большинство статей из книги Й. Курбалийи, написанных, правда, другим языком, можно найти и в Википедии. Но вот единого места, где все это было бы логично связано, до сих пор не было.

И еще одна неожиданность, которая для меня как человека, долгое время связанного с Интернетом и привыкшего большую часть информации получать с экрана монитора, стала своего рода открытием: книгу в руках держать гораздо приятнее, чем читать с экрана. Я думаю, что для этой книги ее «печатность», ее «бумажность» является большим преимуществом: для государственных служащих и чиновников, которые интересуются темой управления Интернетом, держать в руках и читать книгу гораздо привычнее и понятнее, чем пользоваться Сетью для поиска информации. Именно поэтому Координационный центр национального домена сети Интернет выступил инициатором перевода книги «Управление Интернетом» на русский язык и подготовил ее издание специально к Российскому форуму по управлению Интернетом. Я буду рад, если эта книга поможет всем нам еще на шаг приблизиться к пониманию непростого процесса управления Интернетом и даст повод для новых обсуждений и дискуссий.

Обращение к читателям МИХАИЛА ЯКУШЕВА, Председателя Совета Координационного центра национального домена сети Интернет

Предлагаемую читателю книгу можно назвать первым в нашей стране справочным изданием по «управлению Интернетом». Она не только рассказывает об актуальных проблемах того, что в настоящий момент называют «управление Интернетом», но и раскрывает неоднозначность самого этого понятия (в английском оригинале — «Internet Governance»), а также содержит необходимые сведения о принципах устройства всемирной Сети.

В отличие от многих других сфер управления (менеджмента, регулирования), специфика возникновения и развития Интернета как распределенной, «саморегулируемой» и «саморазвивающейся» сети, не позволяет сводить вопросы упорядочивания соответствующих общественных отношений к формулированию «желательных» управляющих воздействий и их фиксации в виде норм права. Иначе говоря, «управлять Интернетом» только путем принятия неких норм национального законодательства или международных соглашений абсолютно бесперспективно.

Как показывает практика последний десятилетий, эффективное управление Интернетом возможно, только если в соответствующие процессы вовлечены и заинтересованные государственные организации, и бизнес-сообщество, и гражданское общество. Без их конструктивного взаимодействия поставленные в настоящей книге проблемы решить невозможно, что показывается и доказывается в ней в занимательной и доступной даже «неподготовленному пользователю» манере изложения. С учетом того, что все эти проблемы являются относительно новыми, недостаточно исследованными с теоретической точки зрения, вполне извинительны отдельные терминологические «шероховатости», на которые может обратить внимание читатель более подготовленный. Тем интереснее будет этот справочник прочитать первый раз, а потом вновь и вновь обращаться к его отдельным разделам, чтобы хотя бы мысленно подискутировать с автором или

предложить какое-то новое решение или новое объяснение тому или иному вопросу. Интернет позволяет сделать этот процесс реально интерактивным, а значит, и вовлечь всех читателей книги в процесс управления Интернетом :).

Так что выражаю благодарность Йовану и желаю всем интересного чтения!

ПРЕДИСЛОВИЕ

У этой книги достаточно долгая, по меркам Интернета, история. Первые тексты и общий подход, включая методологию «пяти корзин», были разработаны в 1997 г. при подготовке образовательного курса по политике в области информационно-коммуникационных технологий (ИКТ) для чиновников государственных ведомств стран Содружества. С 1997 г. подготовку по ИКТ/управлению Интернетом в рамках различных курсов и онлайн-программ фонда DiploFoundation прошли около 700 дипломатов, специалистов по компьютерным технологиям, активистов гражданского общества и исследователей. Каждый раз при проведении курса материалы обновлялись и совершенствовались.

В 2004 г. Diplo впервые опубликовал печатную версию своих материалов по управлению Интернетом в форме книги «Управление Интернетом: проблемы, субъекты, преграды». Эта книга, соавторами которой были Стефано Балди, Эдуардо Гелбстайн и Йован Курбалийя, стала частью «Библиотеки информационного общества», изданной Diplo. Отдельную благодарность выражаем Эдуардо Гелбстайну, который внес значительный вклад в подготовку разделов по кибербезопасности, спаму и защите тайны частной жизни, а также Владимиру Радуновичу и Джинджер Пак, обновлявшим материалы курса. Комментарии и предложения других коллег отмечены по тексту. Стефано Балди, Эдуардо Гелбстайн и Владимир Радунович очень помогли в разработке идей для иллюстраций этой книги.

Настоящее издание книги подготовлено Координационным центром национального домена сети Интернет (www.cctld.ru) специально к первому региональному Форуму по управлению Интернетом в России, проходящему в мае 2010 года в Москве.

Раздел 1

Введение

Управление Интернетом — непростая проблема. Хотя она имеет дело с главным символом ЦИФРОВОГО мира, к ней нельзя применять цифровую (двоичную) логику «правда—ложь» или «хорошо—плохо». Многочисленные тонкости и оттенки значений и представлений в рамках этой проблемы вызывают необходимость использования АНАЛОГОВОГО подхода, допускающего целый спектр вариантов и компромиссов.

Поэтому в этой брошюре мы не пытаемся дать какие-либо окончательные заключения по вопросам, связанным с управлением Интернетом. Скорее, она преследует цель предложить практические рамки для анализа, дискуссий и решения ключевых вопросов в этой области.

ВВЕДЕНИЕ

За относительно недолгое время Интернет стал неотъемлемой частью современного общества. Вот некоторые характерные черты Интернета на сегодняшний день (конец 2009 г.):

- по некоторым оценкам, около 1,5 миллиардов пользователей по всему миру;
- крайне важное влияние на общество в сфере образования, здравоохранения, функционирования органов власти и в других сферах деятельности;
- киберпреступность, например, мошенничество, незаконные азартные игры и фишинг (кража и ненадлежащее использование персональной информации);
- ненадлежащее и незаконное использование технологии в форме вредоносного кода (вирусов) и спама.

Растущая информированность о социальном, экономическом и политическом влиянии Интернета на общество активизировала внимание к вопросам управления Интернетом. Применительно к Интернету регулирование необходимо, среди прочего, для того, чтобы:

- предотвратить или, по крайней мере, минимизировать риск распада Интернета на несколько несвязанных сетей;
- сохранить техническую совместимость и способность к взаимодействию всех компонентов Интернета;
- защитить права и определить ответственность различных действующих лиц;
- оградить пользователей от последствий ненадлежащего и незаконного использования технологий;
- защитить общественные интересы на государственном и глобальном уровнях;
- способствовать дальнейшему развитию Интернета.

Анализ правовых аспектов и социальных последствий технологического развития неизбежно отстает от технологических инноваций. Это

Интернет и статистика не очень дружны между собой. С самых первых дней существования Интернета точно определить число пользователей и веб-сайтов, объем передаваемых данных (трафика), финансовые показатели и большинство других параметров было сложно. К тому же цифры часто используются для создания шумихи вокруг темпов развития Интернета, что делает их еще менее достоверными [1].

относится и к Интернету. Международные переговоры по вопросам регулирования Интернета прошли через несколько важных этапов, но все еще далеки от завершения и даже от достижения консенсуса относительно того, каким образом следует управлять Интернетом. Какие действующие лица вероятнее всего будут влиять на развитие Интернета? Какова будет их политика в отношении обеспечения доступа к Сети, коммерции, содержания материалов (контента), финансирования, безопасности и других вопросов, являющихся центральными для развития Интернета? Это лишь некоторые ключевые вопросы, ответы на которые необходимо искать в рамках управления Интернетом.

ЧТО ОЗНАЧАЕТ ТЕРМИН «УПРАВЛЕНИЕ ИНТЕРНЕТОМ»

Само определение термина «Интернет» порождает споры, которые затем продолжаются в спорах об управлении Интернетом. Это не просто вопрос лингвистической аккуратности. Различные оттенки смысла, вкладываемые в данный термин, порождают разные ожидания и подходы к выработке политического курса. Например, специалисты в области телекоммуникаций рассматривают проблему управления Интернетом сквозь призму технической инфраструктуры. Профессионалы в области компьютерных технологий в основном уделяют внимание разработке различных стандартов, языков и приложений — таких, как XML или Java. Специалисты по коммуникации делают акцент на упрощении обмена информацией. Активисты борьбы за права человека рассматривают управление Интернетом с точки зрения свободы выражения убеждений, защиты тайны частной жизни и других основных прав личности. Юристы обращают внимание на вопросы юрисдикции и разрешения споров. Политики по всему миру обычно говорят о средствах массовой информации и о вопросах, находящих отклик у избирателей, например о перспективах (больше компьютеров — больше образования) и угрозах (безопасность Интернета, защита детей). Дипломатов в первую очередь беспокоит сам процесс регулирования и защита национальных интересов. Список потенциально противоречащих друг другу профессиональных точек зрения на управление Интернетом можно продолжить.

В рамках Всемирной встречи на высшем уровне по вопросам информационного общества[1] было предложено следующее определение управления Интернетом: «Управление Интернетом представляет собой разра-

[1] Всемирная встреча на высшем уровне по вопросам информационного общества была созвана по инициативе ООН и прошла в два этапа: в Женеве в 2003 г. и в Тунисе в 2005 г. — ***Примеч. перев.***

ботку 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» [2]. Это рабочее определение является хорошей отправной точкой для дискуссий, тем не менее, оно не помогает решить проблему различных интерпретаций двух ключевых терминов: «Интернет» и «управление».

Интернет

Некоторые авторы утверждают, что понятие «Интернет» не охватывает все существующие аспекты развития цифровых технологий. Обычно в качестве более полных предлагаются два других термина: «информационное общество» и «информационно-коммуникационные технологии». Эти понятия включают в себя сферы, выходящие за пределы непосредственно Интернета — такие как мобильная связь. Однако в пользу употребления термина «Интернет» свидетельствует стремительный переход глобальных коммуникаций к использованию протоколов передачи данных Интернета как основного технического стандарта. Вездесущий Интернет продолжает стремительно расти не только в количественном отношении, но и с точки зрения спектра предлагаемых услуг, среди которых наиболее заметен протокол передачи голоса по Интернету (VoIP), способный заменить обычную телефонную связь.

Управление

В дискуссиях по проблемам управления Интернетом, особенно в ходе первого этапа WSIS (World Summit of the Information Society, Всемирная встреча на высшем уровне по вопросам информационного общества) в Женеве в 2003 г., предметом противоречий стал термин «управление» и его различные интерпретации. В соответствии с одной из интерпретаций управление является синонимом правительства. Представители многих государств изначально вкладывали в это понятие такой смысл и полагали, что Интернет должен регулироваться государствами на межправительственной основе с ограниченным участием других, в основном негосударственных, акторов [3]. Подобному толкованию противостояло иное, более широкое понимание термина «управление», которое предполагает регулирование деятельности различных институтов, в том числе негосударственных. Именно такой трактовки придерживались члены интернет-сообщества, поскольку она наиболее соответствует особенностям регулирования Интернета с момента его создания.

Терминологическая путаница усугублялась различными переводами термина «управление» (governance, *англ.*) на другие языки. В испанском

«И»нтернет или «и»нтернет и язык дипломатии

Еще в 2003 г. журнал «The Economist» впервые напечатал слово «Интернет» с маленькой буквы. Подобная политика редакции явилась отражением того факта, что Интернет стал частью повседневной жизни, перестал быть чем-то уникальным и особенным, нуждающимся в особом обозначении. Таким образом, глобальную сеть постигла та же участь, что и многие другие изобретения, такие как (т)елеграф, (т)елефон, (р)адио и (т)елевидение.

Вопрос о написании Интернета/интернета со строчной или прописной буквы вновь возник в ходе конференции Международного союза электросвязи (МСЭ)[2] в Анталье в ноябре 2006 г. Вопрос приобрел политическое измерение, когда в резолюции МСЭ по вопросам управления Интернетом появилось слово «Интернет», начинающееся, в отличие от традиционного написания, со строчной буквы. Дэвид Гросс, посол США, занимавшийся проблемами управления Интернетом, выразил озабоченность по поводу того, что использование МСЭ строчной буквы может свидетельствовать о намерении организации рассматривать Интернет в одном ряду с другими телекоммуникационными системами, регулируемыми на международном уровне в рамках МСЭ. Некоторыми это было интерпретировано как дипломатический сигнал, отражающий стремление МСЭ играть более значимую роль в управлении Интернетом [4].

языке этот термин относится преимущественно к государственной деятельности или правительству (gestión pública, gestión del sector público, función de gobierno). Связь с государственной деятельностью и правительством также заметна во французском языке (gestion des affaires publiques, efficacité de l'administration, qualité de l'administration, mode de gouvernement). Похожая ситуация наблюдается и в португальском языке: налицо связь с государственным сектором и правительством (gestăo pública, administração pública).

ЭВОЛЮЦИЯ УПРАВЛЕНИЯ ИНТЕРНЕТОМ

Начальный период управления Интернетом (1970-е — 1994)

Интернет начался как правительственный проект. В конце 1960-х гг. правительство США финансировало развитие сети DAPRA Net, проектировавшейся Управлением перспективных исследовательских проектов Министерства обороны как надежное средство коммуникации. К середине 1970-х гг., когда был создан протокол TCP/IP, сеть превратилась в то, что сегодня называется Интернет. Одним из ключевых принципов Интернета является его распределенная природа: пакеты данных могут передаваться в сети по различным маршрутам, обходя традиционные

[2] Международный союз электросвязи — международная организация, в рамках которой правительствами и частным сектором координируются глобальные сети и услуги электросвязи. Основанный в Париже в 1865 г. как Международный телеграфный союз, МСЭ получил свое нынешнее название в 1934 г., а в 1947 г. стал специализированным учреждением Организации Объединенных Наций. — ***Примеч. перев.***

барьеры и механизмы контроля. Этому технологическому принципу соответствовал схожий подход к регулированию Интернета на ранних этапах: Рабочая группа по проектированию Интернета (IETF)[3], созданная в 1986 г., управляла дальнейшим развитием Интернета, принимая решения на основе сотрудничества и консенсуса, с привлечением широкого круга участников. У Интернета не было центрального правительства, централизованного планирования, «великой стратегии».

В результате популярным стало утверждение, что Интернет формирует уникальное пространство, альтернативное политической системе современного мира. Джон Перри Барлоу, автор знаменитой «Декларации независимости киберпространства», обращается ко всем правительствам: « [Интернет] по своей природе транснационален, к нему не применим принцип государственного суверенитета, и ваш [государственный] суверенитет на нас не распространяется. Мы должны сами принимать решения»[4].

Слова «электронный» («е-»), «виртуальный», «кибер», «цифровой»

Прилагательные «электронный» («е-»), «виртуальный», «кибер», «цифровой» используются для описания различных аспектов развития Интернета и информационно-коммуникационных технологий (ИКТ). Использование этих слов берет начало в 1990-х гг. и отражает различные социальные, экономические и политические факторы, оказывавшие влияние на развитие Интернета. Например, представители научного сообщества и первые разработчики (так называемые пионеры Интернета) использовали слова «кибер», «цифровой», чтобы подчеркнуть инновационный характер Интернета, формирующего «прекрасный новый мир». Определение «электронный» («е-»), как правило, ассоциируется с электронной торговлей (e-commerce) и коммерциализацией Интернета в конце 1990-х гг. Термин «цифровой» вошел в употребление в основном в технологических кругах и получил распространение в контексте дискуссий о «цифровом разрыве».

На международном уровне слово «кибер» было употреблено Советом Европы в Конвенции о киберпреступности, принятой в 2001 г. В настоящее время оно используется при описании проблем кибербезопасности. Инициатива МСЭ в этой области получила название «Глобальная повестка дня кибербезопасности». Слово «виртуальный» редко используется в международных документах.

Прилагательное «электронный» («е-») приобрело особенную популярность в ЕС, где с его помощью описывают различные политические инициативы в области электронного здравоохранения (e-health) или электронной науки (e-science). В рамках WSIS этот термин впервые был использован в ходе Общеевропейской региональной встречи в Бухаресте, а затем стал одним из основных в текстах WSIS, в том числе и в итоговых документах.

Реализация решений WSIS организована по направлениям деятельности, включающим электронное правительство, электронный бизнес, электронное обучение, электронное здоровье и электронное трудоустройство, электронное сельское хозяйство и электронную науку (e-government, e-business, e-learning, e-health, e-employment, e-agriculture, e-science).

[3] Английское название — Internet Engineering Task Force. — ***Примеч. перев.***

[4] Приведенная фраза не является точной цитатой, а передает общий пафос «Декларации независимости киберпространства». — ***Примеч. перев.***

«Война DNS» (1994—1998)

Подробный обзор эволюции управления Интернетом приведен на стр. 197–199.

Вскоре государства и бизнес осознали значимость глобальной сети, и децентрализованный подход к управлению Интернетом подвергся изменениям. В 1994 г. Национальный фонд науки США, управлявший ключевой инфраструктурой Интернета, принял решение передать управление системой доменных имен субподрядчику — частной компании Network Solutions Inc. (NSI), зарегистрированной в США. Интернет-сообщество негативно отреагировало на этот шаг, что привело к так называемой войне DNS. «Война DNS» вовлекла в процесс регулирования Интернета новых участников: международные организации и государства. Она закончилась в 1998 г. созданием новой организации — Корпорации по присвоению имен и номеров в Интернете (Internet Corporation for Assigned Names and Numbers, ICANN). С этого времени дискуссия по вопросам управления Интернетом характеризуется более активным вовлечением правительств.

Всемирная встреча на высшем уровне по вопросам информационного общества (2003—2005)

Всемирная встреча на высшем уровне по вопросам информационного общества (WSIS), прошедшая в Женеве (2003) и в Тунисе (2005), официально внесла вопрос об управлении Интернетом в дипломатическую повестку дня. Участники Женевского этапа WSIS, которому предшествовал ряд подготовительных комитетов и региональных встреч, предложили обсудить широкий круг вопросов, связанных с информацией и коммуникациями. Более того, в ходе первых подготовительных и региональных встреч не упоминалось даже само слово «Интернет», не говоря уже об «управлении Интернетом» [5]. Управление Интернетом стало частью переговорного процесса WSIS в ходе Западноазиатской региональной встречи, прошедшей в январе 2005 г., а по итогам Женевского этапа WSIS управление Интернетом стало ключевым вопросом саммита.

В результате длительных переговоров и соглашений, заключенных в последнюю минуту, участники встречи в Женеве приняли решение создать Рабочую группу по вопросам управления Интернетом (Working Group on Internet governance, WGIG). WGIG подготовила отчет, послуживший основой для дальнейших переговоров в рамках второго этапа WSIS, прошедшего в Тунисе в ноябре 2005 г. Итоговый документ встречи — «Программа для информационного общества» — подробно рассматривает проблему управления Интернетом, включая определение этого понятия, список проблемных областей, а также содержит решение о создании Форума по вопросам управления использованием Интернета (Internet Governance Forum, IGF). Форум, первое заседание которого

прошло в октябре 2006 г. в Афинах, представляет собой новую модель международного обсуждения проблем управления Интернетом. Это многосторонний институт, созванный по решению Генерального секретаря ООН. Мандат Форума будет пересмотрен через пять лет.

События 2006 г.

После завершения встречи в Тунисе (ноябрь 2005 г.) предметом дискуссий по вопросам управления Интернетом в 2006 г. стали важнейшие три события.

Во-первых, истечение срока действия Меморандума о взаимопонимании между ICANN и Министерством торговли США и подписание нового. Надежды на то, что это событие изменит характер взаимоотношений между правительством США и ICANN и последняя станет международной организацией нового типа, не оправдались. Новый вариант Меморандума лишь слегка ослабил связь между ICANN и правительством США, существовавшую с момента основания организации, хотя и не исключил в перспективе возможности окончательной интернационализации ICANN.

Вторым событием 2006 г. стал Форум по вопросам управления Интернетом, прошедший в Афинах. Это был первый форум такого рода; во многих отношениях он представлял собой экспериментальный формат многосторонней дипломатии. Форум был по-настоящему многосторонним. Все действующие лица, вовлеченные в процесс регулирования Интернетом — государства, бизнес-структуры и представители гражданского общества — участвовали на равноправной основе. Необычной была организационная структура основных событий и семинаров Форума. Журналисты модерировали все дискуссии, и, следовательно, Форум отличался от традиционных конференций формата ООН. Однако критики заявили, что Форум — всего лишь «говорильня», не дающая реальных результатов в форме итоговых документов или планов действий.

Третьим важным событием была Полномочная конференция МСЭ, прошедшая в Анталье (Турция) в ноябре 2006 г. На конференции был избран новый Генеральный секретарь МСЭ, доктор Хамадун Турэ. Он объявил о необходимости более пристального внимания организации к проблемам кибербезопасности и содействия развитию. Ожидалось также, что с его приходом изменится подход МСЭ к управлению Интернетом.

События 2007 г.

В 2007 г. в ICANN шли дискуссии вокруг возможного создания домена «для взрослых» «.xxx». В результате возобновились дебаты и по многим другим вопросам управления Интернетом, включая сферу компетенции ICANN, а именно должна ли ICANN заниматься исключительно техничес-

ким регулированием или в ее компетенцию входят вопросы государственной политики. Вмешательство со стороны США и других стран в отношении домена «.xxx» заострило вопрос об участии государств в работе ICANN. В ходе второй встречи IGF, прошедшей в ноябре 2007 г. в Рио-де-Жанейро, главным событием стало внесение в повестку дня Форума пункта о критически важных ресурсах Интернета (пространство имен и адресов).

События 2008 г.

Важнейшим событием 2008 г., которое продолжит влиять на процессы управления Интернетом (как и на многие другие области политики), стало избрание Барака Обамы президентом США. В ходе президентской кампании он широко использовал Интернет и технологии Веб 2.0. Некоторые утверждают, что именно использование Интернета стало одной из причин успеха Обамы. Среди советников Б. Обамы — много представителей интернет-индустрии, включая генерального директора компании Google. Помимо технологической компетентности, президента Обаму характеризует приверженность многостороннему решению международных проблем, что неизбежно окажет влияние на дискуссии об интернационализации ICANN и формировании международного режима управления Интернетом.

В 2008 г. одним из важнейших вопросов управления Интернетом стала так называемая сетевая нейтральность[5]. Эти вопросы даже фигурировали в предвыборной кампании, причем Барак Обама выступал в поддержку принципа сетевой нейтральности.

Дискуссии по этой теме проходят в США между двумя противостоящими группами. В поддержку сетевой нейтральности в основном выступают представители так называемой интернет-индустрии, в том числе такие компании, как Google, Yahoo! и Facebook. Изменение архитектуры Интернета в результате нарушения принципа сетевой нейтральности может поставить под угрозу их бизнес. Противоположную позицию занимают телекоммуникационные компании, такие как Verizon и AT&T, интернет-провайдеры и представители мультимедийной индустрии. По ряду различных причин представители этой сферы бизнеса предпочитают некоторую дифференциацию по отношению к передаваемым по сети данным.

Еще одним важным событием стал быстрый рост Facebook и других социальных сетей. В сфере управления Интернетом растущая популярность инструментов Веб 2.0 ставит на повестку дня вопросы неприкосновенности частной жизни и защиты данных в Facebook и аналогичных сетях.

---

[5] В соответствии с принципом «сетевой нейтральности» данные должны передаваться по интернет-каналам без какой-либо дискриминации, независимо от содержания, отправителя, получателя и т. д. Нарушением этого принципа является, например, предоставление телекоммуникационной компанией приоритета в виде более быстрой загрузки материалов определенным сайтам. — *Примеч. перев.*

События 2009 г.

В первой половине 2009 г. представители вашингтонских кругов пытались определить последствия и будущие направления политики президента США Б. Обамы в отношении Интернета. Назначения на ключевые посты, связанные с регулированием Интернета, не принесли сюрпризов, подтвердив приверженность Обамы принципам открытости Интернета. В соответствии с обещаниями, данными в ходе предвыборной кампании, его команда приняла ряд мер в поддержку принципа сетевой нейтральности.

Наиболее заметным событием 2009 г. стало подписание «Подтверждения обязательств» между ICANN и Министерством торговли США, что должно сделать Корпорацию более независимой. Хотя этот шаг разрешает одну из проблем управления Интернетом — контроль США над деятельностью ICANN — он ставит целый ряд других вопросов, таких как международный статус организации и проблема контроля над ее деятельностью. «Подтверждение обязательств» содержит общие руководящие принципы, но оставляет много вопросов открытыми.

В ноябре 2009 г. в Шарм-эш-Шейхе (Египет) прошла четвертая встреча IGF. На содержание дискуссии повлияло подписание «Подтверждения обязательств», а также два предстоящих в 2010 г. события: решение о необходимость продолжения встреч IGF после 2011 г. и очередная Полномочная конференция МСЭ в Мексике. Несмотря на то что в 2009 г. внимание было приковано к ситуации в США после избрания Обамы, в 2010 г. международные аспекты регулирования Интернета (международный статус ICANN, будущее IGF, стратегия МСЭ), вероятно, выйдут на первый план.

АНАЛИТИЧЕСКИЙ ИНСТРУМЕНТАРИЙ УПРАВЛЕНИЯ ИНТЕРНЕТОМ

Аналитический инструментарий управления Интернетом — набор инструментов, предназначенных для выработки политического курса и подготовки политической аргументации. Для всех, кто участвует в управлении Интернетом, эти инструменты имеют практическое значение. Во-первых, инструментарий призван помочь ориентироваться в больших объемах информации, документов и исследовательских работ, посвященных проблемам управления Интернетом. Во-вторых, его можно использовать для выработки политической аргументации и лучшего понимания политических заявлений иных сторон. Наконец, инструментарий может повысить эффективность переговорного процесса, позволяя

договаривающимся сторонам находить компромиссы, более выгодные всем участникам, чем просто «наименьший общий знаменатель».

Аналитический инструментарий управления Интернетом — часть формирующегося режима управления Интернетом, становление которого только начинается. Опыт иных международных режимов (например, в сфере защиты окружающей среды, воздушного транспорта или контроля над вооружениями) показывает, что в подобных областях вырабатываются общая система взглядов, ценностей, представлений о причинно-следственных связях, единые способы аргументации, терминология, специальная лексика, жаргон, сокращения. Такая система взглядов имеет большое значение в политической жизни. Она формирует восприятие различных проблем, что, в свою очередь, оказывает влияние на предпринимаемые действия.

Во многих случаях на становление системы взглядов влияет специфическая профессиональная культура (способ мышления и поведения, общие для представителей одной профессии). Установление неких «общих рамок» обычно помогает улучшить коммуникацию и понимание. Однако порой они используются для защиты «территории» и препятствия влиянию извне. По словам американского лингвиста Джефри Майрела, «всякий профессиональный язык — это язык сферы влияния».

Любой режим управления Интернетом будет сложным, поскольку должен включать множество вопросов, участников, механизмов, процедур и инструментов.

Эта иллюстрация, выполненная по мотивам работ голландского художника М.К. Эшера, демонстрирует некоторые парадоксальные точки зрения, связанные с управлением Интернетом.

Аналитический инструментарий управления Интернетом отражает специфические черты этой области как «грязной» политической проблемы[6]. Проблемы управления Интернетом, как правило, имеют множество катализаторов, поэтому выявить для каждой из них единственную причину чаще всего непросто. Во многих случаях одна проблема — это симптом другой, что иногда создает «порочный круг» политических решений. Некоторые методы познания, такие как линейное мышление, поиск единственной причины, подход «или-или», лишь отчасти применимы к проблемам управления Интернетом. Международные переговоры по проблемам управления Интернетом подразумевают почти бесконечный поиск равновесия между различными интересами и подходами.

Аналитический инструментарий управления Интернетом включает набор разнообразных инструментов. Некоторые из них используются при разрешении глубинных политических противоречий («широкий» и «узкий» подходы к управлению Интернетом), в то время как иные представляют собой риторические приемы аргументации и политического дискурса («не сломано — не чините»).

Если попытаться упорядочить эти инструменты, можно выделить следующие основные категории:

- модели и подходы;
- руководящие принципы;
- аналогии.

Как и сам процесс управления Интернетом, этот инструментарий находится в постоянном изменении. Подходы, модели, руководящие принципы и аналогии появляются и исчезают в зависимости от их уместности и важности для процесса переговоров в данный момент.

ПОДХОДЫ И МОДЕЛИ

Как управление Интернетом в целом, так и относящиеся к этой области отдельные вопросы давно являются предметом политических дискуссий и научных споров. Постепенно в этой области сложилось несколько подходов и моделей, которые отражают различия между позициями участ-

[6] «Грязная» проблема (wicked problem) — термин, используемый в социальных науках для описания проблемы, которую сложно или невозможно решить по причине неполноты, противоречивости информации, изменяющихся условий и др. «Грязные» проблемы, как правило, настолько вписаны в контекст, что решение может стать источником целого ряда новых сложностей; кроме того, у них нет и не может быть единственно верного решения. Проблемы такого рода противопоставляются простым, решаемым проблемам, которые встречаются в математике, шахматах и т. п. — ***Примеч. перев.***

ников переговоров, а также между профессиональными и национальными культурами. Выявление общих подходов и моделей может упростить процесс переговоров и помочь выстроить общую «систему координат».

«Широкий» или «узкий» подход

До сегодняшнего дня противостояние между «узким» и «широким» подходами к управлению Интернетом является одним из центральных вопросов, отражающих различные интересы в процессе управления Интернетом. При «узком» подходе внимание сосредоточено в первую очередь на инфраструктуре Интернета (системе доменных имен, IP-адресов и «корневых» серверов) и на позиции ICANN как ключевого игрока на этом поле.

В соответствии с широким подходом переговоры по управлению Интернетом должны выйти за пределы вопросов инфраструктуры и обратиться к другим проблемам: правовым, экономическим, социокультурным, связанным с развитием. Широкий подход взят за основу в отчете Рабочей группы по вопросам управления Интернетом и итоговых документов Всемирной встречи на высшем уровне по вопросам информационного общества. Он также используется как основополагающий принцип архитектуры Форума по вопросам управления Интернетом.

Проведение различий между этими двумя подходами было важной темой в ходе переговоров WSIS, однако консенсуса по ней достигнуть так и не удалось. Дискуссии в ходе Форума по вопросам управления Интернетом в Рио-де-Жанейро, прошедшего в ноябре 2007 г., со всей ясностью показали, что обсуждения в рамках «широкого» подхода, тем не менее, могут быть весьма конкретными. Появление в повестке дня Форума вопроса о ключевых ресурсах Интернета (так называемая проблема ICANN) демонстрирует, что проблемы «узкого» подхода также сохраняют свое значение.

Согласованность политических и технических решений

В управлении Интернетом интеграция технических и политических вопросов является непростой задачей, поскольку провести четкую границу между ними сложно. Технические решения не нейтральны. В конечном счете, любое техническое решение способствует продвижению чьих-то интересов, усиливает позицию определенных групп и в известной степени влияет на общественную, политическую и экономическую жизнь.

На раннем этапе развития Интернета и технические, и политические аспекты его функционирования долгое время регулировались лишь одной социальной группой — сообществом разработчиков и пользователей. С распространением Интернета и появлением в 1990-е гг. новых

заинтересованных сторон, в первую очередь представителей бизнеса и правительств, члены интернет-сообщества уже не могли удерживать «в одних руках» управление как технологическими, так и политическими вопросами. Последующие реформы, в том числе создание ICANN, ставили своей целью восстановление равновесия между техническими и политическими аспектами. Проблема нахождения такого равновесия еще не решена и остается одной из наиболее спорных в ходе обсуждений на Форуме по вопросам управления Интернетом.

Старый «реальный» подход или новый «киберподход»

Практически любой вопрос в рамках управления Интернетом можно рассмотреть с двух разных сторон. Сторонники старого «реального» подхода — по принципу «новое вино в старые мехи» — доказывают, что Интернет не привнес ничего нового в сферу управления. По их мнению, Интернет, с точки зрения регулирования — еще одно техническое устройство, не отличающееся от предшественников: телеграфа, телефона или радио.

Например, в дискуссиях по правовым вопросам сторонники этого подхода указывают, что существующие законы с небольшой корректировкой можно применить и к Интернету. В области экономики приверженцы этого подхода утверждают, что разницы между обычной и «электронной» коммерцией нет. Следовательно, нет необходимости специального правового регулирования электронной коммерции.

Приверженцы нового «киберподхода» (назовем его «новое вино в новые мехи») доказывают, что Интернет — принципиально новая система коммуникации по сравнению со всеми предшествующими. Основная посылка «киберподхода» состоит в том, что Интернету удалось отделить современную социальную и политическую реальность от мира (географически разделенных) суверенных государств. Киберпространство отличается от реального мира, а потому требует иной формы управления. В области права представители «киберподхода» утверждают, что существующие законы, касающиеся юрисдикции, киберпреступности и заключения контрактов, не могут применяться к Интернету, а потому должны быть созданы новые законы.

Децентрализованная или централизованная структура управления Интернетом

В соответствии с децентрализованным подходом структура управления должна отражать саму природу Интернета: сеть сетей. Сторонники данного подхода подчеркивают, что столь сложную систему невозможно поместить под единый «зонтик» управления, например, в рамках международной организации, и что именно отсутствие централизованного управления является одной из главных причин стремительного роста Интернета. Эту точку зрения в основном разделяют техническое интернет-сообщество и развитые страны.

Сторонники же централизованного подхода апеллируют, среди прочего, к практической сложности, которую представляет для стран с ограниченными людскими и финансовыми ресурсами необходимость участвовать в обсуждении вопросов управления Интернетом в условиях сильной децентрализации и наличия множества институтов. Таким странам трудно участвовать во встречах в основных дипломатических центрах (Женева, Нью-Йорк), а тем более — следить за деятельностью других институтов, таких как ICANN, W3C[7] и IETF. Такие страны (в основном развивающиеся) выступают за принцип «единого окна», предпочтительно в виде международной организации.

Защита общественных интересов в Интернете

Одной из наиболее сильных сторон Интернета является его общественная природа, которая обеспечила быстрый рост сети, а также поощряла креативность и открытость. Защита общественной природы Интернета останется одной из важнейших проблем управления Интернетом. Эта проблема осложняется тем, что основная часть технической инфраструктуры Интернета — от межконтинентальных магистральных кабелей до локальных подсетей — находится в частной собственности. Можно ли обязать частные компании управлять своей собственностью в общественных интересах, какие части Интернета могут рассматриваться как глобальное общественное благо — вот некоторые из сложных вопросов, которые необходимо разрешить. В последнее время вопрос об общественной природе Интернета вновь приобрел актуальность в связи с дебатами о сетевой нейтральности.

---

[7] W3C, World Wide Web Consortium (Консорциум «всемирной паутины») — международная неправительственная организация, занимающаяся разработкой и внедрением технологических стандартов для «всемирной паутины» (WWW). — ***Примеч. перев.***

География и Интернет

На заре развития Интернета было распространено мнение, что эта глобальная сеть преодолевает государственные границы и разрушает принцип суверенитета. Коммуникации в Интернете легко пересекают национальные границы, а принцип анонимности пользователей заложен в самой структуре Интернета, что дало повод многим полагать, цитируя знаменитую «Декларацию независимости киберпространства», что «правительства не имеют ни морального права управлять нами [пользователями], ни методов принуждения, которые действительно могли бы нас устрашить».

Однако последние тенденции в развитии технологии, в том числе и создание более сложного геолокационного программного обеспечения, все чаще ставят под вопрос утверждение о «конце географии» в эпоху Интернета. Сегодня все еще сложно определить точно, кто находится «с той стороны экрана», но достаточно просто понять, через какого провайдера этот человек получил доступ в Интернет.

Чем сильнее Интернет привязывается к географии, тем менее уникальной становится система управления им. Например, при возможности определять географическое местоположение пользователей и транзакций сложная проблема юрисдикции в Интернете может быть решена с опорой на существующие законы.

Политическая неопределенность

Дискуссии по вопросам управления Интернетом идут в обстановке неопределенности относительно будущих направлений развития технологии, и эта неопределенность оказывает влияние на повестку дня в сфере управления Интернетом. Например, в 2002 г., когда был инициирован процесс WSIS, Google был всего лишь одной из многих поисковых систем. На завершающем этапе WSIS, в ноябре 2005 г., Google уже был одной из наиболее влиятельных компаний, определяющих будущее Интернета.

В 2002 г. блоги лишь начинали приобретать популярность. В настоящее время блогеры расшатывают правительства, расширяют границы свободы самовыражения, обладают значительным влиянием на социальную и экономическую жизнь. Список новых технологий, имеющих отношение к проблемам управления Интернетом, включает в себя Facebook, Skype, YouTube, Twitter и Wikipedia.

Сегодня многие полагают, что проблемы, изначально бывшие центральными в сфере управления Интернетом (вопросы функционирования ICANN), постепенно утрачивают свое значение. На их место приходят такие вопросы, как сетевая нейтральность, сближение различных технологий (например, телефонии, телевидения и Интернета), проблемы регу-

лирования социальных сетей (Facebook и MySpace), а также роль Google и Wikipedia как «хранителей» цифрового знания и информации.

Достижение политического равновесия

Пожалуй, весы — наиболее точный образ, отражающий суть дебатов по вопросам политики и управления в Интернете. Многие области управления Интернетом требуют нахождения равновесия между различными интересами и подходами. Такое равновесие часто представляет собой результат компромисса. Существует несколько областей политического «балансирования», в том числе:

- противоречие между свободой самовыражения и защитой общественного порядка. Широко известное противоречие между статьей 19 (свобода самовыражения) и статьей 29 (защита общественного порядка) Всеобщей декларации прав человека нашло свое отражение и в Интернете. Данное противоречие обсуждается в контексте регулирования содержания материалов и цензуры в Интернете;
- противоречие между кибербезопасностью и неприкосновенностью частной жизни. Как и в реальной жизни, обеспечение безопасности в киберпространстве ставит под угрозу некоторые права человека, в том числе право на неприкосновенность частной жизни. Баланс между кибербезопасностью и неприкосновенностью частной жизни постоянно колеблется в ту или иную сторону в зависимости от политической ситуации в мире. После террористических актов 11 сентября 2001 г. вопросы безопасности приобрели больший вес в глобальной повестке дня, и баланс сместился в сторону кибербезопасности;
- противоречие между защитой авторских прав и добросовестным использованием материалов; еще одна правовая дилемма реального мира, получившая дополнительное онлайн-измерение.

Достижение политического баланса в прошлом

В 1875 г. Международный телеграфный союз (предшественник МСЭ) проводил конференцию в Санкт-Петербурге, оказавшую влияние на будущее развитие телеграфа.

Наиболее спорным вопросом стал контроль над содержанием сообщений, передаваемых по телеграфным сетям. Такие участники конференции, как США и Великобритания, выступали за соблюдение принципа неприкосновенности частной жизни и тайны переписки с использованием телеграфа, в то время как Россия и Германия настаивали на ограничении личной неприкосновенности с целью защиты государственной безопасности, общественного порядка и морали общества.

Компромисс был достигнут с помощью старейшего дипломатического приема — дипломатической двусмысленности. Статья 2 Петербургской конвенции гарантировала тайну переписки, осуществляемой при помощи телеграфа, а статья 7 ограничивала неприкосновенность частной жизни и допускала возможность государственной цензуры. США отказались подписать конвенцию по причине статьи, одобряющей цензуру.

РУКОВОДЯЩИЕ ПРИНЦИПЫ

Руководящие принципы представляют собой определенные ценности и интересы, которые лежат в основе складывающегося режима управления Интернетом. Некоторые из этих принципов, такие как прозрачность и открытость для участия, были одобрены на WSIS. Другие были внедрены неявно, в ходе дискуссий по вопросам управления Интернетом.

«Не изобретайте колесо»

Любая инициатива в области управления Интернетом должна начинаться с анализа существующих норм, которые можно разделить на три большие группы:

- созданные специально для Интернета (например, ICANN);
- требующие существенной адаптации для применения к связанным с Интернетом вопросам (например, защита торговых марок, налогообложение электронной коммерции);
- применимые к Интернету без существенных изменений (например, защита свободы слова).

Использование существующих норм может значительно повысить правовую стабильность и упростить задачу создания режима управления Интернетом.

«Не сломано — не чините!»

Управление Интернетом должно сохранить существующую функциональность и надежность Интернета и вместе с тем оставаться достаточно гибким для внесения изменений в интересах расширения технических возможностей и повышения легитимности. Общепризнано, что стабильность и функциональность Интернета должны быть ключевыми принципами управления им. Стабильность Интернета должна быть сохранена путем использования давно известного подхода «работающего кода», предполагающего постепенное внедрение тщательно проверенных изменений в техническую инфраструктуру. Однако существует риск, что использование лозунга «Не сломано — не чините!» будет означать безоговорочный отказ от каких-либо перемен в существующей системе управления Интернетом, включая перемены, не обязательно связанные с технической инфраструктурой. В качестве одного из возможных решений предлагается использовать этот принцип как критерий оценки конкретных шагов в области управления Интернетом (например, внедрения новых протоколов и перемен в механизмах принятия решений).

Важность комплексного подхода и определения приоритетов

Комплексный подход подразумевает обсуждение не только технических, но и правовых, социальных, экономических и связанных с развитием аспектов функционирования и эволюции Интернета. Необходимо также учитывать активное сближение цифровых технологий, включая перевод телекоммуникационных услуг на использование интернет-протоколов.

«За деревьями не видно леса»

Придерживаясь комплексного подхода к переговорам по управлению Интернетом, заинтересованные стороны в то же время должны определить приоритетные с точки зрения своих интересов вопросы. Ни развивающиеся, ни развитые страны не являются однородной группой. Среди развивающихся стран имеются существенные различия в приоритетах, уровне развития и «ИКТ-готовности» (например, между развитыми с точки зрения информационно-коммуникационных технологий странами — такими, как Индия, Китай, Бразилия — и некоторыми наименее развитыми странами Африки южнее Сахары).

Комплексный подход и определение приоритетов в управлении Интернетом должны помочь заинтересованным сторонам — как из развитых, так и из развивающихся стран — сосредоточиться на определенном круге вопросов. Это должно привести к более содержательным и, возможно,

РУКОВОДЯЩИЕ ПРИНЦИПЫ ICANN

«Белая книга» по управлению Интернетом, подготовленная правительством США в 1998 г., определяет следующие руководящие принципы, которые относятся к созданию ICANN.

- Стабильность: функционирование Интернета не должно быть нарушено, особенно в том, что касается работы его ключевых структур, включая «корневые» серверы.
- Конкуренция: важно поддерживать творческий подход и гибкость, что будет способствовать дальнейшему развитию Интернета.
- Принятие решений: новая система должна включить в себя ряд ранее сложившихся правил и принципов Интернета, включая организацию «снизу», открытость и т. д.
- Представительность: в новую структуру должны войти все основные заинтересованные стороны — как в географическом (разные страны), так и профессиональном (различные профессиональные сообщества) смысле.

менее политизированным переговорам. Заинтересованные стороны тогда будут группироваться вокруг проблем, а не традиционных сильно политизированных «разделительных линий» (например, развитые — развивающиеся страны, правительства — гражданское общество).

Принцип технологической нейтральности

В соответствии с принципом технологической нейтральности политический курс вырабатывается независимо от отдельных технологических или технических решений. Например, правовые нормы в области защиты частной жизни должны определять то, что подлежит защите (например, личные данные, медицинские записи), но не то, как это должно защищаться (например, доступ к базам данных, шифрование данных).

Технологическая нейтральность предоставляет множество преимуществ с точки зрения управления. Она обеспечивает долгосрочную применимость регулирующих принципов вне зависимости от будущих направлений технологического развития и вероятной конвергенции ключевых технологий (телекоммуникаций, СМИ, Интернета). Однако можно обозначить ряд недостатков, присущих данному принципу, особенно в случаях перехода от существующих правил регулирования телекоммуникационной отрасли к новым.

Принцип сетевой нейтральности

Сетевая нейтральность — один из центральных принципов Интернета, делающий возможной передачу данных между конечными точками Интернета (пользователями и службами) независимо от содержания этих данных. Принцип нейтральности зачастую приводится в качестве основной причины, обусловившей быстрое развитие Интернета. Создателям Google, Skype и Wikipedia, как и многих других компаний, нужно было лишь следить за работой нескольких интернет-протоколов, чтобы воплотить свои идеи в жизнь. Они не нуждались в разрешении или специальном допуске, чтобы использовать свои изобретения для создания бизнеса в Интернете.

Споры о сетевой нейтральности — результат значительного коммерческого потенциала интернет-услуг. Различные заинтересованные стороны и по разным причинам предлагают дифференцировать интернет-трафик. Новые и более быстрые интернет-сервисы для передачи мультимедиа и видеотрафика — одно из наиболее прибыльных направлений коммерческого использования Интернета. Для предоставления подобных услуг необходимо создание нового «уровня», иногда описываемого как «VIP-Интернет». Основные сторонники подобного решения — крупные телекоммуникационные компании, такие как Verizon, AT&T, Comcast, представители индустрии развлечений и поставщики оборудования.

Противоположный этому подходу принцип сетевой нейтральности получил горячую поддержку представителей интернет-индустрии, включая таких гигантов, как Google, eBay, Yahoo! и Amazon, организаций по защите прав пользователей, а также организаций гражданского общества. Сетевая нейтральность уже стала предметом обсуждения на самом высоком политическом уровне, в том числе в Конгрессе США; сохранение сетевой нейтральности — один из важнейших принципов на технологической повестке дня президента США Барака Обамы.

Превращайте подразумеваемые технические решения в ясные политические принципы

В интернет-сообществе весьма распространено мнение, что особенности технического устройства Интернета способствуют распространению определенных общественных ценностей, например свободы общения. Например, принцип сетевой нейтральности, в соответствии с которым данные передаются в сети между двумя конечными точками без привлечения «посредников», часто провозглашается гарантом свободы слова в Интернете. Из этого можно сделать ошибочный вывод, что технологические решения сами по себе достаточны для защиты и продвижения общественных ценностей.

Развитие Интернета в последнее время, например, использование «брандмауэров» для ограничения потока информации, доказывает, что технологию можно использовать с разными целями, в том числе взаимно противоречащими друг другу. Всегда, когда это возможно, политические принципы, такие как свобода коммуникации, должны быть четко обозначены на политическом уровне, а не предполагаться неявно, на техническом уровне. Технические решения призваны способствовать реализации политических принципов, но не должны быть единственным способом их продвижения.

Помните о рисках управления обществом с помощью программного кода

Лоренс Лессиг в книге «Код и другие законы киберпространства» обращает внимание на один из ключевых аспектов взаимоотношений между технологией и политикой: по мере возрастания зависимости от Интернета современное общество начинает регулироваться программным кодом, а не законами. В конечном счете, некоторые законодательные функции парламентов и правительств могут де-факто принять на себя компьютерные компании и разработчики программного обеспечения. С помощью программного обеспечения и технических решений они смогут влиять на жизнь обществ, все больше зависящих от Интернета. Если

общество будет управляться с помощью кода (а не законов), это будет существенным вызовом самим основам политической и правовой организации современного общества.

АНАЛОГИИ

Хотя аналогии часто обманчивы,
они менее обманчивы, чем что-либо другое.
Сэмюэл Батлер, английский писатель

Аналогия помогает нам понимать новые явления через уже известные. Проведение параллелей между примерами из прошлого и сегодняшним днем, несмотря на связанные с этим риски, является ключевым познавательным процессом в праве и политике. Большинство судебных дел, связанных с Интернетом, решаются посредством аналогий.

Использование аналогий в управлении Интернетом имеет ряд важных ограничений. Во-первых, Интернет — широкое понятие, охватывающее разнообразные услуги: электронную почту (см. аналогию с телефоном), услуги «всемирной паутины» WWW (см. аналогию с теле- и радиовещанием) и базы данных (см. аналогию с библиотекой). Любая аналогия с каким-либо одним аспектом Интернета может излишне упростить понимание данной технологии.

Во-вторых, по мере сближения разнообразных телекоммуникационных и медиа-услуг традиционные различия между ними исчезают. Например, с внедрением технологии интернет-телефонии (VoIP) становится все сложнее провести разграничение между Интернетом и телефонной связью.

Несмотря на эти ограничения, аналогии остаются мощным и основным познавательным инструментом при разрешении судебных дел и создании режима управления Интернетом. Некоторые из наиболее часто используемых аналогий обсуждаются ниже.

Интернет — телефонная связь

Общие черты. На ранних этапах развития Интернета на появление этой аналогии повлиял тот факт, что телефонные линии использовались для коммутируемого доступа в Интернет. К тому же между телефоном и Интернетом (электронной почтой и чатом) существует и функциональное сходство: оба являются средствами непосредственного и личного общения. Более поздняя аналогия между телефоном и Интернетом обращает внимание на возможное использование системы телефонных номеров при организации системы доменных имен.

Отличия. Передача данных в Интернете основана на использовании пакетов данных, а не электрических цепей (как при телефонной связи).

В отличие от телефонной связи, в Интернете нельзя гарантировать предоставление услуг; можно только обещать, что для этого будут предприняты «все усилия». Эта аналогия отражает только один аспект коммуникации: использование электронной почты или чата. Другие важные способы применения Интернета — «всемирная паутина» (WWW), мультимедиа и т. д., не имеют сходства с телефоном.

Кем используется. Противниками какого-либо существенного регулирования материалов Интернета (в основном в США). Если Интернет схож с телефоном, то содержание данных, передаваемых по Интернету, как и телефонные разговоры, не должно контролироваться.

Эту аналогию также используют те, кто доказывает, что Интернет должен регулироваться, как и другие системы коммуникации (например, телефонная связь, почта), национальными органами власти при координирующей роли международных организаций — таких как Международный союз электросвязи [6].

Интернет — почта

Общие черты. Существует аналогия с точки зрения функций, а именно доставки сообщений. Само название «электронная почта» подчеркивает это сходство.

Отличия. Эта аналогия касается только одного из интернет-сервисов — электронной почты. Кроме того, почтовая служба является гораздо более сложной посреднической структурой между отправителем и получателем почты, чем система электронной почты, где функцию посредника выполняет интернет-провайдер или почтовая система вроде Yahoo! или Hotmail.

Кем используется. Всемирная почтовая конвенция проводит эту аналогию между обычной почтой и электронной, определяя последнюю как «почтовую службу, использующую телекоммуникации для передачи сообщений». Эта аналогия может иметь важные последствия, например, с точки зрения доставки официальных документов. Так, получение решения суда по электронной почте должно в таком случае считаться официальным вручением соответствующего документа.

Семьи погибших в Ираке американских солдат пытались апеллировать к аналогии между частной корреспонденцией (письмами) и электронной почтой, чтобы получить доступ к частным электронным сообщениям и блогам (онлайн-дневникам) своих близких, доказывая, что они должны унаследовать электронные письма и блоги, как это делается с письмами и дневниками.

Интернет-провайдерам оказалось непросто разрешить эту проблему, вызвавшую бурю эмоций. Вместо того, чтобы согласиться с аналогией

между письмами и электронной почтой, большинство провайдеров отказало в доступе, сославшись на соглашение о защите тайны корреспонденции, заключаемое с пользователями.

Бывший глава Совета директоров ICANN Пол Туми привел такую аналогию между почтовой системой и функциями ICANN: «Если представить себе Интернет в виде почтовой системы, то доменные имена и IP-адреса, по сути, гарантируют, что письмо дойдет по адресу, написанному на конверте. Они не имеют отношения к тому, что лежит в конверте, кто отправляет конверт, кто имеет право прочитать письмо, сколько времени конверт будет добираться до адресата, сколько стоит его отправка. Ни один из этих вопросов не важен для деятельности ICANN. Ее функция — гарантировать, что письмо дойдет по адресу».

Интернет — телевидение

Общие черты. Изначально аналогия была связана с внешним сходством между экраном компьютера и телевизора. Более утонченная аналогия опирается на использование обоих средств коммуникации — Интернета и телевидения — для вещания на широкую аудиторию.

Отличия. Интернет обладает более широкими возможностями передачи данных, чем телевидение. Хотя сходство между телевизором и экраном компьютера очевидно, между ними существуют важные структурные отличия. Телевидение позволяет передавать информацию «от одного ко многим», в то время как Интернет делает возможными различные виды коммуникации («один с одним», «один со многими», «многие со многими»).

Кем используется. Эту аналогию используют те, кто стремится к установлению более строгого контроля над содержанием материалов Интернета. По их мнению, поскольку возможности Интернета как средства массовой информации сходны с возможностями телевидения, Интернет необходимо строго контролировать. Правительство США пыталось использовать эту аналогию в знаменитом деле «Рино против Американского союза за гражданские свободы» (Reno vs. ACLU). Источником этого дела стал принятый Конгрессом Акт о пристойности коммуникаций, предусматривавший тщательный контроль над содержанием материалов Интернета для предотвращения доступа детей к порнографическим материалам. Суд отказался признать правомочность аналогии с телевидением.

Интернет — библиотека

Общие черты. Интернет иногда рассматривают как огромное хранилище информации и употребляют для его описания термин «библиотека»: «огромная цифровая библиотека», «кибербиблиотека», «Александрийская библиотека XXI века» и т. д.

Отличия. Хранение информации и данных — лишь один из аспектов Интернета; между Интернетом и библиотекой существуют важные различия:

- традиционные библиотеки обычно обслуживают людей, живущих в определенном месте (городе, стране и т. д.), в то время как Интернет — глобальное явление;
- книги и статьи обычно публикуются с соблюдением определенных процедур, гарантирующих контроль качества (редактура). Материалы, размещенные в Интернете, не всегда проходят редактирование;
- материалы библиотеки организованы определенным образом, облегчающим их поиск. В Интернете, помимо нескольких каталогов (таких как Yahoo!), индексирующих лишь небольшую часть доступной информации, такой схемы классификации нет;
- помимо библиографических описаний содержание материалов библиотеки (текст книг и статей) недоступно читателю, пока он не возьмет ту или иную книгу. В Интернете доступ к информации открыт для всех и немедленно — через поисковые машины.

Кем используется. Специалистами в различных проектах, целью которых является создать всеобъемлющую систему информации и знаний по определенным вопросам (порталы, базы данных и т. д.). В последнее время аналогия с библиотекой используется в связи с проектом Google Books, основная задача которого — оцифровка всех печатных изданий.

Интернет — видеомагнитофон, копировальный аппарат

Общие черты. Центральным моментом этой аналогии является воспроизведение и распространение материалов (например, текстов книг). Компьютеры упростили создание копий за счет функции «скопировать и вставить». Это, в свою очередь, упростило распространение информации с использованием Интернета.

Отличия. Функции компьютера не ограничены копированием материалов, хотя сам процесс копирования в Интернете гораздо проще, чем в случае с видеомагнитофоном или копировальным аппаратом.

Кем используется. Эта аналогия использовалась в связи с принятым в США Законом об авторских правах в цифровую эпоху (Digital Millennium Copyright Act, DMCA), который устанавливал ответственность организаций, способствующих нарушению авторского права (например, разрабатывающих соответствующее программное обеспечение). Контраргумент в таких случаях состоит в том, что разработчики программного обеспечения, как и производители видеомагнитофонов и ксероксов, не

могут знать наверняка, будут ли их продукты использоваться в незаконных целях. Эта аналогия использовалась в судебных делах против разработчиков программного обеспечения для обмена файлами по принципу пиринга (непосредственно между компьютерами пользователей), такого, как Grokster и StreamCast.

Хамадун Турэ, Генеральный секретарь МСЭ, использовал аналогию с автомагистралью, сравнив автомагистрали с телекоммуникационными сетями, а интернет-трафик — с грузовиками или машинами: «Я привел простой пример, сравнив Интернет и передачу данных с потоками грузовиков или машин на автомагистрали. То, что вы владеете автомагистралью, не дает вам прав собственности на грузовики и машины, проезжающие по ней, и, конечно, на товары, которые они перевозят, и наоборот. Это простая аналогия. Но для того, чтобы транспорт ехал без помех, при постройке дорог и мостов необходимо учесть вес, высоту и скорость грузовиков. В противном случае система не будет работать. По моему мнению, это отражает взаимосвязь между Интернетом и телекоммуникационными сетями. Они обречены на совместную работу» [7].

Интернет — магистраль

Общие черты. Эта аналогия связана с тем, насколько новые открытия и достижение новых рубежей очаровывают американцев. Железные дороги и автомагистрали, как правило, являются частью этого процесса. Интернет, как граница виртуального мира, метафорически соотносится с магистралями реального мира.

Отличия. Помимо концепции «перевозки — передачи» информации, другого сходства между Интернетом и магистралями нет. По Интернету перемещаются неосязаемые материалы (данные), в то время как дороги облегчают передвижение людей и товаров.

Кем используется. Аналогия с автомагистралью активно использовалась с середины 1990-х гг., после того, как А. Гор ввел в употребление термин «информационная супермагистраль» (information superhighway). Термин «магистраль» также использовался немецким правительством, чтобы оправдать введение в июне 1997 г. более строгого закона о контроле над содержанием Интернета: «Это либеральный закон, который не имеет ничего общего с цензурой, но четко обозначает, что может и не может делать провайдер. Интернет — это средство передачи и распространения знания... как и для магистралей, для него необходимы правила движения».

Интернет — открытое море

Общие черты. Изначально аналогия появилась благодаря тому, что Интернет, как и открытое море, находился за пределами юрисдикции государств. На сегодняшний день очевидно, что большая часть Интер-

нета подпадает под юрисдикцию той или иной страны. Техническая инфраструктура, по которой передается интернет-трафик, находится в собственности частных и государственных компаний, как правило, телекоммуникационных операторов. Ближайшей аналогией в этом смысле является судоходная компания, транспортирующая контейнеры.

Отличия. Морской транспорт регулируется обширным массивом международных соглашений, который берет свое начало от Конвенции по морскому праву. Ее положения развивает и дополняет множество конвенций, принятых Международных морской организацией, которые регулируют проблемы обеспечения безопасности или защиты окружающей среды. Эти конвенции регулируют деятельность, выходящую за пределы государственной юрисдикции, например, в открытом море. В отношении передачи данных в Интернете не существует ничего подобного.

Кем используется. Эта аналогия используется теми, кто выступает за международное регулирование Интернета. Практическим следствием этой аналогии является то, что к Интернету применима концепция римского права res communis omnium (общего достояния), которая используется в отношении открытого моря.

КЛАССИФИКАЦИЯ ВОПРОСОВ УПРАВЛЕНИЯ ИНТЕРНЕТОМ

Управление Интернетом — сложная новая область, требующая предварительного «нанесения на карту» и классификации. Сложность управления Интернетом связана с его междисциплинарной природой, охватывающей технологию, общественно-экономические вопросы, развитие, право и политику.

Практическая потребность в классификации ярко проявилась в процессе WSIS. На начальном этапе, в ходе подготовки к встрече в Женеве в 2003 г., многим участникам было непросто разобраться во всех тонкостях управления Интернетом. Концептуальная схема проблемного поля, предложенная в различных исследовательских трудах, а также в итоговом отчете Рабочей группы по вопросам управления Интернетом (WGIG), способствовала повышению эффективности переговорного процесса WSIS.

Итоговый отчет WGIG (2004) обозначил следующие важнейшие проблемы:

- вопросы, касающиеся инфраструктуры и управления важнейшими интернет-ресурсами;
- вопросы, касающиеся использования Интернета, включая спам, сетевую безопасность и киберпреступность;

- вопросы, связанные с Интернетом, но имеющие далеко идущие последствия, выходящие за рамки Интернета, за которые отвечают соответствующие действующие организации, например, вопросы прав интеллектуальной собственности или международной торговли;
- вопросы, касающиеся проблем развития в контексте управления Интернетом, в частности, укрепления потенциала развивающихся стран.

Повестка дня первого Форума по вопросам управления использованием Интернета, проходившего в Афинах в 2006 г., включала в себя обсуждение следующих проблемных областей: доступ, безопасность, открытость и разнообразие. В ходе второго IGF, проходившего в Рио-де-Жанейро в 2007 г., в повестку дня была внесена пятая проблемная область — управление ключевыми ресурсами Интернета.

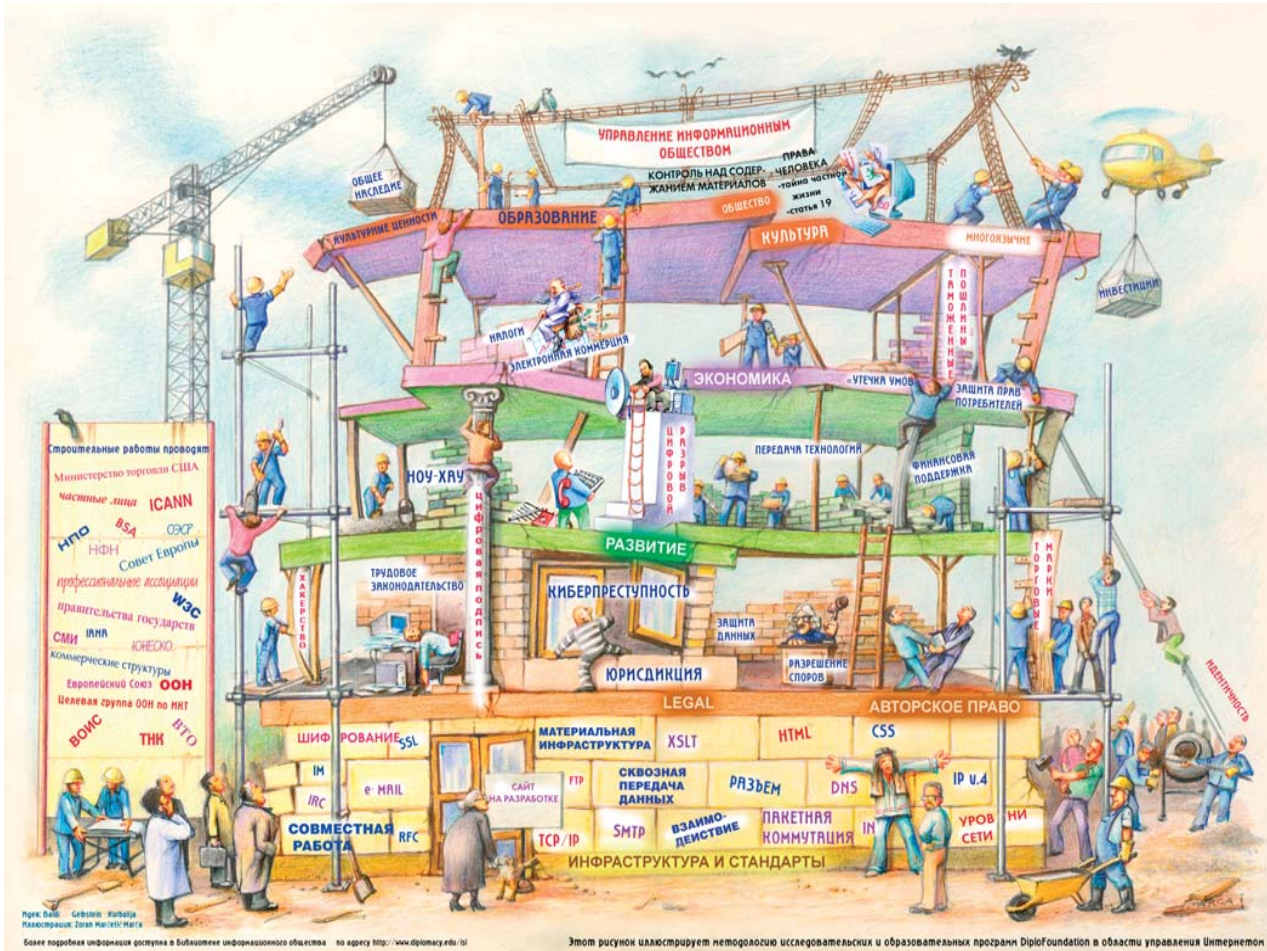
При всех различиях в подходах к классификации управление Интернетом затрагивает относительно неизменный набор из 40—50 конкретных проблем; актуальность каждой из них может изменяться. В частности, спам выступал в качестве отдельной проблемы в классификации WGIG 2004 г., однако в ходе встреч IGF его политическое значение снизилось, и спам стал всего лишь одной из не самых существенных тем, обсуждаемых в рамках проблем безопасности.

Разработанная Diplo классификация аспектов управления Интернетом разбивает основные проблемы управления Интернетом на пять групп. Чтобы приблизить терминологию к миру дипломатии, Diplo использует понятие «корзина». (Оно было введено в дипломатическую практику во время Совещания по безопасности и сотрудничеству в Европе, СБСЕ.) С 1997 г., когда фонд Diplo начал разработку классификатора, используются пять корзин:

1) инфраструктура и стандартизация;
2) правовые аспекты;
3) экономические аспекты;
4) аспекты, связанные с развитием;
5) социокультурные аспекты.

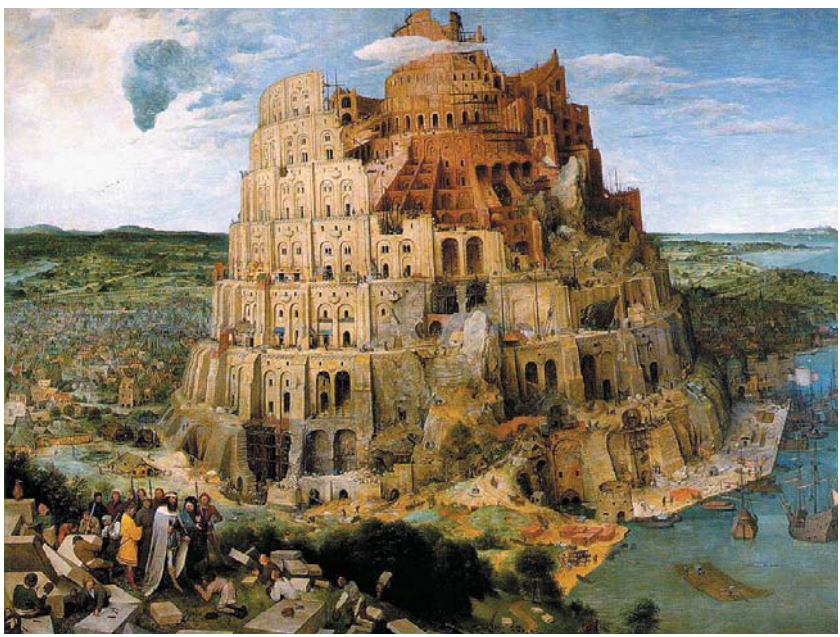
Классификация, разработанная Diplo, отражает как упомянутые выше политические подходы WGIG и IGF, так и результаты научных исследований в данной области. Классификация постоянно уточняется и дополняется с учетом комментариев от участников образовательных программ Diplo (700 выпускников на 2009 г.), результатов научных исследований и политической практики.

Модель «пяти корзин» представлена в метафорической форме на иллюстрации «Строящееся здание», разработанной исследователями Diplo.


УПРАВЛЕНИЕ ИНФОРМАЦИОННЫМ ОБЩЕСТВОМ
ОБЩЕЕ НАСЛЕДИЕ
КОНТРОЛЬ НАД СОДЕРЖАНИЕМ МАТЕРИАЛОВ
ПРАВА ЧЕЛОВЕКА
-тайна частной жизни
-статья 19
ОБЩЕСТВО
КУЛЬТУРНЫЕ ЦЕННОСТИ
ОБРАЗОВАНИЕ
КУЛЬТУРА
МНОГОЯЗЫЧИЕ
ИНВЕСТИЦИИ
ТАМОЖЕННЫЕ ПОШЛИНЫ
НАЛОГИ
ЭЛЕКТРОННАЯ КОММЕРЦИЯ
ЭКОНОМИКА
УТЕЧКА УМОВ
ЗАЩИТА ПРАВ ПОТРЕБИТЕЛЕЙ
ЦИФРОВОЙ РАЗРЫВ
ПЕРЕДАЧА ТЕХНОЛОГИЙ
ФИНАНСОВАЯ ПОДДЕРЖКА
НОУ-ХАУ
ЦИФРОВАЯ ПОДПИСЬ
РАЗВИТИЕ
ТОРГОВЫЕ МАРКИ
ХАКЕРСТВО
ТРУДОВОЕ ЗАКОНОДАТЕЛЬСТВО
КИБЕРПРЕСТУПНОСТЬ
ЗАЩИТА ДАННЫХ
ЮРИСДИКЦИЯ
РАЗРЕШЕНИЕ СПОРОВ
LEGAL
АВТОРСКОЕ ПРАВО
ПАТЕНТНОСТЬ
Строительные работы проводят
Министерство торговли США
частные лица
ICANN
НПО
BSA
ОЭСР
НФН
Совет Европы
профессиональные ассоциации
W3C
правительства государств
СМИ
IRMA
ЮНЕСКО
коммерческие структуры
Европейский Союз
ООН
Целевая группа ООН по ИКТ
ВОИС
ТНК
ВТО
ШИФРОВАНИЕ
SSL
МАТЕРИАЛЬНАЯ ИНФРАСТРУКТУРА
XSLT
HTML
CSS
IM
IRC
e-MAIL
САЙТ НА РАЗРАБОТКЕ
FTP
СКВОЗНАЯ ПЕРЕДАЧА ДАННЫХ
РАЗЪЕМ
DNS
IP v.4
СОВМЕСТНАЯ РАБОТА
RFC
TCP/IP
SMTP
ВЗАИМОДЕЙСТВИЕ
ПАКЕТНАЯ КОММУТАЦИЯ
IN
УРОВНИ СЕТИ
ИНФРАСТРУКТУРА И СТАНДАРТЫ
Идея: Baldi Gebstein Kurbalija
Иллюстрация: Zoran Marcetic Mar'a
Более подробная информация доступна в Библиотеке информационного общества по адресу http://www.diplomacy.edu/isl
Этот рисунок иллюстрирует методологию исследовательских и образовательных программ DiploFoundation в области управления Интернетом

«СТРОЯЩЕЕСЯ ЗДАНИЕ»: УПРАВЛЕНИЕ ИНТЕРНЕТОМ — НЕ СТРОИМ ЛИ МЫ ВАВИЛОНСКУЮ БАШНЮ XXI ВЕКА?

Картина Питера Брейгеля Старшего (1563), находящаяся в Музее истории искусств в Вене, изображает строительство Вавилонской башни (другая, меньшая по размерам, картина того же года и на тот же сюжет выставлена в музее Бойманса ван Бейнингена в Роттердаме). Согласно Библии (Быт. 11:5-7), Бог не позволил людям достроить башню, смешав язык строителей, «так чтобы один не понимал речи другого».



При рассмотрении вопросов Интернета аналогия со строительством Вавилонской башни кажется весьма уместной. Это сравнение натолкнуло авторов на образ другого строящегося здания, цель которого не достичь небес, а затронуть каждого на планете. Сотрудники Diplo разработали общую схему для дискуссий по управлению Интернетом, которую иллюстрирует рисунок на предыдущей странице. Каждый этаж здания обсуждается в последующих главах. Важно понимать, что все этажи здания связаны между собой, а его строительство постоянно продолжается и никогда не закончится.

ПРИМЕЧАНИЯ

[1] Показатели, характеризующие рост Интернета, следует воспринимать со здоровой долей скепсиса и осторожности. Сейчас доступно множество документальных подтверждений того, что телекоммуникационный бум конца 1990-х гг. и провал крупных инвестиций в этот сектор стали результатом абсолютно нереалистичных оценок, в соответствии с которыми интернет-трафик должен был удваиваться каждые три месяца. Данное предположение, в корне неверное, в ряде случаев упоминалось даже государственными чиновниками, работающими в сфере телекоммуникаций, в том числе Ридом Хантом, главой Федеральной комиссии по связи США. Этот феномен описан в ряде статей, в том числе: Andrew Odlyzko, "Internet Growth: Myth and Reality, Use and Abuse" [8] (адрес в Интернете: http://www.dtc.umn.edu/~odlyzko/doc/internet.growth.myth.pdf), а также "Internet as Hyperbole" (адрес в Интернете: http://folk.uio.no/gisle/essay/diff.html).

[2] Это определение опирается на положения теории международных режимов. Основатель теории международных режимов Стивен Краснер отмечает, что «режим может быть определен как набор явных и неявных принципов, норм, правил и процедур принятия решений, вокруг которых сходятся ожидания акторов в данной области международных отношений. Принципы — это представления о фактах, причинно-следственных связях и нормах морали. Нормы — это стандарты поведения, определенные в терминах прав и обязательств. Правила — это специфические запреты и предписания к действию. Процедуры принятия решений представляют собой доминирующие практики принятия и реализации коллективных решений». Krasner, Stephen "Introduction" // Stephen D. Krasner (ed.) International Regimes, Ithaca, N.Y.: Cornell University Press, 1983.

[3] Терминологическая путаница усугубляется в результате различного использования термина «управление» международными организациями. Например, термин «надлежащее управление» (good governance) употреблялся в программах Всемирного банка по реформе государственного аппарата, нацеленных на достижение прозрачности, уменьшение коррупции и повышение эффективности деятельности чиновников. В этом контексте термин «управление» был непосредственно связан с ключевыми правительственными функциями.

[4] Shannon, Victoria. "What's in an 'i'? Internet Governance" // International Herald Tribune, 3.12.2006 (адрес в Интернете: http://www.iht.com/articles/2006/12/03/technology/btitu.php).

[5] Об эволюции использования термина «Интернет» в ходе подготовки к Женевскому этапу WSIS см.: DiploFoundation. The Emerging Language of ICT Diplomacy — Key Words (адрес в Интернете: http://www.diplomacy.edu/IS/Language/html/words.htm).

[8] Все ссылки на интернет-ресурсы, приведенные в книге, проверены 14 ноября 2008 г.

[6] Фолькер Китц приводит доказательства в пользу правомерности проведения аналогий между системой телефонной связи и пространством имен и адресов Интернета. См.: Volker Kitz (2004). ICANN May Be the Only Game in Town, But Marina del Rey Isn't the Only Town on Earth: Some Thoughts on the So-Called "Uniqueness" of the Internet (адрес в Интернете: http://www.smu.edu/csr/articles/2004/Winter/Kitz.pdf).

[7] Выдержки из речи, произнесенной в ходе Конференции ICANN в Каире 6 ноября 2008 г. (адрес в Интернете: https://cai.icann.org/files/meetings/cairo2008/toure-speech-06nov08.txt).

Раздел 2

Инфраструктура и стандартизация

ИНФРАСТРУКТУРА И СТАНДАРТИЗАЦИЯ

Корзина «Инфраструктура и стандартизация» включает в себя основополагающие, в основном технические, вопросы, связанные с функционированием Интернета. Основным критерием отнесения того или иного вопроса к данной корзине является его значимость с точки зрения базовой технической функциональности Интернета. Проблемы, относящиеся к этой корзине, можно разделить на две группы.

Первая группа включает в себя наиболее важные вопросы, без решения которых ни Интернет, ни «всемирная паутина» (WWW) не могли бы существовать [1], и представлена следующими тремя уровнями, или слоями:

1) телекоммуникационная инфраструктура, по которой передаются потоки интернет-данных (трафик);
2) технические стандарты и услуги — инфраструктура, благодаря которой Интернет работает (например, TCP/IP, DNS, SSL);
3) стандарты материалов (контента) и приложений (например, HTML, XML).

Вторая группа проблем включает в себя вопросы, связанные с обеспечением безопасного и стабильного функционирования инфраструктуры Интернета, и охватывает проблемы кибербезопасности, шифрования данных и борьбы со спамом.

ТЕЛЕКОММУНИКАЦИОННАЯ ИНФРАСТРУКТУРА

СОВРЕМЕННОЕ СОСТОЯНИЕ

Потоки интернет-данных могут передаваться с помощью самых разнообразных носителей: телефонных проводов, оптоволоконного кабеля, спутников, УКВ-сигналов и беспроводной связи. Для передачи интернет-трафика может быть использована даже обычная электрическая сеть [2].

Поскольку передача интернет-трафика опирается на уровень телекоммуникаций, любые новые меры регулирования этой отрасли неизбежно влияют и на Интернет. Телекоммуникационная инфраструктура регулируется целым рядом государственных и частных организаций, как на национальном, так и на международном уровне. Ключевыми международными организациями в сфере регулирования телекоммуникаций являются, например, Международный союз электросвязи (МСЭ), который разработал подробные правила, регулирующие отношения между национальными операторами, распределение радиочастот и положение спутников, а также Всемирная торговая организация (ВТО), сыгравшая ключевую роль в либерализации телекоммуникационных рынков по всему миру [3].

Однако роли ВТО и МСЭ существенно отличаются. МСЭ устанавливает детально разработанные технические стандарты, международные нормы, касающиеся непосредственно телекоммуникаций, и предоставляет помощь развивающимся странам [4]. ВТО же задает рамки общих правил рынка [5].

Регламент международной электросвязи, подготовленный МСЭ в 1988 г., способствовал международной либерализации ценообразования и услуг и сделал возможным инновационное использование таких базовых услуг, как международная аренда линий. Таким образом, была создана инфраструктурная база для быстрого развития Интернета в 1990-е гг.

Либерализация национальных рынков телекоммуникаций дала крупным компаниям отрасли (AT&T, Cable and Wireless, France Telecom, Sprint, WorldCom) возможность глобального расширения своих рынков. Поскольку основная часть интернет-трафика передается по линиям связи, принадлежащим этим компаниям, они оказывают существенное влияние на развитие Интернета.

ВОПРОСЫ

«Последняя миля» — местные линии связи

«Последней милей» (или, по-английски, «местной петлей», local loop) называется линия связи между компанией — поставщиком услуг Интернета (провайдером) и конечным пользователем. Проблемы с местными линиями связи являются препятствием для более широкого распространения Интернета во многих (чаще развивающихся) странах.

Одним из возможных недорогих решений проблемы «последней мили» может стать использование беспроводной связи. Помимо новых технологий, которые становятся все более доступными, решение проблемы местных линий связи зависит также от либерализации этого сегмента рынка телекоммуникаций.

Либерализация рынка телекоммуникаций

Местные рынки услуг связи либерализованы во многих странах. Однако многие развивающиеся страны, правительства которых обладают монополией на телекоммуникационные услуги, столкнулись с непростой задачей: как либерализовать рынок услуг связи и сделать его более эффективным и в то же время сохранить важный источник поступлений в бюджет от монополии на телекоммуникации [6]. Международная помощь, постепенные реформы и увязывание процесса либерализации с защитой общественных интересов могут помочь выйти из этой непростой ситуации.

Установление технических стандартов инфраструктуры

Технические стандарты все в большей степени устанавливаются частными и профессиональными институтами. Например, стандарт беспро-

Технология, стандарты и политика

Дискуссия о сетевых протоколах демонстрирует, как стандарты могут быть «политикой иными средствами». Вмешательство правительства в бизнес и технологию (например, в виде установления норм безопасности или антимонопольной деятельности) обычно воспринимается как явление, имеющее политическую и общественную значимость; в то же время технические стандарты обычно считаются социально нейтральными, а потому не представляющими интереса для истории. Однако технические решения могут иметь далеко идущие экономические и социальные последствия, изменяя баланс сил между конкурирующими фирмами или странами и ограничивая свободу пользователей. Попытки установить официальные стандарты выводят частные технические решения разработчиков той или иной системы на общественное поле; таким образом, «битвы» по поводу стандартов могут выявить скрытые надежды и конфликты интересов. Сам пыл, с которым заинтересованные стороны спорят по поводу тех или иных решений в отношении стандартов, служит для нас признаком того, что за чисто техническими решениями скрывается более глубокий смысл.

Источник: Janet Abbate. *Inventing the Internet*. MIT Press, 1999.

водной связи (WiFi) IEEE 802.11b был разработан Институтом инженеров по электротехнике и электронике (IEEE). Сертификация оборудования, совместимого со стандартом WiFi, осуществляется организацией WiFi Alliance. Сама роль этих институтов, а именно установление и внедрение стандартов на столь быстро развивающемся рынке, дает им возможность оказывать существенное влияние на него.

ПРОТОКОЛ УПРАВЛЕНИЯ ПЕРЕДАЧЕЙ / ИНТЕРНЕТ-ПРОТОКОЛ (TCP/IP)

СОВРЕМЕННОЕ СОСТОЯНИЕ

TCP/IP — основной технический стандарт, определяющий способ передачи данных по Интернету. Этот протокол основан на трех принципах: пакетная коммутация, сквозная передача данных и устойчивость к помехам. В вопросах управления Интернетом, связанных с протоколом TCP/IP, можно выделить два важных направления: а) внедрение новых стандартов, б) распределение IP-адресов. Стандарты для TCP/IP устанавливаются Рабочей группой по проектированию Интернета (IETF). Поскольку этот протокол имеет принципиальное значение для функционирования Интернета, он строго охраняется IETF. Любые изменения, вносимые в протокол TCP/IP, нуждаются в предварительном всестороннем обсуждении и подтверждении их эффективности для решения текущих проблем (принцип «работающего кода»).

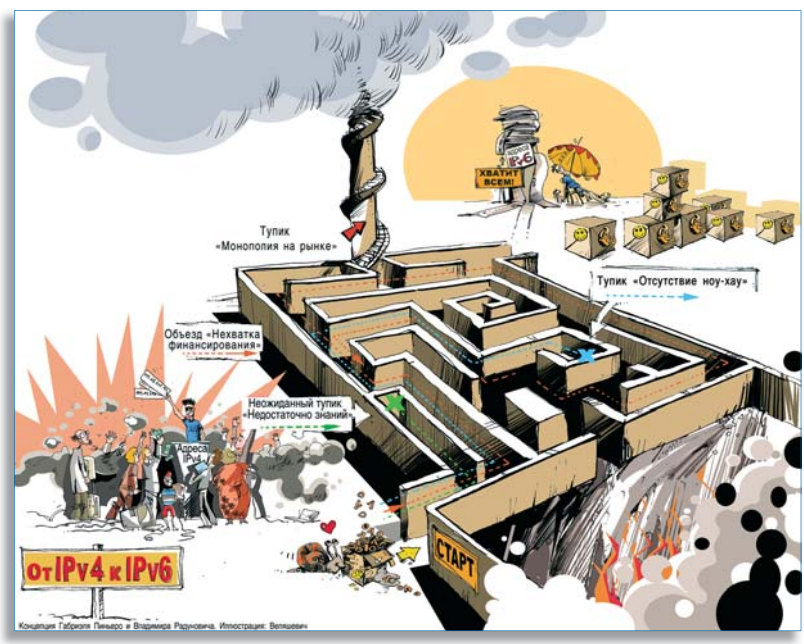
IP-адреса — это числовые адреса, которые должны иметь все компьютеры, подключенные к сети. Эти адреса уникальны; два компьютера, подключенные к Интернету, не могут иметь одинаковый IP-адрес. Это делает адреса потенциально дефицитным ресурсом. Система распределения IP-адресов организована иерархически. «Наверху» находится Администрация по присвоенным именам в Интернете (Internet Assigned Numbers Authority, IANA), являющаяся дочерней структурой ICANN. IANA распределяет блоки IP-адресов между пятью региональными интернет-регистратурами [7]. Региональные интернет-регистратуры распределяют адреса между национальными и местными интернет-регистратурами, которые, в свою очередь, передают IP-адреса на более низкий уровень, небольшим интернет-провайдерам, компаниям и частным лицам.

ВОПРОСЫ

Как преодолеть ограниченность IP-адресов: переход на протокол IPv6

На сегодняшний день при использовании IPv4 (интернет-протокола версии 4) общее количество IP-адресов составляет около 4 миллиардов и может быть исчерпано в течение ближайших нескольких лет в результате появления новых поколений устройств, подключенных к Интернету — таких как мобильные телефоны, карманные компьютеры, игровые приставки и бытовые электроприборы. Озабоченность тем, что IP-адреса могут закончиться (что, в итоге, воспрепятствует дальнейшему развитию Интернета), заставила техническое сообщество предпринять следующие важные шаги:

- рационализация использования существующего запаса IP-адресов, что было достигнуто за счет использования технологии преобразования сетевых адресов (NAT);
- внедрение механизма бесклассовой адресации (Classless Inter-Domain Routing, CIDR) с целью приостановить расточительное распределение IP-адресов региональными регистратурами;
- внедрение новой версии интернет-протокола, IPv6, которая предоставляет гораздо больший запас IP-адресов (430 000 000 000 000 000 000).



Действия технического интернет-сообщества в отношении потенциальной проблемы исчерпания IP-адресов представляют собой пример быстрого и упреждающего управления ситуацией. Технологии NAT и CIDR позволили преодолеть текущие сложности, однако оптимальным долгосрочным решением является переход на новую версию протокола IPv6. Хотя IPv6 был разработан еще в 1996 г., его внедрение идет очень медленными темпами. Поскольку IP-адреса, доступные в версии протокола IPv4, в 2011 г. будут полностью исчерпаны, такой медленный переход на новую версию протокола начинает угрожать настоящим кризисом.

Одной из основных сложностей в ходе внедрения IPv6 является недостаточная обратная совместимость между версиями IPv6 и IPv4. Сети, использующие IPv6, не могут напрямую взаимодействовать с сетями, использующими IPv4, которых на сегодняшний день большинство. Так как велика вероятность того, что сетям, использующим версии IPv4 и IPv6, в будущем придется сосуществовать, важно обеспечить доступность новых IPv6-сетей, чтобы они не оставались изолированными «островами». Техническое решение проблемы предполагает создание специальных «туннелей» между двумя типами сетей, что усложнит систему маршрутизации в Интернете, а также повлечет за собой появление ряда иных сопутствующих проблем.

Внедрение также откладывается по причине отсутствия интереса со стороны провайдеров интернет-услуг и пользователей. Хотя им известно об угрозе исчерпания IP-адресов, они предпочитают действовать по принципу «поживем — увидим». Так, например, результаты недавнего исследования, проведенного в Японии, показывают, что хотя более 70 % провайдеров знают об угрозе исчерпания IP-адресов в версии протокола IPv4, только 30 % из них готовятся к переходу на IPv6. В ситуации, когда проблема не может быть решена на основании рыночных механизмов, появляется необходимость более активного участия правительств и иных органов государственной власти в поддержке перехода на IPv6 путем распространения информации об угрозе исчерпания IP-адресов, финансовой поддержки перехода на версию IPv6 и использования IPv6 в правительственных сетях.

Принимая во внимание сложности перехода на IPv6, развивающиеся страны, в основном расположенные в Африке, могут извлечь выгоды от запоздалой информатизации и возможности изначально внедрять сети, основанные на IPv6. В ходе внедрения развивающимся странам потребуется техническая помощь [8].

Политический план действий по переходу на IPv6, помимо проблем собственно перевода на новую версию протокола, должен решать проблемы справедливого распределения IP-адресов, для чего необходимо

внедрение новых конкурентных механизмов, наилучшим образом удовлетворяющих потребности конечных пользователей.

Изменения в интернет-протоколах и кибербезопасность

Безопасность не входила в список важных вопросов для первых разработчиков Интернета, поскольку в то время Интернет состоял из закрытой сети исследовательских институтов. Глобальное распространение Интернета и его возрастающая коммерческая значимость привели к тому, что вопросы безопасности вышли на одно из первых мест в списке проблем управления Интернетом.

Поскольку архитектура Интернета создавалась без учета вопросов кибербезопасности, встраивание в нее соответствующих инструментов потребует существенного изменения самой основы Интернета, протокола TCP/IP. Новый протокол IPv6 предусматривает некоторые усовершенствования с точки зрения безопасности, но все же не является полноценным решением. Обеспечение такой защищенности потребует существенной модификации TCP/IP [9].

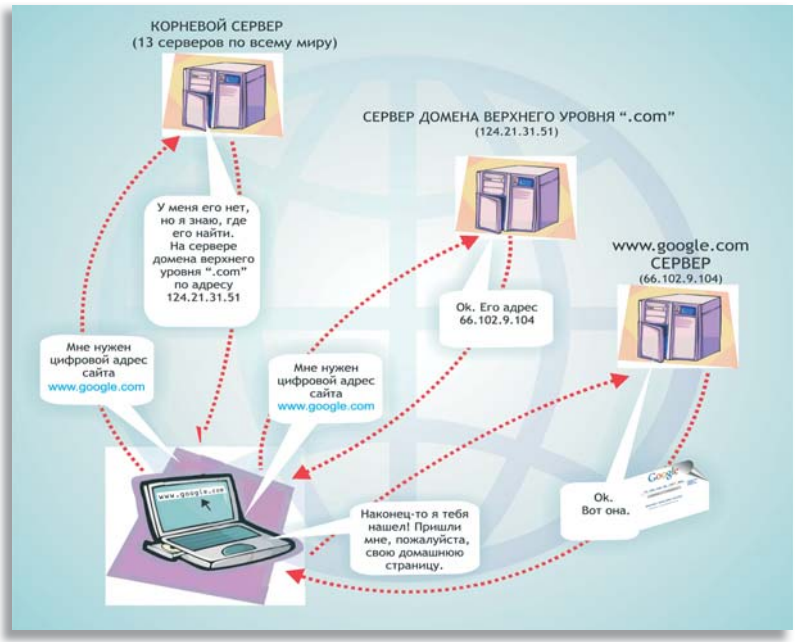
Изменение TCP/IP и проблема ограниченной пропускной способности

Чтобы облегчить передачу по Интернету мультимедийных материалов (например, голосовой связи или «видео по запросу»), необходимо обеспечить качество услуг, гарантирующее определенный минимальный уровень эксплуатационных показателей. Это особенно важно для приложений, где задержка недопустима, например, при передаче репортажа в режиме реального времени. Основной проблемой является недостаточная пропускная способность интернет-каналов. Обеспечение качества услуг может потребовать изменений в интернет-протоколах вплоть до возможного отказа от принципа сетевой нейтральности.

СИСТЕМА ДОМЕННЫХ ИМЕН (DNS)

СОВРЕМЕННОЕ СОСТОЯНИЕ

Система доменных имен (DNS) работает с интернет-адресами (например, www.google.com) и превращает их в IP-адреса (упрощенная схема представлена на рисунке ниже). DNS состоит из «корневых» серверов,



серверов доменов верхнего уровня и множества DNS-серверов, расположенных в разных частях мира. Управление системой доменных имен всегда было предметом жарких споров при обсуждении управления Интернетом. Одним из наиболее противоречивых моментов является контроль правительства США (через Министерство торговли) над корневыми серверами — верхним уровнем иерархически организованной системы доменных имен. Ситуацию усугубляет тот факт, что 10 из 13 существующих корневых серверов расположены в США (остальные 3 расположены в Европе и Азии). Чтобы решить эту проблему и обеспечить масштабируемость системы доменных имен, была разработана технология «Anycast», которая на сегодняшний день включает более ста серверов по всему миру на всех континентах.

DNS включает в себя два типа доменов верхнего уровня. Первый тип — это так называемые родовые (или «общие»); второй — домены, основанные на кодах стран. Список адресов для каждого родового домена верхнего уровня (generic top-level domain, gTLD) поддерживает одна регистратура. Например, домен .com администрируется компанией VeriSign. Функцию «продавцов» берут на себя регистраторы. ICANN (Корпорация по присвоению имен и адресов Интернета) осуществляет общую координацию системы DNS, заключая соглашения

и выдавая аккредитацию регистратурам и регистраторам. Эта организация также назначает оптовую цену, по которой регистратура (например, VeriSign) сдает в аренду регистраторам доменные имена, и устанавливает определенные условия оказания услуг регистратур и регистраторов. Таким образом, ICANN действует как регулирующий орган по экономическим и правовым вопросам на рынке доменных имен верхнего уровня.

Важной частью управления системой доменных имен является защита торговых марок и разрешение споров. На заре Интернета регистрация доменных имен основывалась на принципе «первым пришел — первым обслужили», что в результате породило явление, известное как киберсквоттинг: регистрация доменных имен с целью их последующей перепродажи. Единая политика рассмотрения споров о доменных именах (Uniform Dispute Resolution Policy, UDRP), разработанная ICANN и Всемирной организацией интеллектуальной собственности (ВОИС), помогла существенно сократить киберсквоттинг.

Другой важной составляющей существующей структуры управления DNS является управление национальными доменами верхнего уровня (country code top-level domains, ccTLDs). В настоящй момент многие из них находятся под контролем негосударственных институтов и частных лиц, получивших это право на начальных этапах развития Интернета, когда правительства не интересовались такими вопросами.

ВОПРОСЫ

Создание новых доменных имен

С технической точки зрения, возможности создания новых доменных имен верхнего уровня (gTLDs) практически не ограничены. Однако до сегодняшнего дня внедрение новых доменных зон шло очень медленными темпами; лишь недавно было создано несколько новых gTLD. В настоящее время существует 20 gTLD, обсуждается возможность создания еще трех [10]. Основное сопротивление внедрению новых gTLD оказывают коммерческие компании, обеспокоенные тем, что увеличение числа доменов усложнит проблему защиты торговых марок.

Испытывая давление в вопросе создания новых доменных имен верхнего уровня, ICANN начала процесс консультаций, направленных на разработку новой политики в этой области. Эта политика, помимо прочего, призвана решить проблемы урегулирования споров о доменных именах, общественной морали, а также стоимости регистрации. Новая политика в отношении доменов верхнего уровня должна быть внедрена в 2009 г.

Домены верхнего уровня для особых видов материалов

Еще одна политическая проблема, с которой столкнулась ICANN, — принятие решения о создании новых доменных зон, название которых отражает особенности содержимого размещенных в них сайтов [11]. Последний пример такого рода — предложение о создании домена .xxx для порнографических сайтов, которое Совет директоров ICANN отклонил в марте 2007 г. Критики заявили, что ICANN приняла это решение под давлением со стороны правительства США, категорически воспротивившегося созданию домена .xxx [12]. Интересно отметить, что многие другие правительства поддержали США; в их числе были Китай и Бразилия, как правило, выступающие резко против «особой роли» США в управлении Интернетом.

Возможным положительным результатом создания домена .xxx, по мнению некоторых, было бы создание в Интернете «зоны для взрослых» и ограничение доступа детей к сомнительным материалам. Другие авторы выступали против создания домена .xxx по религиозным и культурным причинам. Решение ICANN относительно домена .xxx возобновило дискуссию о роли ICANN в вопросах государственного управления.

Домены верхнего уровня для культурных и языковых сообществ

В 2003 г. ICANN приняла решение о создании нового домена .cat для материалов на каталанском языке. Впервые домен был создан специально для сайтов на определенном языке [13]. Этот прецедент может привести к новым противоречиям. Во-первых, многие языковые и культурные сообщества во всем мире, вероятно, потребуют такой же привилегии. Во-вторых, в ряде случаев языковые и религиозные сообщества стремятся создать собственное государство, и появление подобного домена может стать причиной противоречий и конфликтов с уже существующими странами. В случае с доменом .cat правительство Испании не выступило против подобного решения.

Управление национальными доменами (ccTLD)

Управление национальными доменами верхнего уровня включает в себя три важных вопроса. Первый касается зачастую противоречивого с политической точки зрения решения о том, какие именно национальные коды должны регистрироваться в случаях, когда международный статус страны или образования неясен или оспаривается (например, для государств, недавно получивших независимость, или движений сопротивления). Одним из недавних спорных вопросов была регистрация доменного имени властями Палестинской автономии. В оправдание своего решения

о присвоении доменного имени .ps IANA вновь заявила о принципе регистрации доменных имен в соответствии со стандартом ISO 3166, как предлагал Джон Постел, один из «отцов-основателей» Интернета [14].

Второй вопрос: кто должен управлять национальными кодами? Многие правительства пытались получить контроль над доменами своих стран, считая их национальным достоянием. При этом государства применяли различные политические подходы [15]. Передача новому институту права управления национальным доменом («переделегирование») одобряется ICANN только в том случае, если внутри страны был достигнут консенсус между всеми заинтересованными сторонами. Вследствие высокой значимости проблемы и разнообразия подходов к ее решению на международном уровне были запущены две инициативы, направленные на достижение определенного уровня гармонизации. Первой такой инициативой стали «Принципы ПКК», одобренные Правительственным консультативным комитетом ICANN[1], который вырабатывает рекомендации и определяет процедуры управления процессом переделегирования права управления национальными доменами верхнего уровня [16]. Второй инициативой стали «Лучшие практики», разработанные Всемирным альянсом доменных имен верхнего уровня в июне 2001 г.

Третий вопрос связан с нежеланием операторов доменов во многих странах становиться частью системы ICANN. До сегодняшнего дня ICANN не удалось собрать операторов национальных доменов «под одной крышей». Некоторые операторы доменов создали организации регионального уровня (CENTR в Европе, AFTLD в Африке, APTLD в Азии, NATLD в Северной Америке, LACTLD в Южной Америке). На глобальном уровне основным форумом является Всемирный альянс операторов доменов верхнего уровня. В настоящее время ICANN ведет работу над созданием «Принципов подотчетности» — менее формального механизма сотрудничества с операторами ccTLD.

Многоязычные доменные имена (IDN)

Интернет изначально создавался для общения на английском языке, однако быстро превратился в глобальное средство коммуникации, причем число неанглоязычных пользователей возрастает. Ограничения инфраструктуры Интернета с точки зрения многоязычия могут оказаться одним из основных факторов, препятствующих развитию глобальной сети в будущем.

[1] Правительственный консультативный комитет — структура ICANN, представляющая интересы государств и обладающая совещательными полномочиями. — *Примеч. перев.*

Техническое сообщество, организованное при IETF, разработало техническое решение для многоязычных доменных имен (Internationalised Domain Names, IDN), которое позволяет использовать в их названиях наряду с латиницей и другие системы письма (например, китайскую, арабскую, кириллицу). В настоящее время ICANN тестирует систему технического обеспечения IDN.

Помимо технических трудностей, еще одной, возможно, более сложной проблемой будет разработка политики и процедур управления системой IDN. Все более активно продвигается идея передачи управления частями такой системы странам или группам стран, жители которых говорят на одном языке. Так, правительство Китая несколько раз указывало, что системой IDN на китайском языке должен управлять Китай. С аналогичным предложением в отношении кириллических доменов выступила Россия. Разработка и реализация политики управления системой IDN послужит одной из важнейших проверок на прочность действующего режима управления Интернетом.

«КОРНЕВЫЕ» СЕРВЕРЫ

«Корневые» серверы, находящиеся на самой вершине иерархической структуры системы доменных имен, привлекают к себе большое внимание и являются предметом обсуждения в большинстве политических и научных дебатов по вопросам управления Интернетом.

СОВРЕМЕННОЕ СОСТОЯНИЕ

Чтобы проанализировать функции и надежность системы DNS, рассмотрим беспокоящую многих ситуацию, при которой корневые серверы будут отключены и Интернет перестанет функционировать. Во-первых, существует 13 корневых серверов — максимально технически возможное количество, — которые распределены по всему миру (10 — в США, 3 — в других странах; из 10 серверов в США некоторые находятся в ведении правительственных ведомств). Если один из серверов выйдет из строя, функционирование остальных не нарушится. Даже если все 13 серверов выйдут из строя одновременно, поиск доменных имен (основная функция корневых серверов) продолжится на других серверах доменных имен, иерархически распределенных по Интернету [17].

Иными словами, копии файлов корневой зоны хранятся на тысячах серверов доменных имен, и немедленный и катастрофический коллапс

Интернета невозможен. Какие-либо серьезные последствия с точки зрения функционирования будут заметны только по прошествии определенного времени, за которое можно будет восстановить поврежденные серверы или создать новые.

К тому же систему корневых серверов существенно укрепляет технология «Anycast», копирующая содержимое этих серверов по всему миру. Такая структура дает много преимуществ, включая повышенную надежность системы DNS и более быстрое получение информации об интернет-адресах (благодаря схеме «Anycast» выбирается ближайший к конечному пользователю сервер).

13 корневых серверов находятся под управлением разнообразных организаций: научных и общественных институтов, коммерческих компаний, правительственных ведомств. Организации, управляющие корневыми серверами, получают файл корневой зоны, подготовленный Администрацией по присвоенным именам в Интернете (IANA) и одобренный правительством США (Министерством торговли). После получения согласия от Министерства торговли содержимое файла копируется на основной корневой сервер, находящийся под управлением компании VeriSign по контракту с Министерством торговли.

Файл основного корневого сервера затем автоматически копируется на все остальные корневые серверы. Таким образом, правительство США потенциально может в одностороннем порядке вносить изменения в систему DNS, что вызывает озабоченность многих государств.

ВОПРОСЫ

Интернационализация контроля над корневыми серверами

Многие страны выражают озабоченность существующей на данный момент схемой, в которой окончательные решения о содержимом корневых серверов принимаются только одним государством (США). В ходе переговоров по вопросам управления Интернетом были выдвинуты различные предложения, в том числе идея заключить «Соглашение о корневых серверах» (Root Convention), которое бы передало политический контроль над этими серверами международному сообществу или, по крайней мере, дало бы государствам право распоряжаться своими национальными доменами. Новые перспективы открывает подписание «Подтверждения обязательств» (Affirmation of Commitments) [18], которое призвано создать условия для обеспечения институциональной независимости ICANN от Министерства торговли США и будущей интернационализации ICANN. Соглашение с IANA будет пересмотрено в

2011 г. Можно выделить несколько элементов возможного переходного состояния, которое будет включать в себя два этапа:

- инициированная «Подтверждением обязательств» реформа ICANN, результатом которой станет создание уникальной в своем роде международной организации, приемлемой для всех государств институциональной формы управления Интернетом;
- передача контроля над корневыми серверами от Министерства торговли США к ICANN, как и предполагалось изначально.

Альтернативные корневые серверы — возможности и ограничения

Создание альтернативного корневого сервера не является технически сложной задачей. Основной вопрос заключается в том, сколько «последователей» будет у альтернативного сервера, или, точнее, сколько компьютеров в Интернете будет обращаться к нему с запросами. Без пользователей альтернативная DNS теряет смысл. Попытки создать альтернативную систему DNS предпринимались неоднократно (Open NIC, New.net и Name.space), но большинство из них были неудачными и привлекли лишь несколько процентов пользователей Интернета.

Роль США в управлении корневыми серверами — парадокс влияния

После принятия документа «Подтверждение обязательств» парадокс влияния США в отношении корневых серверов, возможно, станет историей. Суть парадокса в том, что потенциальная возможность стереть любое государство с «политической карты Интернета» (удалив домен верхнего уровня этой страны) едва ли может считаться влиянием, так как у нее нет практического применения. Важнейший элемент влияния — возможность заставить другую сторону действовать в соответствии с волей того, кто таким влиянием обладает. Использование США своего «влияния» на инфраструктуру Интернета может повлечь за собой нежелательные последствия, включая создание странами и даже регионами своих альтернативных проектов Интернета. При таком развитии событий Интернет может распасться на несколько несвязанных частей, что поставит под угрозу интересы США (преобладание американских ценностей и статус английского языка как языка международного общения в Интернете, доминирующее положение американских компаний в сфере электронной коммерции). На основании первых инициатив администрации Б. Обамы (например, принятие «Подтверждения обязательств») можно сделать вывод, что США осознает всю парадоксальность своей власти; с точки зрения будущего развития глобального режима управления Интернетом, это важный сигнал.

ПОСТАВЩИКИ ИНТЕРНЕТ-УСЛУГ

Поставщики интернет-услуг (провайдеры) подключают конечных пользователей к Интернету. Поэтому, с точки зрения многих правительств, они являются самым простым и очевидным механизмом обеспечения соблюдения правовых норм в Интернете. По мере возрастания коммерческой значимости Интернета и актуализации вопросов кибербезопасности многие государства начинают использовать провайдеров как инструмент правоприменения.

ВОПРОСЫ

Телекоммуникационные монополии и поставщики интернет-услуг

В странах, где существуют телекоммуникационные монополии, типичной является ситуация, когда они же предоставляют и доступ в Интернет. Монополии препятствуют выходу провайдеров на рынок и не дают развиваться конкуренции. В результате устанавливаются завышенные цены, качество услуг остается низким, а проблема разрыва в цифровых технологиях не решается. В некоторых случаях телекоммуникационные монополии терпят существование других интернет-провайдеров, но прямо вмешиваются в их деятельность (например, ограничивая пропускную способность или создавая помехи для оказания услуг).

Ответственность интернет-провайдеров с точки зрения авторских прав

Большинство правовых систем признает, что провайдер не может нести ответственности за использование предоставляемых им услуг для размещения нарушающих авторское право материалов, если не знает об этом. Основное отличие заключается в том, какие юридические действия предпринимаются после того, как провайдер проинформирован о нарушении авторских прав, связанном с размещенным на его сервере материалом.

Законы США и ЕС предусматривают процедуру «предупреждение — удаление», в соответствии с которой провайдер должен удалить материал, чтобы избежать судебного преследования. Японское законодательство предполагает более сбалансированный подход (процедура «предупреждение — предупреждение — удаление»), который предоставляет ис-

пользующему материал лицу право обжаловать требование об удалении материала с сайта.

Подход, ограничивающий ответственность провайдеров, в целом поддерживается судебной практикой. Вот некоторые наиболее значимые судебные прецеденты, в которых с провайдеров была снята ответственность за размещение материалов, нарушающих права интеллектуальной собственности: дело саентологов (Нидерланды), дело «RIAA против Verizon» (США), «SOCAN против CAIP» (Канада) и «Sabam против Tiscali» (Бельгия) [19].

Роль интернет-провайдеров в контроле над содержанием материалов Интернета

Под давлением общественного мнения интернет-провайдеры постепенно, хоть и неохотно, вовлекаются в регулирование материалов Интернета. При этом у них есть два варианта поведения. Первый — обеспечивать следование нормам, выработанным органами власти. Второй, основанный на саморегулировании — самим определять, какие материалы подходят для размещения. Этот вариант связан с риском «приватизации» политики в отношении содержания интернет-ресурсов, когда провайдеры будут брать на себя функции правительства.

Роль интернет-провайдеров в политике противодействия спаму

Поставщики интернет-услуг часто рассматриваются как основные участники инициатив по противодействию спаму. Обычно интернет-провайдеры сами проводят мероприятия, направленные на снижение объемов рассылки нежелательной почты, используя технические средства фильтрации данных или принимая стратегии противодействия спаму. В отчете МСЭ по вопросам спама отмечается, что ответственность за распространение спама должна быть возложена на интернет-провайдеров, и предлагается принять «Кодекс поведения по противодействию спаму», который включал бы два основных положения: а) интернет-провайдеры должны запретить пользователям рассылку спама, б) интернет-провайдеры не должны обмениваться данными с другими провайдерами, не принявшими сходный кодекс поведения [20].

Проблема спама создает новые сложности для провайдеров. Например, фильтрация материалов компанией Verizon с целью предотвратить спам вылилась в судебный процесс. Наряду со спамом фильтры Verizon блокировали и допустимые сообщения. Это создавало неудобства для пользователей, которые не получали часть писем от законопослушных отправителей и в итоге подали на Verizon в суд [21].

ОПТОВЫЕ ПРОВАЙДЕРЫ УСЛУГ ШИРОКОПОЛОСНОЙ СВЯЗИ

Архитектура доступа в Интернет состоит из трех уровней. Провайдеры интернет-услуг, подключающие конечных пользователей, составляют уровень 3. Уровни 1 и 2 состоят из оптовых поставщиков услуг широкополосной связи. Передача данных на уровне 1 осуществляется крупнейшими провайдерами услуг широкополосной связи. Они, как правило, заключают так называемые пиринговые соглашения об обмене данными с другими компаниями, работающими на том же уровне [22]. Основное различие между провайдерами, работающими на уровне 1 и уровне 2, заключается в том, что первые обмениваются трафиком друг с другом бесплатно, по принципу пиринга («равный с равным»), в то время как вторые вынуждены оплачивать передачу данных на уровень 1 соответствующим провайдерам [23].

Уровень 1 обычно контролируется крупными компаниями — такими как MCI, AT&T, Cable Wireless и France Telecom. В области широкополосных каналов связи традиционные телекоммуникационные компании распространили свое присутствие на глобальных рынках и на интернет-магистрали.

ВОПРОСЫ

Должна ли интернет-инфраструктура быть услугой общего пользования?

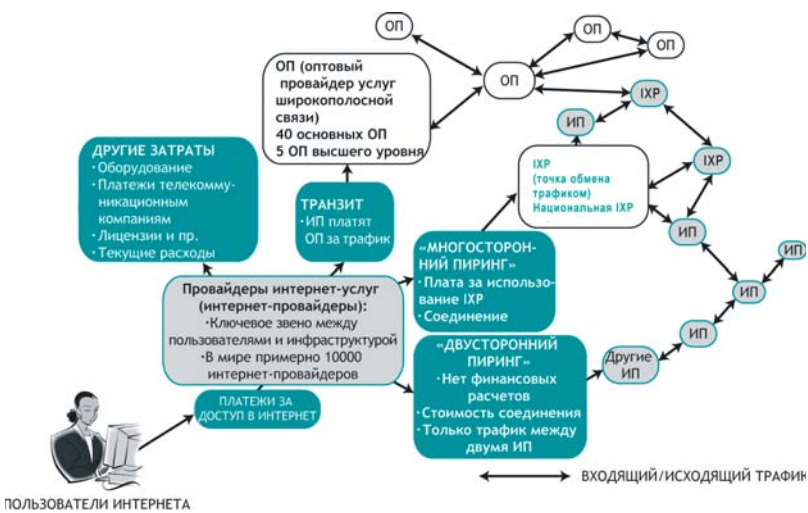
Интернет-трафик может передаваться по любому каналу связи. Однако на практике определенные мощности, например, магистрали уровня 1 (как правило, использующие оптоволоконные кабели или спутниковые каналы), особенно важны для функционирования Интернета. Их центральное положение в структуре Интернета дает их владельцам возможность устанавливать цены и диктовать условия на предоставление своих услуг. В конечном счете, само функционирование Интернета зависит от решений, принимаемых владельцами магистральных каналов передачи данных. Имеет ли глобальное сообщество пользователей Интернета право требовать от крупнейших телекоммуникационных операторов гарантий надежного функционирования критической инфраструктуры Интернета? Управляют ли эти компании объектами общего пользования?

Провайдеры услуг широкополосной связи и критическая инфраструктура

В начале 2008 г. в Средиземном море, недалеко от Египта был поврежден один из основных кабелей, передающих интернет-трафик. Этот инцидент поставил под угрозу доступ к Интернету в обширном регионе, достигающем границ Индии. Два схожих инцидента произошли в 2007 г. (кабель рядом с Тайванем и основной кабель, передающий трафик в Пакистан). Подобные события со всей ясностью демонстрируют, что инфраструктура Интернета — часть национальной и глобальной критической инфраструктуры. Сбои в предоставлении интернет-услуг могут негативно сказаться на экономике и общественной жизни региона. Возможность нарушения работы Интернета ставит несколько вопросов. Надежно ли защищены основные кабели, передающие интернет-трафик? Какова роль правительств государств, международных организаций и частных компаний в защите кабелей? Как мы можем снизить риски, связанные с возможным повреждением основных кабелей Интернета?

Либерализация телекоммуникаций и роль поставщиков телекоммуникационных услуг

Существуют противоположные точки зрения на то, в какой степени провайдеры интернет-услуг и телекоммуникационные компании должны подпадать под действие правил ВТО. Развитые страны доказывают, что либеральные правила, предоставленные ВТО телекоммуникационным



операторам, могут быть распространены и на интернет-провайдеров. Сторонники ограничительной трактовки указывают, что режим ВТО применим только к рынку телекоммуникаций. Регулирование рынка интернет-провайдеров требует выработки новых правил в рамках ВТО.

ЭКОНОМИЧЕСКИЕ МОДЕЛИ ОБЕСПЕЧЕНИЯ ПОДКЛЮЧЕНИЯ К ИНТЕРНЕТУ

Мы знаем, как регулировать передачу пакетов, но совершенно не знаем, как регулировать передачу долларов.
Дэвид Кларк

СОВРЕМЕННОЕ СОСТОЯНИЕ

Зачастую обсуждение вопросов управления Интернетом упирается в проблему распределения средств и источников дохода [24]. Кто платит за Интернет? Между различными сторонами, вовлеченными в процесс функционирования Интернета, происходит множество финансовых операций. Индивидуальные пользователи и компании платят интернет-провайдерам за доступ в Интернет и предоставляемые услуги. Но каким образом эти деньги распределяются по различным сетям, предоставляющим услуги доступа в Интернет, или, иными словами, «как деньги перемещаются по Интернету?» [25]. Вот некоторые затраты, которые вынуждены покрывать интернет-провайдеры (см. рисунок на предыдущей странице):

- интернет-провайдеры платят за услуги операторов связи и за канал доступа в Интернет;
- интернет-провайдеры платят региональным или местным интернет-регистратурам, от которых они получают IP-адреса для дальнейшего распределения;
- интернет-провайдеры платят поставщикам за оборудование, программное обеспечение и обслуживание (включая инструменты диагностики и персонал, необходимый для функционирования линий связи, центров помощи и административных служб);
- организации, регистрирующие доменные имена, платят за услуги не только регистратору, но и IANA;
- операторы связи платят производителям кабелей и спутников, а также компаниям, предоставляющим телекоммуникационные услуги. Поскольку эти операторы часто берут средства в кредит, они выплачивают проценты различным банкам и консорциумам.

Этот список можно продолжить, но общий вывод ясен: «бесплатных обедов» не бывает. В результате, все затраты указанной цепочки оплачиваются из кармана конечных пользователей Интернета, будь то индивиды или организации.

ВОПРОСЫ

Нуждается ли экономика доступа к Интернету в реформе?

Текущая экономическая политика и порядок взаимодействия в Интернете сложились еще на заре Интернета и прошли в своем развитии несколько этапов. Современную практику экономического взаимодействия в Интернете можно считать эффективной, поскольку в большинстве случаев она обеспечивает устойчивое функционирование Интернета по доступной цене. Основная критика текущей экономической политики связана с двумя аспектами:

- не исключается возможность монополизации сферы доступа к Интернету основными игроками и, следовательно, нарушения принципов функционирования свободного рынка;
- доходы и издержки несправедливо распределяются между участниками экономики Интернета.

В академических кругах предпринималось бессчетное число попыток разработать справедливую экономическую модель доступа к Интернету. Нгуен и Армитраж отмечают, что в Интернете необходимо найти оптимальный баланс между тремя элементами: технической эффективностью, экономической эффективностью и общественными интересами [26]. Другие авторы указывают на сложности, которые создаст переход от существующей простой, одинаковой для всех структуры ценообразования к более сложной, зависящей от объема переданного трафика. Что касается практических результатов изменений, многие полагают, что изменение текущей экономической политики в Интернете может открыть «ящик Пандоры».

Недопущение образования монополий на рынке ресурсов Интернета

Возможно, благодаря поглощениям несколько монополий смогут контролировать весь рынок интернет-трафика [27]. Подобная проблема существует как в развитых, так и в развивающихся странах. Некоторые авторы надеются, что процесс либерализации телекоммуникационного рынка решит проблему монополий (особенно в отношении действующих операторов). Однако либерализация может привести к замещению общественной монополии частной. Джефф Хастон утверждает, что установ-

ление монополии и утрата разнообразия на рынке ресурсов Интернета неизбежно отразятся на цене и качестве услуг Интернета [28].

Кто должен покрывать затраты на связь между развивающимися и развитыми странами?

«Когда пользователь из Кении отправляет электронное сообщение получателю в США, кенийский интернет-провайдер оплачивает международное соединение между США и Кенией. Но когда американский пользователь отправляет электронное сообщение в Кению, кенийский провайдер все так же оплачивает международное соединение; в конечном итоге, кенийскому пользователю приходится оплачивать более высокую стоимость доступа» [29].

На сегодняшний день за передачу данных между развитыми и развивающимися странами платят последние [30]. По сравнению с системой традиционной телефонии, где стоимость каждого международного звонка делится между двумя странами, принятая в Интернете модель возлагает все бремя на одну сторону — развивающиеся страны, которые должны подключаться к магистралям, расположенным преимущественно в развитых странах. Таким образом, небольшие и бедные страны субсидируют Интернет в развитых странах.

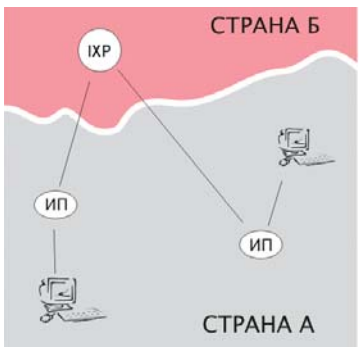
Основной довод в спорах об изменении существующей системы оплаты услуг Интернета основан на аналогии с оплатой услуг телефонии, где стоимость делится поровну между конечными точками коммуникации. Однако Джефф Хастон указывает, что эта аналогия не имеет под собой оснований. В системе традиционной телефонии существует лишь одна оплачиваемая услуга, а именно телефонный звонок, делающий возможным общение между людьми, находящимися возле своих телефонных аппаратов [31]. В Интернете нельзя выделить единственную «оплачиваемую услугу»; в нем есть только пакеты данных, передаваемые по различным маршрутам внутри сети. Это фундаментальное различие делает вышеуказанную аналогию неприменимой и является основным источником проблем при попытках применить модель оплаты телефонных услуг к Интернету.

По инициативе МСЭ были начаты переговоры о возможном усовершенствовании существующей системы покрытия затрат на Интернет, цель которых — более сбалансированное распределение стоимости доступа в Интернет. В результате противодействия со стороны развитых стран и телекоммуникационных операторов принятая МСЭ Резолюция № D.50 практически не имела последствий [32]. Попытки обсудить эту проблему в рамках ВТО также окончились неудачей. Вопрос о необходимости усовершенствования схемы платы за подключение к Интернету был вновь поднят в ходе WSIS и нашел отражение в итоговых документах встречи и отчете WGIG.

Сокращение стоимости доступа за счет использования точек обмена интернет-трафиком

Точки обмена интернет-трафиком (Internet Exchange Points, IXP) — это технические комплексы, с помощью которых провайдеры обмениваются интернет-трафиком на основе пиринга (бесплатно). Обычно такие точки создаются для обмена трафиком внутри ограниченной группы пользователей (например, внутри города, региона, страны), чтобы избежать ненужной маршрутизации данных через географически удаленные точки [33].

Интернет-трафик без национальной IXP



Интернет-трафик при наличии национальной IXP

ИП — интернет-провайдер

Точки обмена интернет-трафиком также могут сыграть важную роль в сокращении разрыва в цифровых технологиях [34]. Например, если в стране нет национальной точки обмена, необходимо направлять существенную долю интернет-трафика между пользователями через другую страну. Это увеличивает объем международной передачи данных на дальние расстояния и стоимость предоставления услуг Интернета. Создание национальных и региональных точек обмена трафиком может снизить стоимость доступа к Интернету для развивающихся стран.

СТАНДАРТЫ «ВСЕМИРНОЙ ПАУТИНЫ» (WWW)

К концу 1980-х гг. «битва» за сетевые стандарты завершилась. TCP/IP постепенно стал основным сетевым протоколом, оттеснив другие: поддерживавшийся МСЭ протокол X-25 (часть архитектуры Взаимодействия

открытых систем) и многие проприетарные стандарты, такие как разработанный IBM стандарт SNA. Хотя Интернет и облегчил коммуникацию между разнообразными сетями за счет использования TCP/IP, в системе еще не было общих стандартов приложений.

Решение было разработано Тимом Бернерсом-Ли и его коллегами в лаборатории CERN в Женеве и представляло собой новый стандарт обмена информацией по Интернету, названный HTML (по сути, упрощение существовавшего стандарта ISO, называвшегося SGML). Появление HTML как основы «всемирной паутины» стало началом стремительного роста Интернета.

С момента появления первой версии HTML этот стандарт постоянно обновлялся и наполнялся новыми возможностями. Растущая значимость Интернета для разных сфер человеческой деятельности поставила вопрос о стандартизации HTML. Он приобрел особую актуальность во время так называемых браузерных войн между Netscape и Microsoft, когда каждая из компаний старалась усилить свое положение на рынке, влияя на стандарты HTML. Изначально HTML позволял работать только с текстом и изображениями, однако новые интернет-приложения требовали более сложных технологий для управления базами данных, работы с видео и анимацией. Такое разнообразие приложений требовало существенных усилий по стандартизации, чтобы гарантировать адекватное отображение любого размещенного в Интернете материала большинством браузеров.

Стандартизация приложений вступила в новую фазу с появлением языка XML, предоставившего большую гибкость в установлении стандартов для содержимого интернет-страниц. Появились и новые группы XML-стандартов. Например, стандарт для распространения материалов по беспроводной связи называется Wireless Mark-up Language (WML). Стандартизация приложений осуществляется преимущественно в рамках Консорциума «всемирной паутины» (W3C), возглавляемого Тимом Бернерсом-Ли. Интересно отметить, что, несмотря на свою большую важность для Интернета, W3C пока не привлек к себе достаточного внимания в дискуссиях по управлению Интернетом.

«ОБЛАЧНАЯ ОБРАБОТКА ДАННЫХ»

Выражение «облачная обработка данных» («облачные вычисления») используется для описания новой тенденции в компьютерной индустрии, заключающейся в предоставлении компьютерных приложений как интернет-услуг за счет использования огромных «серверных ферм». Первые примеры облачной обработки данных — онлайновые сервисы электронной почты (Gmail, Yahoo, Hotmail), а также онлайн-инструменты

обработки текстов (wiki, службы Google). Распространение приложений для социальных сетей, таких как Facebook и блоги, ускорило развитие «облачных вычислений». Все больше цифровых ресурсов перемещается с наших жестких дисков на «облачные» серверы. Основные игроки на рынке «облачной обработки данных» — Google, Microsoft, Apple, Amazon и Facebook, которые владеют большими «серверными фермами».

Историки, изучающие развитие технологий, могут обратить внимание на то, что с развитием «облачной обработки данных» круг замкнулся. На начальных этапах развития компьютеров, использовались мощные ЭВМ общего пользования («мейнфреймы») и пользовательские терминалы, не обладающие самостоятельными вычислительными возможностями. Основной «интеллект» был сосредоточен на центральном компьютере. Затем благодаря развитию персональных компьютеров и приложений Windows вычислительные мощности были перенесены на конечные точки сети. Замкнется ли цикл в результате появления «облачной обработки данных»? Появятся ли в будущем несколько крупных центральных компьютеров/«серверных ферм» и миллиарды «неинтеллектуальных» устройств в виде ноутбуков, мониторов и мобильных телефонов? Ответ на этот и другие вопросы потребует времени. Сейчас мы можем лишь назвать несколько проблем управления Интернетом, которые, скорее всего, возникнут в результате развития «облачной обработки данных».

Во-первых, по мере того, как все большее количество услуг будет доступно в режиме онлайн, зависимость современного общества от Интернета возрастет. В прошлом без подключения к Интернету мы не могли отправить электронное письмо или просмотреть информацию. В эпоху «облачной обработки данных» без Интернета недоступным может стать даже написание текста или проведение вычислений. Эта возросшая зависимость от Интернета усилит потребность в обеспечении его стабильности и надежности. Она неизбежно приведет к формированию более мощного режима управления Интернетом, в котором более активную роль будут играть государства.

Во-вторых, с увеличением количества персональных данных, хранящихся в «облаках», на первый план выйдут вопросы конфиденциальности и защиты данных. Будем ли мы контролировать наши текстовые файлы, электронную почту и другие данные? Смогут ли операторы использовать их без нашего разрешения? Кто будет получать доступ к нашим данным?

В третьих, по мере оцифровки постоянно возрастающего объема данных о гражданах, государства будет все больше беспокоить то, что их ресурсы находятся за пределами «национальных границ». Возможно, они попытаются создать национальные или региональные «облака», либо обеспечить

определенный уровень межгосударственного контроля над существующими «облаками». Тенденция к национализации «облаков» может усилиться также потому, что основные операторы в данной области базируются в США. Некоторые утверждают, что текущие споры вокруг ICANN могут уступить место спорам о регулировании «облачной обработки данных».

В-четвертых, поскольку услуги «облачной обработки данных» предоставляются различными операторами, возрастает значимость вопросов стандартизации. Принятие общих стандартов обеспечит беспрепятственную передачу данных между различными «облаками» (например, между Google и Apple). Обсуждается возможность принятия открытых стандартов основными игроками на рынке «облачной обработки данных».

Когда речь заходит об этой сфере, вопросов гораздо больше, чем ответов. Ее регулирование, вероятно, будет результатом взаимодействия различных участников. Например, Европейский Союз озабочен вопросами конфиденциальности и защиты данных. Соглашение о «безопасной гавани» (Safe Harbour), разработанное с целью согласовать различные режимы защиты персональной информации в США и ЕС, оказалось неэффективным. По мере того, как все большее количество цифровых данных пересекает Атлантический океан, ЕС и США будут вынуждены решать вопросы обеспечения конфиденциальности на основании принятия стандартов ЕС американскими компаниями — основными операторами в сфере «облачной обработки данных». В области стандартизации крупные компании, скорее всего, будут договариваться между собой. Google уже начал мощную кампанию по лоббированию открытых стандартов, создав «Фронт освобождения данных», задачей которого является обеспечение бесперебойной передачи данных между различными «облаками». Это только первые кирпичики в фундаменте системы регулирования «облачной обработки данных» в Интернете. Вероятно, будут появляться и иные решения конкретных политических проблем.

КОНВЕРГЕНЦИЯ: ИНТЕРНЕТ — ТЕЛЕКОММУНИКАЦИИ — МУЛЬТИМЕДИА

Широкое и все возрастающее использование интернет-протоколов привело к сближению (конвергенции) телекоммуникаций, теле- и радиовещания, а также систем передачи информации. Сегодня с помощью Интернета можно делать телефонные звонки, слушать радио, смотреть

телепрограммы и обмениваться музыкой. Всего несколько лет назад эти задачи выполнялись различными системами.

В сфере традиционных коммуникаций основным направлением конвергенции является интернет-телефония (VoIP). Растущая популярность программ интернет-телефонии, таких как Skype, основывается на низкой стоимости, возможности объединить линии голосового общения и передачи данных, а также использовать разнообразные компьютерные инструменты. Благодаря YouTube и аналогичным сетям Интернет также объединяется с традиционными медийными и развлекательными услугами. В то время как с технической точки зрения процесс сближения идет стремительно, его экономические и правовые последствия проявятся лишь через некоторое время.

ВОПРОСЫ

Экономические последствия конвергенции

С экономической точки зрения, конвергенция технологий начала перекраивать традиционные рынки, сделав компании, ранее действовавшие в разных областях, прямыми конкурентами. В этих условиях компании используют различные стратегии, наиболее распространенными из которых являются слияния и поглощения. Например, слияние компаний America Online (AOL) и Time Warner ставило своей целью объединение телекоммуникационных услуг с медийными/развлекательными услугами. В настоящее время AOL/Time Warner объединяет интернет-провайдеров, телевидение, музыку и разработку программного обеспечения под крышей единой компании.

Необходимость правовых рамок

Правовая система наиболее медленно адаптируется к переменам, связанным с сближением технологий. Каждый из сегментов — телекоммуникации, теле- и радиовещание, ИКТ — имеет собственную нормативную базу. Сближение этих областей порождает несколько вопросов, относящихся к управлению и регулированию: что произойдет с существующими национальными и международными режимами в таких областях, как телефонная связь или телерадиовещание? Будут ли разрабатываться новые режимы, связанные преимущественно с Интернетом? Должно ли регулирование процесса конвергенции осуществляться органами власти (правительствами государств и международными организациями) или же методами саморегулирования?

Некоторые страны, например, Малайзия и Швейцария, а также Европейский Союз, уже начали предлагать собственные ответы на эти вопросы.

В Малайзии в 1998 г. был принят Акт о коммуникациях и мультимедиа, заложивший общие рамки для регулирования процесса конвергенции. Новые рамочные директивы ЕС, сегодня преобразуемые в национальное законодательство, также являются шагом в этом направлении, как и законы и правила в области телекоммуникаций, существующие в Швейцарии.

Опасность конвергенции: слияние операторов кабельных сетей и интернет-провайдеров

Во многих странах широкополосный доступ в Интернет осуществляется через кабельные сети. Наиболее активно это происходит в США, где кабельный Интернет гораздо более распространен, чем ADSL, второй возможный вариант широкополосного Интернета. Какие риски связаны с таким объединением функций?

Некоторые участники дискуссий утверждают, что положение операторов кабельных сетей как «буфера» между пользователями и Интернетом может представлять угрозу для принципа сетевой нейтральности.

Основное отличие между традиционным доступом в Интернет по технологии ADSL и использованием для этого кабельных сетей заключается в том, что «кабель» не подпадает под действие правил для так называемых общедоступных линий связи. Эти правила, применяемые к системе телефонной связи, запрещают какую-либо дискриминацию в предоставлении доступа. Деятельность операторов кабельных сетей не регулируется этими нормами, что дает им полный контроль над доступом их клиентов в Интернет. Они могут заблокировать использование определенных приложений или регулировать доступ к определенным материалам. Возможности слежки за пользователями и, как следствие, нарушение их права на тайну частной жизни также существенно выше в системе кабельного Интернета, поскольку доступ контролируется с помощью системы, схожей с локальными сетями.

В докладе на эту тему, опубликованном Американским союзом за гражданские свободы, приводится следующий пример рисков, связанных с монополизацией кабельного Интернета: «Это как если бы телефонной компании разрешили также владеть ресторанами и предоставлять клиентам, звонящим в ресторан “Domino’s”, качественные услуги и четкий сигнал, а тем, кто звонит в “Pizza Hut”, — постоянные сигналы “занято”, обрывы связи и помехи».

Данная проблема может быть решена, когда будет выработано четкое определение, чем является кабельный Интернет — «информационной услугой» или «телекоммуникационной услугой». Если будет выбран второй вариант, кабельный Интернет будет регулироваться правилами для общедоступных линий связи.

КИБЕРБЕЗОПАСНОСТЬ

СОВРЕМЕННОЕ СОСТОЯНИЕ

Интернет был изначально создан для использования ограниченным кругом лиц, поэтому вопросам безопасности, если они вообще принимались во внимание, не придавалось особого значения. Члены академического сообщества, они же основные пользователи Интернета, разработали влиятельные, но неформальные правила с целью обеспечить безопасность Интернета.

Вопросы кибербезопасности приобрели актуальность в связи с резким ростом числа пользователей Интернета. Интернет подтвердил опасения, давно существовавшие у многих: технология может одновременно предоставлять новые возможности и порождать угрозы. То, что может использоваться для блага общества, может также применяться и ему во вред.

Побочным последствием стремительного внедрения Интернета почти во все сферы человеческой деятельности является повышение уязвимости современного общества. Интернет стал частью глобальной критической инфраструктуры, наряду с такими ее составляющими, как электрические сети, транспортные системы и системы здравоохранения. Поскольку атака на эти системы может вызывать серьезное нарушение их функционирования и повлечь серьезные финансовые последствия, критически важные элементы инфраструктуры достаточно часто оказываются объектом нападения.

Вопросы кибербезопасности можно классифицировать по трем критериям: тип действий, тип злоумышленника и тип цели. Классификация, основанная на типе действий, может включать: перехват данных, нарушение целостности данных, нелегальный доступ, внедрение шпионского программного обеспечения, изменение данных, информационную диверсию, нарушение нормального предоставления услуг (DoS-атаки) и кражу личности. Типы возможных злоумышленников: хакеры, киберпреступники, кибервоины и кибертеррористы. Потенциальные цели весьма многочисленны: от индивидов, частных компаний и государственных учреждений до критической инфраструктуры, правительств и военных объектов.

ПОЛИТИЧЕСКИЕ ИНИЦИАТИВЫ В СФЕРЕ КИБЕРБЕЗОПАСНОСТИ

Вопросам кибербезопасности посвящено множество национальных, региональных и глобальных инициатив. На национальном уровне возрастает количество законодательных актов и судебных дел в области кибербезопасности. Наиболее известны инициативы США, связанные с расширением полномочий государства по борьбе с терроризмом. Основным ведомством, занимающимся вопросами безопасности Интернета, является Министерство внутренней безопасности США. Сложно найти развитую страну, где не выдвигались бы какие-либо инициативы, связанные с кибербезопасностью.

На международном уровне наиболее активной организацией является МСЭ, разработавший большое количество рамочных документов, архитектур и стандартов безопасности, включая X.509. Этот стандарт является основой инфраструктуры «открытого ключа» (PKI), используемой, например, в защищенной версии протокола HTTP (HTTPS). Не так давно МСЭ вышел за рамки исключительно технологических аспектов и запустил инициативу «Глобальная повестка дня МСЭ в области кибербезопасности» [35]. Данная инициатива предусматривает юридические меры, политическое сотрудничество и помощь развивающимся странам.

«Большая восьмерка» также выступила с несколькими инициативами в области кибербезопасности, направленными на совершенствование механизмов сотрудничества между правоохранительными органами. Эта организация создала Подгруппу по преступлениям в сфере высоких технологий для установления постоянной (24 часа в сутки и 7 дней в неделю) коммуникации между центрами кибербезопасности государств-участников, подготовки персонала и усовершенствования правовых систем государств. Подгруппа призвана противостоять киберпреступности и способствовать развитию сотрудничества между индустрией ИКТ и правоохранительными органами.

Генеральная Ассамблея ООН за последние несколько лет приняла ряд резолюций по «достижениям в сфере информатизации и телекоммуникации в контексте международной безопасности», в частности, резолюции 53/70 (1998), 54/49 (1999), 55/28 (2000), 56/19 (2001), 57/239 (2002) и 58/199 (2003). С 1998 г. все последующие резолюции имеют сходное содержание без каких-либо существенных улучшений. Они не отражают значительных перемен, произошедших в области кибербезопасности с 1998 г.

Важным международным правовым инструментом, связанным с безопасностью Интернета, является Конвенция Совета Европы по киберпреступности, вступившая в силу 1 июля 2004 г. [36] Некоторые страны заключили также двусторонние соглашения. США имеют двусторонние

соглашения о правовом сотрудничестве по вопросам уголовных преступлений с более чем 20 странами [37]. Эти соглашения также применимы в отношении киберпреступлений.

Одной из попыток выработать международное соглашение в данной области силами исследователей и неправительственных организаций является Стэндфордская предварительная конвенция о защите от киберпреступлений и кибертерроризма. Этот документ рекомендует создать международный орган — Агентство по защите информационной инфраструктуры.

ВОПРОСЫ

Влияние архитектуры Интернета на кибербезопасность

На безопасность Интернета влияют особенности его структуры. Должны ли мы продолжать придерживаться текущего подхода, пытаясь «надстроить» безопасность поверх существующего небезопасного фундамента, или стоит что-то изменить в самих основах инфраструктуры Интернета? Как скажутся такие изменения на других чертах Интернета, в частности, на его открытости и прозрачности? Большинство прежних инициатив по разработке стандартов Интернета преследовало цель улучшения производительности или внедрения новых приложений. Безопасность не была приоритетом.

Нельзя предсказать, сможет ли IETF изменить стандарты электронной почты, чтобы гарантировать удостоверение подлинности (аутентификацию) и в итоге сократить ненадлежащее использование Интернета (например, спам, киберпреступность). Учитывая противоречия, связанные с любым изменением основных стандартов Интернета, вероятнее всего, усовершенствования базового интернет-протокола в области безопасности будут постепенными и медленными.

Дальнейшее развитие электронной коммерции требует высокого уровня кибербезопасности

Кибербезопасность часто упоминают в числе предварительных условий для быстрого развития электронной коммерции. Пока Интернет не станет защищенным и надежным, клиенты будут неохотно предоставлять через него конфиденциальную информацию (к примеру, номера кредитных карт). То же относится к банковским услугам в Интернете и использованию электронных денег. Если общий уровень кибербезопасности будет повышаться медленно (например, по причине отсутствия стандартов), вероятно, бизнес-структуры будут способствовать ускоренному развитию кибербезопасности. В этих условиях могут возникнуть

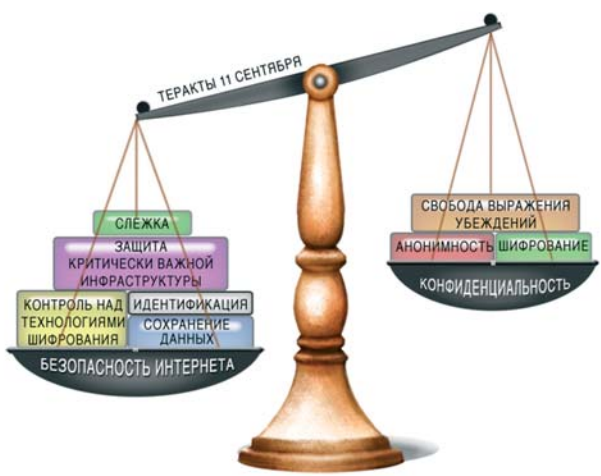
новые угрозы принципу сетевой нейтральности, а также предпосылки к созданию «нового Интернета», который, среди прочего, поможет сделать коммуникацию в Интернете более безопасной.

Кибербезопасность и тайна частной жизни

Еще одним спорным моментом является соотношение между безопасностью и защитой тайны частной жизни. Потребует ли обеспечение кибербезопасности принятия мер, предполагающих частичный отказ от права на тайну частной жизни? Как должно регулироваться использование программного обеспечения для шифрования, которое может применяться и для законной защиты тайны переписки, и для защиты незаконной коммуникации террористов и преступников? Ответ на этот и иные вопросы зависит от постоянно колеблющегося равновесия между кибербезопасностью и неприкосновенностью частной жизни.

После террористической атаки в Нью-Йорке 11 сентября 2001 г. соображения безопасности вышли в США на первое место, следствием чего стало принятие ряда законодательных актов, предусматривающих, помимо прочего, более активную слежку в Интернете. Представители гражданского общества отреагировали на это привлечением внимания к защите тайны частной жизни и принципу свободы выражения убеждений.

На международном уровне вопрос о балансе между обеспечением безопасности ИКТ и защитой тайны частной жизни был в центре дискуссий о распространении Конвенции Совета Европы по киберпреступности на глобальный уровень. Основным возражением активис-



тов, отстаивающих права человека, было то, что Конвенция стремится решить проблемы кибербезопасности за счет тайны частной жизни и других прав человека.

ШИФРОВАНИЕ

Одним из центральных вопросов в дискуссиях по обеспечению безопасности Интернета является проблема шифрования, или криптографической защиты, которая касается инструментов, используемых для защиты передаваемых данных.

Шифровальное программное обеспечение (ПО) с помощью определенных математических алгоритмов делает электронную коммуникацию (электронную почту, изображения) непонятной для посторонних. Равновесие между необходимостью обеспечить конфиденциальность некоторой информации и потребностями правительств отслеживать потенциально преступную или террористическую деятельность так и не найдено.

Международные аспекты политики в отношении криптозащиты относятся к сфере управления Интернетом, поскольку регулирование шифрования должно быть глобальным или, по крайней мере, касаться всех стран, способных производить криптографические инструменты.

Например, политика США в области контроля над экспортом ПО для шифрования была не слишком успешной, поскольку США не могли контролировать распространение такого ПО на международном уровне. Американские компании, производящие ПО, начали мощную лоббистскую кампанию, основная идея которой заключалась в том, что контроль над экспортом не укрепляет национальную безопасность, а только подрывает позиции американского бизнеса.

МЕЖДУНАРОДНЫЕ РЕЖИМЫ, КАСАЮЩИЕСЯ ИНСТРУМЕНТОВ ШИФРОВАНИЯ

Вопросы криптографической защиты информации до сих пор рассматривались в двух контекстах: Вассенаарского соглашения и ОЭСР (Организация экономического сотрудничества и развития, Organization for Economic Co-operation and Development, OECD). Вассенаарское соглашение — это международный режим, установленный 33 развитыми

странами[2] с целью ограничения экспорта обычных вооружений и технологий «двойного назначения» в воюющие страны и «страны-изгои». Соглашением создан секретариат в Вене. Целью лоббистских усилий США в рамках Вассенаарского соглашения было распространение на международном уровне подхода по принципу технологии «Клиппер чип»[3], позволяющей контролировать шифровальное ПО с помощью системы депонирования ключей. Этому воспротивились многие страны, в особенности Япония и государства Скандинавии.

Компромисс был достигнут в 1998 г. благодаря внедрению норм криптографии, в соответствии с которыми в контрольный список шифровального оборудования и ПО «двойного назначения» включались все продукты с длиной ключа более 56 бит. Это правило касалось и интернет-программ — таких, как браузеры и клиенты электронной почты. Интересно отметить, что это соглашение не затрагивает «неосязаемые» виды передачи технологий (например, загрузку файлов по Интернету). Неудача с внедрением международной версии «Клиппер чип» способствовала тому, что правительство США перестало продвигать эту технологию и внутри страны. Этот пример демонстрирует связь между событиями на национальной и международной арене: в данном случае последние имели решающее влияние на первые.

ОЭСР — еще одна площадка международного сотрудничества в области шифрования данных. Хотя документы ОЭСР не имеют обязательной юридической силы, ее указания по различным вопросам считаются весьма авторитетными. Они появляются в результате работы экспертов и принятия решений на основе консенсуса. Большинство таких указаний в итоге включается в национальные законы. Деятельность ОЭСР в области криптографической защиты порождает очень много споров. Начало ей было положено в 1996 г. предложением США принять систему депонирования ключей в качестве международного стандарта. Как и в случае с Вассенаарским соглашением, переговоры по предложению США вызвали сильное противодействие со стороны Японии и скандинавских стран. В результате появилась компромиссная версия основных составляющих политики в области криптозащиты.

---

[2] На начало 2010 г. участниками Соглашения являются 40 государств. — ***Примеч. перев.***

[3] Система обеспечения криптозащиты телефонных переговоров, предложенная в 1993 г. властями США. Согласно ей, шифрование переговоров могло осуществляться только с помощью технических средств, которые при необходимости могли быть расшифрованы правоохранительными органами с помощью особого ключа доступа, заранее депонированного у «третьей стороны». Проект вызвал резкое возражение в американском обществе и так и не был реализован. — ***Примеч. перев.***

Несколько попыток создать международный режим шифрования, преимущественно в контексте Вассенаарского соглашения, не привели к установлению действенного международного режима. До сегодняшнего дня в Интернете можно приобрести мощные инструменты криптозащиты.

СПАМ

СОВРЕМЕННОЕ СОСТОЯНИЕ

Спам обычно определяется как не запрашиваемая получателем электронная корреспонденция, рассылаемая большому количеству пользователей Интернета. Спам в основном используется в рекламных целях. Наряду с этим спам рассылается для проведения общественных кампаний, политической пропаганды и распространения порнографических материалов. Проблема спама включена в «корзину», посвященную инфраструктуре, поскольку он препятствует нормальному функционированию Интернета, нарушая работу одного из основных интернет-приложений — электронной почты. Это одна из проблем управления Интернетом, касающаяся почти каждого пользователя. Согласно последней статистике, из каждых 20 электронных сообщений 19 можно классифицировать как спам. Помимо того, что спам раздражает, он приводит и к существенным экономическим потерям с точки зрения затрат пропускной способности и времени, потраченного на его чтение и удаление. Некоторые недавние исследования показали, что только потери пропускной способности, связанные со спамом, ежегодно составляют около 10 млрд евро.

Со спамом можно бороться как техническими, так и юридическими средствами. С технической точки зрения, существует много программ, фильтрующих сообщения и удаляющих спам. Основная проблема систем фильтрации состоит в том, что они порой удаляют сообщения, не являющиеся спамом. Индустрия противодействия спаму

является растущим сектором, где разрабатываются все более сложные механизмы, помогающие отличить спам от обычной почты. Однако технические методы имеют лишь ограниченное влияние, и их использование необходимо сопровождать конкретными правовыми мерами.

Что же касается правовых аспектов вопроса, отметим, что во многих странах было принято законодательство по борьбе со спамом. В США попытка найти тонкую грань между законным использованием электронной почты для рекламы и спамом предпринята в так называемом Can-Spam Act [38]. Хотя закон предусматривает суровое наказание за распространение спама, вплоть до тюремного заключения на срок до пяти лет, некоторые его положения, как утверждают критики закона, вполне терпимы к спаму или даже могут способствовать его распространению. Изначальная позиция, обозначенная в законе, предполагает, что спам разрешается, пока получатель таких сообщений не скажет «стоп» (используя право отказа от рассылок). С декабря 2003 г., когда закон был принят, статистика не зафиксировала уменьшения количества спама.

Спам и «мода в политике»

Спам — яркий пример тенденций и, в ряде случаев, «моды» в глобальной политике. В 2005 г. спам был серьезной проблемой управления Интернетом, обозначенной как важная область в отчете WGIG. Спам обсуждался в ходе Тунисского этапа WSIS, а также ряда других международных встреч. Проблема спама также получила широкое освещение в прессе.

С 2005 г., по самым скромным оценкам, объемы спама утроились (2005 г.: 30 млрд сообщений в день; 2008 г.: 100 млрд сообщений в день). Политическая же значимость спама не соответствует статистике. В глобальной политике проблема спама почти незаметна. В ходе Форума по управлению использованием Интернета в Хайдарабаде спам упоминался в названии всего лишь одного семинара (всего было предложено проведение 91 семинара). Причины подобных изменений глобальной политики в отношении спама еще только предстоит выяснить.

В июле 2003 г. в Европейском Союзе был принят собственный закон по борьбе со спамом, ставший частью Директивы по конфиденциальности и электронным коммуникациям. Законодательство ЕС делает акцент на саморегулировании и инициативах частного сектора, способствующих сокращению спама [39]. В ноябре 2006 г. Европейская комиссия выпустила Сообщение по борьбе со спамом, шпионским и противозаконным ПО. В Сообщении перечислен ряд действий, необходимых для обеспечения выполнения уже существующего законодательства, так как основную проблему авторы документа видят именно в этом.

МЕЖДУНАРОДНЫЕ ИНИЦИАТИВЫ

Законы о противодействии спаму, принятые как в США, так и в ЕС, имеют одно слабое место: отсутствие мер по предотвращению трансграничного спама. Эта проблема особенно актуальна для таких стран, как Канада, которая, по последним статистическим данным, из 20 спам-сообщений 19 получает из-за рубежа. Министр промышленности Канады Люсьен Робийяр недавно заявила, что проблема не может быть решена «в отдельно взятой стране». К сходному выводу пришли и авторы недавнего исследования законов стран ЕС о противодействии спаму, проведенного Институтом информационного права Университета Амстердама: «Уже тот факт, что источник большинства спам-сообщений находится вне ЕС, существенно ограничивает эффективность Директивы Европейского Союза». Требуется глобальное решение на основе международного договора или сходного механизма.

Меморандум о взаимопонимании, подписанный Австралией, Кореей и Великобританией, является одним из первых примеров международного сотрудничества в кампании против спама.

В ОЭСР создана Рабочая группа по спаму и подготовлен «набор инструментов» по борьбе со спамом. МСЭ также занял активную позицию по этому вопросу, организовав Тематическое совещание по вопросам противодействия распространению спама (2004) с целью рассмотреть различные возможности заключения глобального меморандума о взаимопонимании в области противодействия спаму. На региональном уровне в ЕС создана Сеть агентств по внедрению мер по борьбе со спамом, а в рамках АТЭС было подготовлено «Руководство потребителя».

Еще один возможный подход к борьбе со спамом практикуют ведущие интернет-компании, предоставляющие услуги электронной почты: America Online, British Telecom, Comcast, EarthLink, Microsot и Yahoo!. Они создали Технический альянс по противодействию спаму (ASTA), основной задачей которого является координация технических и политических инициатив в сфере борьбы со спамом.

ВОПРОСЫ

Различные определения спама

Разное понимание того, что представляет собой спам, влияет на эффективность борьбы с ним. В США кампанию по борьбе со спамом «тормозит» озабоченность защитой свободы слова и Первая поправка к Конституции. Американские законодатели считают спамом только «не запрашиваемые получателем коммерческие сообщения», игнори-

руя другие типы спама (политическую пропаганду и порнографические материалы). В большинстве стран спамом считается любая «не запрашиваемая получателем массовая электронная рассылка», независимо от ее содержания. Поскольку источником большей части спама являются США, такое разночтение в определениях существенно ограничивает любую возможность создания эффективного международного механизма по борьбе со спамом.

Спам и удостоверение подлинности электронных сообщений

Одной из структурных предпосылок спама является возможность отправки электронных сообщений с поддельным адресом отправителя. Существует техническое решение для этой проблемы, введение которого требует изменения используемых сейчас стандартов электронной почты. Рабочая группа по проектированию Интернета изучает возможность изменения протоколов электронной почты, чтобы гарантировать подлинность электронных сообщений. Это один из примеров того, как технические вопросы (стандарты) могут влиять на политику. Возможная уступка, на которую необходимо будет пойти для обеспечения подлинности электронных сообщений, — ограничение анонимности в Интернете.

Необходимость действий на глобальном уровне

Как указывалось выше, большая часть спама приходит из-за рубежа. Это глобальная проблема, требующая глобального решения. Существуют различные инициативы, которые могу привести к повышению эффективности глобального сотрудничества. Некоторые из них — такие как двусторонние меморандумы о взаимопонимании — уже упоминались. Другие включают в себя, например, наращивание потенциала и обмен информацией. Более всеобъемлющее решение потребует создания какого-либо глобального инструмента борьбы со спамом. До сих пор развитые страны предпочитали укреплять национальное законодательство, параллельно проводя двусторонние или региональные кампании по борьбе со спамом. С учетом своего невыгодного положения как получателей «глобального общественного зла», исходящего преимущественно от развитых стран, большинство развивающихся стран заинтересовано в выработке глобального ответа на проблему спама.

ПРИМЕЧАНИЯ

[1] Термины «Интернет» и «всемирная паутина» (WWW) используются как синонимы, однако между ними есть различия. Интернет — это огромная сеть сетей, предоставляющая множество различных услуг. Иногда термин «Интернет» используется для обозначения всей совокупности технологий, от инфраструктуры до приложений (электронная почта, FTP, WWW) и собственно содержания размещенных материалов. WWW — это всего лишь одно из приложений Интернета, система документов, связанных с помощью протокола передачи гипертекста (HyperText Transfer Protocol, HTTP).

[2] Передачу интернет-трафика по электросети иногда называют «Интернет из розетки» (англоязычный термин — Power Line Communication, PLC). Использование линий электропередачи сделает Интернет более доступным для многих пользователей. Для получения дополнительной информации об этой технологии, см.: "Addressing the Digital Divide with IPv6-enabled Broadband Power Line Communication" (Internet Society, ISOC Member Briefing No. 13. Адрес в Интернете: http://www.isoc.org/briefings/013).

[3] Либерализация телекоммуникационных рынков государств-участников ВТО была формально закреплена в 1998 г. в рамках Базового соглашения о телекоммуникациях. После принятия этого Соглашения более 100 государств начали процесс либерализации, связанный с приватизацией национальных телекоммуникационных монополий, введением конкуренции и установлением национальных регулирующих механизмов. Формальное название соглашения — «Четвертый протокол Генерального соглашения по торговле услугами» (принят 30 апреля 1996 г. и вступил в силу 5 февраля 1998 г. Адрес в Интернете: http://www.wto.org/english/tratop_e/serv_e/4prote_e.htm).

[4] Одним из спорных вопросов в ходе WSIS стало стремление МСЭ принимать более активное участие в процессах управления Интернетом, особенно в областях, входящих в сферу ответственности ICANN. Больше об инициативах МСЭ в отношении Интернета см.: http://www.itu.int/osg/spu/ip/.

[5] Более подробно о роли ВТО в области телекоммуникаций см.: http://www.wto.org/english/tratop_e/serv_e/telecom_e/telecom_e.htm.

[6] Распространено мнение, что государства могут получить большие экономические выгоды в результате рыночной монополии национальных операторов; противники этой точки зрения утверждают, что либерализация позволяет повысить общую рыночную стоимость, таким образом повышая уровень доходов, получаемых государством, по сравнению с монопольным рынком.

[7] Действующие региональные регистратуры (RIR): ARIN (Американская регистратура номеров Интернета), APNIC (Азиатско-тихоокеанский центр сетевой информации), LACNIC (Региональная регистратура IP-адресов Латинской Америки и Карибского региона), RIPE NCC (Европейский координационный

центр IP-сетей, охватывает регионы Европы и Ближнего Востока) и AFRINIC (Африканский центр сетевой информации). Подробное описание особенностей функционирования систем региональных регистратур см.: https://www.ripe.net/info/resource-admin/rir-system.html.

[8] Подробная информация о дискуссиях вокруг протокола IPv6 доступна на сайте исследовательского проекта «Распределение IP-адресов и IPv6», проводившегося в рамках программы DiploFoundation «Создание потенциала в сфере управления Интернетом» в 2005 г. Авторы исследования — Жан Филемон Кисангу, Марша Гутри и Муэнде Нджираини (Jean Philémon Kissangou, Marsha Guthrie, and Mwende Njiraini) (адрес в Интернете: http://textus.diplomacy.edu/Textusbin/portal/Ghome.asp?IDspace=84).

[9] Комплексное и выполненное на высоком технологическом уровне исследование вопросов безопасности интернет-протоколов, см.: Chris Chambers, Justin Dolske, and Jayaraman Iyer, TCP/IP Security, Department of Computer and Information Science, Ohio State University (адрес в Интернете: http://www.linuxsecurity.com/resource_files/documentation/tcpip-security.html).

[10] Обзор системы «родовых» доменов верхнего уровня см.: http://www.icann.org/registries/about.htm.

[11] Более ранний пример домена, созданного для материалов определенного содержания — домен kids.us. Конгресс США принял закон о создании домена kids.us, зарезервированного для детской информации. Основной проблемой стало принятие решения относительно того, что представляет собой детская информация. В результате могли возникнуть противоречия как на теоретическом, так и на практическом уровнях, связанные с регулированием контента. В настоящее время домен kids.us используется исключительно как часть странового домена США.

[12] Правительство США не соблюдало процедуры принятия решений ICANN во время спора о создании домена .xxx. Свое неодобрение Министерство торговли США выразило в письме, адресованном главе Совета директоров ICANN.

[13] Бланк заявления на регистрацию доменного имени в зоне .cat см.: http://www.icann.org/tlds/stld-apps-19mar04/cat.htm.

[14] Отчет IANA о выделении ccTLD Палестине, см.: http://www.IANA.org/reports/ps-report-22mar00.htm.

[15] Например, ЮАР использовала суверенное право как основание для восстановления контроля над своим страновым доменом. Недавно вступивший в силу закон гласит, что использование странового домена, выходящее за рамки, обозначенные правительством ЮАР, будет расцениваться как преступление. В качестве удачного примера многостороннего подхода обычно приводится бразильская модель управления национальными доменами. Национальный орган, регулирующий бразильские домены, открыт для всех основных заинтересованных сторон, включая правительственные органы, бизнес и гражданское общество. Напротив, опыт Камбоджи, где управление национальным доменом было отда-

но правительству, часто называется примером неудачной передачи полномочий. Правительство снизило качество услуг и ввело более высокие пошлины, что усложнило регистрацию камбоджийских доменов. Для получения более подробной информации, см.: Alfonso, Carlos, BR: CCTLD An Asset of the Commons, in: MacLean, Internet Governance: A Grand Collaboration (UN ICT Task Force, New York, 2004), pp. 291-299; Norbert Klein, Internet Governance: Perspectives from Cambodia in "Internet Governance: A Grand Collaboration" edited by Don MacLean (United Nations, 2004), pp. 227-237.

[16] «Принципы делегирования и администрации страновых доменов верхнего уровня» в настоящее время пересматриваются; см.: http://www.icann.org/committees/gac/gac-cctldprinciples-23feb00.htm.

[17] Список серверов корневой зоны, точек их подключения к сети и местоположения, а также регулирующих организаций см.: http://www.root-servers.org/.

[18] См.: http://www.icann.org/en/announcements/announcement-30sep09-en.htm

[19] Краткое изложение этих и иных судебных дел см.: http://www.diplomacy.edu/ig/resources/booklet/isp/.

[20] Frances Williams, "ISPs should be liable for spam, says UN report" (Financial Times, 8 November 2006).

[21] "The End user: Junk Payout in Spam Case", International Herald Tribune, 13 April 2006 (адрес в Интернете: http://www.iht.com/articles/2006/04/12/business/PTEND13.php).

[22] В соответствии с определением HSCGroup (www.hscgroup.co.uk), пиринг — это «двустороннее соглашение между сетевыми операторами с целью гарантировать бесплатный доступ пользователей каждой из сторон к ресурсам другой». Договоры о пиринге выгодны для всех участников и широко распространены среди интернет-провайдеров и операторов телекоммуникационных сетей.

[23] Провайдеров интернет-услуг уровня 2 иногда называют интернет-шлюзами (Internet Gateways) или точками подключения к Интернету (Internet Connection Points).

[24] Эндрю Одлижко рассматривает вопросы ценообразования и архитектуры Интернета в исторической перспективе. Он выявляет общие черты ценообразования, начиная с транспортных систем Древнего мира, а затем проводит параллели с текущей политикой ценообразования в Интернете. См.: Andrew Odlyzko, "Pricing and Architecture of the Internet: Historical Perspectives from Telecommunications and Transportation" (адрес в Интернете: http://www.dtc.umn.edu/~odlyzko/doc/pricing.architecture.pdf).

[25] Шон О'Доннел в статье «Экономическая карта Интернета» объясняет, куда уходят деньги пользователей услуг интернет-провайдеров (Shawn O'Donnell. An Economic Map of the Internet. Адрес в Интернете: http://ebusiness.mit.edu/research/papers/162_ODonnell_Map.pdf); ссылка была предложена Дьёрдем Маринковичем, Diplo's Internet Governance Portal.

[26] Thuy T. T. Nguyen and Grenville J. Armitage, "Evaluating Internet Pricing Schemes: A Three-Dimensional Visual Model," ETRI Journal, vol.27, no.1, Feb. 2005, pp. 64-74.

[27] См. веб-сайт, являющийся «онлайн-рынком» ресурсов Интернета, на котором продаются широкополосные линии передачи, доступ в Интернет и другие ресурсы: http://www.bandwidthmarket.com.

[28] Geoff Huston, "Where's the Money? — Internet Interconnection and Financial Settlements," The ISP Column, Internet Society, January 2005 (адрес в Интернете: http://ispcolumn.isoc.org/2005-01/interconns.pdf).

[29] "The Halfway Proposition: Background Paper on Reverse Subsidy of G8 Countries by African ISPs," Conference of African Ministers of Finance, Planning and Economic Development, Johannesburg, South Africa, 19 October 2002.

[30] Подробный анализ стоимости внутрисетевого подключения, см.: B. Esmat and Juan Fernandez, "International Internet Connections Costs" in William J. Drake, "Reforming Internet Governance: Perspectives from the Working Group on Internet Governance (WGIG)," New York: 2005, pp. 73-86. Mike Jensen, in "Interconnection Costs" (APC: 2005), комплексный анализ проблемы см.: http://rights.apc.org/documents/interconnection_costs.pdf.

[31] Geoff Huston, "Where's the Money? Internet Interconnection and Financial Settlement," The ISP Column, January 2005, Internet Society, pp. 7-9.

[32] Одним из препятствий на пути к согласованию этого вопроса на межгосударственном уровне является тот факт, что большинство соглашений о межсетевом подключении заключаются на уровне частных компаний, операторов телекоммуникационных сетей. Как правило, подобные соглашения конфиденциальны.

[33] Список региональных и национальных точек обмена трафиком см.: http://en.wikipedia.org/wiki/List_of_Internet_exchange_points.

[34] Информацию о возможностях точек обмена трафиком в Африке см.: "Internet Exchange Points: Their Importance to the Development of the Internet and Strategies for Their Deployment — The African Example," by Global Internet Policy Initiative (адрес в Интернете: http://www.internetpolicy.net/practices/ixp.pdf).

[35] Более подробную информацию о «Глобальной повестке дня МСЭ в области кибербезопасности» см.: http://www.itu.int/osg/csd/cybersecurity/gca/.

[36] Текст конвенции см.: http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm.

[37] Официальное название данных инструментов — «Договоры об оказании взаимной юридической помощи в вопросах уголовных преступлений» (Mutual Legal Assistance in Criminal Matters Treaties, MLATs).

[38] Дополнительную информацию о законе Can-Spam см.: http://www.ftc.gov/bcp/edu/pubs/business/ecommerce/bus61.shtm.

[39] Контактная сеть ведомств по борьбе со спамом (The Contact Network of Spam Enforcement Authorities CNSA) была основана в 2005 г. 13 странами ЕС (Францией, Австрией, Бельгией, Кипром, Республикой Чехия, Данией, Грецией, Ирландией, Италией, Литвой, Мальтой, Великобританией и Испанией). Цель организации — способствовать развитию сотрудничества между государствами-участниками и координации с институтами вне ЕС, такими как ОЭСР и МСЭ.

Раздел 3

Правовые аспекты

ПРАВОВЫЕ АСПЕКТЫ

Почти каждый вопрос из области управления Интернетом имеет правовые аспекты, однако формирование правовой базы для быстро развивающегося Интернета находится пока на начальном этапе. Существуют два основных подхода к правовым аспектам управления Интернетом:

а) «реальное» право — подход, в рамках которого Интернет рассматривается как явление, аналогичное предшествующим ему технологиям коммуникации (прошедшим в своем развитии долгий путь от сигнальных костров до телефона). Хотя Интернет быстрее и масштабнее, он по-прежнему является способом дистанционного общения между отдельными людьми. Следовательно, любые существующие правовые нормы могут применяться и по отношению к Интернету [1];

б) «киберправо» исходит из предположения, что Интернет породил новые виды социальных взаимоотношений, осуществляющихся в киберпространстве. Следовательно, для их регулирования возникает необходимость формулировать новые «киберзаконы». Доводом в поддержку этого подхода является тот факт, что невероятная скорость и объем межнационального общения, которое ведется с помощью Интернета, препятствует применению существующих правовых норм.

Хотя в обоих подходах содержится зерно истины, «реальное» право доминирует и в теории, и на практике. Согласно наиболее распространенному мнению, большая часть существующего законодательства может применяться по отношению к Интернету. Однако в ряде случаев существующие в реальном мире правовые нормы придется видоизменить для того, чтобы иметь возможность применить их к киберпространству. Для иных, более узких, проблем необходима разработка абсолютно новых законов.

ПРАВОВЫЕ МЕХАНИЗМЫ

Существует обширный набор правовых механизмов, которые либо уже применяются, либо могут быть применены в области управления Интернетом.

ГОСУДАРСТВЕННЫЕ И СОЦИАЛЬНЫЕ ПРАВОВЫЕ МЕХАНИЗМЫ

Законодательные нормы

Любая правовая норма включает в себя диспозицию (правило) и санкцию. Диспозиция определяет принятые в обществе нормы поведения (например, не совершать преступлений, платить налоги), а санкция устанавливает наказание, грозящее в случае, если правила не соблюдаются (например, штрафы, тюремное заключение, в некоторых государствах — смертная казнь).

Законодательная деятельность в отношении Интернета постепенно активизируется. В особенности это касается стран — членов ОЭСР, где информационные технологии широко распространены и оказывают огромное влияние на экономические и социальные отношения. На сегодняшний день приоритетными областями законодательной деятельности являются защита частной жизни, защита данных о пользователях, защита интеллектуальной собственности, налогообложение, противодействие киберпреступности.

Однако социальные отношения слишком многогранны и не могут регулироваться исключительно законодательными способами. Общество динамично по своей сути, и законодательные нормы всегда отстают от происходящих перемен. Это особенно заметно в наши дни, когда технологическое развитие меняет социальную реальность намного быстрее, чем законодатели могут отреагировать на эти изменения. Иногда законы устаревают до того, как их принимают. Об опасности такого устаревания правовых норм необходимо всегда помнить в процессе регулирования Интернета.

Независимо от того, признаем ли мы более адекватным «реальный» или «киберподход», несомненно одно: **законодательные нормы не делают противозаконное поведение невозможным, а только устанавливают наказание за него**. Тот факт, что мошенничество запрещено и в реальном, и в виртуальном мире, не означает, что мошенничество в результате этого полностью исчезнет. Это различие важно потому, что одним из частых аргументов в пользу разработки специальных правовых норм для «кибермира» является то обстоятельство, что различные формы противозаконного поведения (преступность, мошенничество и др.) в Интернете весьма распространены, следовательно, законы реального мира не могут эффективно применяться.

Социальные нормы (обычаи)

Как и нормы закона, социальные нормы запрещают определенное поведение. В отличие от законодательства, ни одно из государственных учреждений не имеет полномочий навязывать исполнение этих норм. Их выполнение обеспечивается сообществом посредством воздействия одних его членов на других. На заре своей истории Интернет регулиро-

вался практически исключительно совокупностью социальных норм, получивших название «нетикет» (netiquette). Основной мерой наказания за их нарушение было давление со стороны других членов интернет-сообщества и исключение из сообщества. В течение этого периода развития, когда Интернет использовался сравнительно небольшой группой людей, преимущественно исследователей, преподавателей и студентов, социальные нормы в целом соблюдались. Рост Интернета сделал предписания социального характера неэффективными. Этот вид регулирования все еще может использоваться, однако лишь внутри закрытых групп, обладающих хорошо развитыми внутренними связями.

Саморегулирование

«Белая книга» по управлению Интернетом, подготовленная правительством США в 1998 г., указывает на предпочтительность саморегулирования в управлении Интернетом. Саморегулирование содержит в себе некоторые элементы, характерные также для описанных выше социальных норм. Основное различие заключается в том, что, в отличие от социальных норм, которые нередко довольно расплывчаты, саморегулирование основывается на хорошо продуманном и организованном подходе. Нормы саморегулирования обычно закрепляются в кодексах надлежащего поведения.

Тенденция к саморегулированию особенно хорошо заметна среди интернет-провайдеров. Во многих странах правительства оказывают все большее давление на провайдеров, стремясь использовать их как инструмент проведения в жизнь политики в отношении материалов Интернета. Провайдеры все чаще прибегают к саморегулированию для установления определенных стандартов поведения и, в конечном счете, для предотвращения вмешательства правительств в их деятельность.

Хотя саморегулирование может стать полезным нормативным инструментом, опора на него при решении вопросов, вызывающих большой интерес общественности (например, политики контроля над содержанием материалов Интернета), сопряжена с определенными рисками. Остается неясным, в какой степени провайдеры смогут регулировать содержание материалов, размещенных на их веб-сайтах. Могут ли они принимать решения вместо уполномоченных правовых институтов? Смогут ли провайдеры оценить, что является приемлемым содержанием? В этом контексте не следует также забывать о свободе выражения убеждений и о тайне частной жизни.

Судебная практика

Судебная практика (решения судов) является важным элементом правовой системы США, в рамках которой предпринимались первые попытки регулировать Интернет. В этой системе судебные прецеденты

могут использоваться в качестве законодательных норм, особенно в случаях, связанных с регулированием таких новых вопросов, как Интернет. Судьям приходится принимать решения даже в том случае, если они не располагают необходимыми правовыми нормами.

Первым правовым инструментом, к которому прибегают судьи, является аналогия, при которой что-то новое связывается с чем-то знакомым. Большинство судебных дел, связанных с Интернетом, разрешаются при помощи аналогии. Список аналогий приводится на стр. 30–35.

МЕЖДУНАРОДНО-ПРАВОВОЕ РЕГУЛИРОВАНИЕ

Различие между международным частным правом и международным публичным правом

В дискуссиях об управлении Интернетом часто идет речь о необходимости опираться на международное право. Термин «международное право», как правило, используется как синоним международного *публичного права*, которое создается государствами и межправительственными организациями, обычно путем заключения международных договоров и конвенций. Однако большинство юридических проблем, связанных с Интернетом, в том числе контрактные отношения и правонарушения, содержат в себе элементы *частного права*. При разрешении таких проблем необходимо использовать международное частное право. Применимость норм международного частного права оговаривается в национальном праве, а не в международных договорах. Подобные нормы определяют критерии, на основании которых устанавливается применяемая юрисдикция и правовая система в судебных делах с международными элементами (например, юридические отношения между двумя или более лицами из различных стран) [2]. Критерием для выбора юрисдикции и правовой системы служит связь между частным лицом и национальной юрисдикцией (например, национальность, место проживания) или связь между отдельной сделкой и национальной юрисдикцией (например, где был заключен контракт, где имел место обмен).

Международное частное право

Вследствие глобального характера Интернета широкое распространение получили правовые споры, в которых участвуют частные лица и институты, подпадающие под различные национальные юрисдикции. Однако международное частное право используется для разрешения судебных споров, связанных с Интернетом, только в редких случаях, возможно, по причине того, что его процедуры зачастую сложны, медленны и дороги. Основные механизмы международного частного права были

разработаны в то время, когда трансграничное взаимодействие не было столь распространенным и интенсивным, и соответственно, судебных дел с участием частных лиц и организаций, относящихся к различным юрисдикциям, было не так много.

Международное публичное право

Международное публичное право регламентирует отношения между государствами. Некоторые инструменты международного публичного права уже регулируют проблемные области, имеющие отношение к управлению Интернетом (например, телекоммуникационные регламенты, конвенции по правам человека, международные торговые договоры). В этой части раздела будут рассмотрены только те элементы международного публичного права, которые могут быть использованы в сфере управления Интернетом, а именно международные договоры и конвенции, правовые обычаи, «мягкое право» и основополагающие принципы международного права (ius cogens).

Международные конвенции

Основные международные конвенции, имеющие отношение к Интернету, были приняты Международным союзом электросвязи. Регламент международной электросвязи 1998 г. заложил принципы регулирования телекоммуникаций, повлиявшие на дальнейшее развитие Интернета. Помимо документов МСЭ, единственной конвенцией, которая напрямую регулирует отношения в Интернете, является Конвенция о киберпреступности Совета Европы. Однако многие другие механизмы международного публичного права применимы для регулирования более широких аспектов управления Интернетом, таких как права человека, торговля и права интеллектуальной собственности.

Международное обычное право

Нормообразование в международном обычном праве включает два элемента: наличие «общей практики» (consuetudo) и признание ее в качестве юридически обязательной (opinio iuris). Развитие обычного права обычно требует длительного времени для «кристаллизации» общей практики.

Некоторые элементы новых норм обычного права уже формируются на основе того, как правительство США осуществляет контроль над корневой зоной Интернета. Правительство США проводит последовательную политику невмешательства в управление записями о национальных доменах в файле корневой зоны Интернета. Подобная устойчивая практика может быть первым шагом в формировании норм

обычного права. Пока нельзя утверждать, основывались ли действия США на признании существования определенных международно-правовых норм (opinio iuris). Если это предположение верно, возможно, будет сформирована отрасль международного обычного права, регламентирующая управление частью системы корневых серверов Интернета, относящейся к национальным доменам верхнего уровня. Подобную логику будет непросто распространить на правовой статус «родовых» доменов верхнего уровня (.com, .org, .edu, .net), которые никак не связаны с конкретными странами.

«Мягкое право»

В дискуссиях об управлении Интернетом часто используется термин «мягкое право». Большинство определений «мягкого права» указывает на то, чем оно не является: это не юридически обязательный инструмент. «Мягкое право» не обладает юридической силой, и поэтому его исполнение не может быть обеспечено международными судами или иными механизмами разрешения споров.

Инструменты «мягкого права» представляют собой принципы и нормы, а не четко определенные правила. Обычно они сформулированы в таких международных документах, как декларации, руководящие принципы и примеры законодательства.

Основные итоговые документы WSIS, включая Декларацию принципов, План действий и Региональные декларации, могут стать базой для создания норм «мягкого права». Они не обладают юридической силой, но, как правило, являются результатом длительных переговоров и достижения консенсуса между всеми странами. Обязательства, которые государства и иные заинтересованные стороны принимают на себя в ходе обсуждения норм «мягкого права» и достижения общего согласия, дают основание рассматривать эти документы как нечто большее, чем политические декларации о намерениях [3].

«Мягкое право» обладает рядом преимуществ при решении проблем управления Интернетом. Во-первых, это менее формальный подход, не требующий принятия государствами официальных обязательств и, следовательно, не нуждающийся в длительных переговорах. Во-вторых, инструменты «мягкого права» достаточно гибки, что способствует выработке новых подходов и дает возможность приспосабливаться к быстро изменяющейся ситуации в сфере управления Интернетом. В-третьих, «мягкое право» более благоприятно с точки зрения участия всех заинтересованных сторон, чем традиционный международно-правовой подход, допускающий участие только государств и межправительственных организаций.

Основополагающие принципы международного права (ius cogens)

В Венской конвенции о праве международных договорах дается следующее определение ius cogens: «Норм [а], которая принимается и признается международным сообществом государств в целом как норма, отклонение от которой недопустимо и которая может быть изменена только последующей нормой общего международного права, носящей такой же характер» [4]. Британский юрист сэр Иэн Браунли приводит следующие примеры норм ius cogens: запрет на применение силы, недопущение геноцида, принцип расовой недискриминации, осуждение преступлений против человечности, а также нормы, запрещающие работорговлю и пиратство [5]. При управлении Интернетом нормы ius cogens могут стать основой для создания определенного набора правил, таких как запрет на размещение в Интернете детской порнографии.

ЮРИСДИКЦИЯ

Количество связанных с Интернетом споров все время увеличивается, что делает юрисдикцию одним из наиболее значимых и спорных аспектов управления Интернетом. Неясность в отношении юрисдикции может иметь два непосредственных и одновременных последствия:

- неспособность государства осуществить свои юридические полномочия для регулирования социальных взаимоотношений на своей территории;
- неспособность отдельных физических и юридических лиц использовать свое право на правосудие (отказ в правосудии).

Другими возможными последствиями могут стать:

- правовая небезопасность Интернета, в том числе возможность выбора наиболее благоприятной юрисдикции и ухода от ответственности;
- замедление развития электронной коммерции.
- дробление Интернета на безопасные в правовом отношении зоны.

Принимая во внимание вышеуказанные последствия, четкое определение юрисдикции и процедурных оснований ее выбора является крайне важной проблемой с точки зрения управления Интернетом.

ВЗАИМОСВЯЗЬ МЕЖДУ ЮРИСДИКЦИЕЙ И ИНТЕРНЕТОМ

Взаимоотношения юрисдикции и Интернета изначально противоречивы, так как юрисдикция основывается главным образом на географическом разделении мира на государства. Каждое государство имеет суверенное право осуществлять юрисдикцию на своей территории. Однако Интернет делает возможным активное трансграничное взаимодействие, которое сложно (хотя и можно) отслеживать с помощью традиционных правительственных механизмов. Вопрос о юрисдикции в Интернете снова возвращает нас к одной из центральных проблем, связанных с управлением Интернетом: каким образом можно «прикрепить» Интернет к существующей правовой и политической карте? [6]

ЮРИСДИКЦИЯ — ОСНОВНЫЕ АСПЕКТЫ

Существуют три основных вопроса, имеющих отношение к юрисдикции.

- Какой суд или другой государственный орган имеет необходимые полномочия (процессуальная юрисдикция)?
- Какие законы должны применяться (материальная юрисдикция)?
- Каким образом исполняются решения суда (исполнительная юрисдикция)?

Для определения юрисдикции в конкретных случаях используются следующие основные принципы:

- территориальный принцип: власть государства над людьми и собственностью на своей территории;
- принцип гражданства: власть государства над своими гражданами вне зависимости от их местонахождения (принцип национальности);
- принцип следствия: право государства регулировать экономические и правовые последствия, проявляющиеся на территории этого государства в результате действий, совершенных за пределами государственных границ.

Другим важным принципом, установленным современным международным правом, является принцип универсальной юрисдикции [7]. Принцип универсальной юрисдикции в широком смысле означает право государства преследовать в уголовном порядке определенные типы преступлений, независимо от того, где и кем они были совершены, без обязательной связи с территорией, национальностью или особым государственным интересом [8]. Под универсальную юрисдикцию подпадают такие правонарушения, как пиратство, военные преступления и геноцид.

КОНФЛИКТ ЮРИСДИКЦИЙ

Принципы установления юрисдикции (территориальный принцип, принцип национальности и принцип следствия) неизбежно создают ситуации, когда пересекаются юрисдикции нескольких государственных судов. Проблемы с определением юрисдикции возникают тогда, когда конфликт имеет экстерриториальную составляющую (например, в нем участвуют граждане разных государств или задействованы международные транзакции). Размещая информацию в Интернете, сложно убедиться, что при этом не нарушается законодательство какой-либо страны. К любому материалу, размещенному в Интернете, можно получить доступ отовсюду. В этом смысле почти каждый вид деятельности в Интернете имеет международную составляющую, что может давать подвод к применению различных юрисдикций и вести к возникновению так называемого «эффекта переливания» [9].

Одним из наиболее наглядных и часто упоминаемых судебных дел, иллюстрирующих проблему юрисдикции, является дело Yahoo!, рассматривавшееся в 2001 г. во Франции [10]. Дело Yahoo! в очередной раз подчеркнуло значимость проблемы множественной юрисдикции [11]. Причиной судебного разбирательства послужило нарушение веб-сайтом Yahoo! французского законодательства о нацистских реликвиях, запрещающего демонстрацию и продажу материалов подобного содержания. Отметим, что сам веб-сайт был размещен в США, где распространение подобных материалов было и остается законным. По данному делу было принято судебное решение, предписывающее использование технических средств (геолокационного программного обеспечения и фильтрации доступа). Yahoo! обязали распознавать пользователей из Франции и блокировать их доступ к страницам с материалами нацистского содержания.

Помимо технических решений (геолокационного программного обеспечения и фильтрации), подходы к разрешению конфликта юрисдикций включают в себя гармонизацию национальных систем законодательства и использование арбитража и иных альтернативных механизмов разрешения споров.

Гармонизация национальных законов должна привести к появлению единого набора норм на мировом уровне. Если правовые нормы одинаковы во всех странах, то вопрос определения юрисдикции должен утратить свою остроту. Гармонизация может быть достигнута в тех сферах, где уже существует достаточная степень согласия на международном уровне — например, в отношении детской порнографии, пиратства, рабства, терроризма и киберпреступности. Постепенно сближаются позиции различных стран и по другим вопросам — таким, как спам и кибербезопасность. Однако в некоторых областях, включая политику контроля

над содержанием материалов Интернета, достижение глобального консенсуса маловероятно, так как культурные противоречия в виртуальном мире еще более непримиримы, чем в реальном [12]. Еще одним возможным следствием недостаточной гармонизации может стать перемещение информационных материалов в страны с низким уровнем регулирования Интернета. По аналогии с морским правом некоторые страны могут стать «удобными флагами» для «офшорных» центров в мире Интернета.

АРБИТРАЖ

Арбитраж (третейское разбирательство) представляет собой механизм разрешения споров, который может использоваться вместо традиционных судебных процедур. При использовании механизма арбитража решения принимаются одним или несколькими независимыми частными лицами, избранными участниками спора. Международный коммерческий арбитраж имеет давнюю традицию. Механизм третейского разбирательства обычно закрепляется в частном соглашении сторон, которые договариваются в будущем разрешать любые споры с помощью арбитража. Существует много вариантов соглашений об арбитраже, в которых регулируются такие вопросы, как место и процедура проведения арбитража, выбор применимого права и т. д.

Ниже приводится обзор основных различий между разрешением споров в суде и арбитражем.

Элементы	Судебная юрисдикция	Арбитраж
Организация	Постоянная, определяется законами /договорами	Временная (ad hoc), определяется участниками Постоянная, определяется конвенциями
Применяемые законы	Право суда (судья принимает решение о применяемом законе)	Участники сами выбирают законы; в противном случае законы определяются в соглашении, если же в соглашении законы не были определены, используются законы арбитражного органа
Процедуры	Судебные процедуры определяются законами/договорами	Определяются участниками (ad hoc). Определяются арбитражным органом (постоянные)
Компетенция/ Предмет спора	Определяются законами /договорами в соответствии с предметом спора	Определяются участниками
Решения	Обязательные	Обязательные

Арбитраж обладает множеством преимуществ по сравнению с традиционными судами, в том числе большей гибкостью, меньшими издержками, скоростью, возможностью выбора юрисдикции, а также простотой приведения в исполнение арбитражных решений, принятых за пределами государства.

Одно из основных преимуществ арбитража состоит в том, что он решает проблему выбора процедурной и материальной юрисдикции. И та, и другая выбираются участниками спора заранее. Арбитраж имеет особые преимущества и в наиболее сложной составляющей судебных дел, связанных с Интернетом — обеспечении исполнения решений. Исполнение арбитражных решений регулируется Нью-йоркской Конвенцией о признании и приведении в исполнение иностранных арбитражных решений [13]. В соответствии с этой конвенцией национальные суды обязаны выполнять арбитражные решения. На основании правового режима Нью-йоркской Конвенции обеспечить выполнение арбитражных решений проще, чем обычных судебных решений.

Арбитраж часто используется при разрешении коммерческих споров. Сформировалась основательно проработанная система правил и институтов, направленных на урегулирование коммерческих споров. Основным международным документом является Типовой закон о международном коммерческом арбитраже, который был разработан UNCITRAL в 1985 г., дополненный другими юридическими инструментами UNCITRAL [14]. Ведущие международные арбитражные организации, как правило, выполняют свои функции при торговых палатах и могут быть организованы на международном (например, Международный арбитражный суд), региональном (например, Европейский арбитражный суд) и национальном уровнях.

АРБИТРАЖ И ИНТЕРНЕТ

Арбитраж и иные альтернативные системы разрешения споров широко используются для заполнения вакуума, вызванного неспособностью существующего международного частного права решать дела, связанные с Интернетом. Частным примером такого применения арбитража является Единая политика рассмотрения споров о доменных именах (UDPR), разработанная Всемирной организацией интеллектуальной собственности (ВОИС) и принятая ICANN в качестве основной процедуры разрешения споров [15].

UDPR изначально оговаривается как механизм разрешения конфликтов во всех договорах, связанных с регистрацией родовых доменов

верхнего уровня (.com, .edu, .org, .net) и некоторых национальных доменов. Уникальным является то, что арбитражные решения применяются непосредственно путем внесения изменений в систему доменных имен, без участия национальных судов.

В целом можно сказать, что арбитраж предоставляет собой более быстрый, простой и дешевый способ разрешения конфликтов. Однако использование его в качестве основного механизма разрешения конфликтов в Интернете имеет ряд существенных недостатков. Во-первых, поскольку обращение в арбитраж обычно оговаривается в предварительном соглашении между сторонами, этот инструмент не распространяется на широкий ряд случаев, когда такое соглашение не может быть заключено заранее (клевета, киберпреступность).

Во-вторых, многие рассматривают существующую практику включения статьи об арбитраже в обычные соглашения как невыгодную для более слабой стороны (обычно для пользователя Интернета или покупателя при осуществлении электронной коммерции).

В-третьих, некоторых волнует тот факт, что арбитраж выводит прецедентное право (лежащее в основе правовых систем США и Великобритании) на глобальный уровень, что постепенно приведет к подавлению национальных правовых систем. В отношении коммерческого права это может оказаться более приемлемым, принимая во внимание уже существующий высокий уровень унификации материально-правовых норм. Однако в таких деликатных областях, как содержание материалов Интернета, и в отношении социокультурных аспектов национальные правовые системы важны, поскольку отражают культурные особенности своих стран.

ПРАВО ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ

Знания и идеи являются важнейшими ресурсами в глобальной экономике. Их защита в форме прав интеллектуальной собственности становится одним из самых важных вопросов управления Интернетом. Право интеллектуальной собственности также находится в центре дискуссий о развитии.

Развитие Интернета повлияло на право интеллектуальной собственности в основном вследствие «оцифровки» знаний и информации, а также появившихся новых возможностей их обработки. Связанные с Интернетом аспекты проблемы касаются торговых марок, авторских прав и патентов [16].

АВТОРСКОЕ ПРАВО

Авторское право защищает только выражение идей в материальной форме, например книг, компакт-дисков, компьютерных файлов и т. п. Сама идея авторским правом не защищается. Однако на практике иногда сложно провести различие между идеей и ее выражением.

Режим защиты авторских прав шел в ногу с технологическим прогрессом. Каждое новое изобретение — печатный станок, радио, телевидение, видеомагнитофон — влияло как на форму, так и на особенности применения авторского права. Интернет не стал исключением. Развитие интернет-технологий, от возможности «вырезать и вставить» отрывок текста до более сложных действий, таких как практически бесплатное распространение музыкальных и видеофайлов через Интернет, бросило вызов традиционной концепции авторского права.

Парадоксально, но Интернет создает новые возможности и для обладателей авторских прав, обеспечивая более надежные технические средства защиты и мониторинга использования материалов. В самом крайнем случае владельцы авторских прав могут вообще запретить доступ к авторским материалам, что сделает саму концепцию авторского права бессмысленной.

Эти возможности ставят под угрозу хрупкое равновесие между правами авторов и общественными интересами, лежащее в основе концепции авторского права. На сегодняшний день обладатели авторских прав, чьи интересы представляют крупные записывающие и мультимедийные компании, защищают свои права активнее, чем рядовые пользователи. Общественные интересы пока не формулируются достаточно четко и не защищаются в нужной степени. Однако постепенно ситуация выравнивается, в основном с помощью множества глобальных инициатив, направленных на предоставление свободного доступа к знаниям и информации.

СОВРЕМЕННОЕ СОСТОЯНИЕ

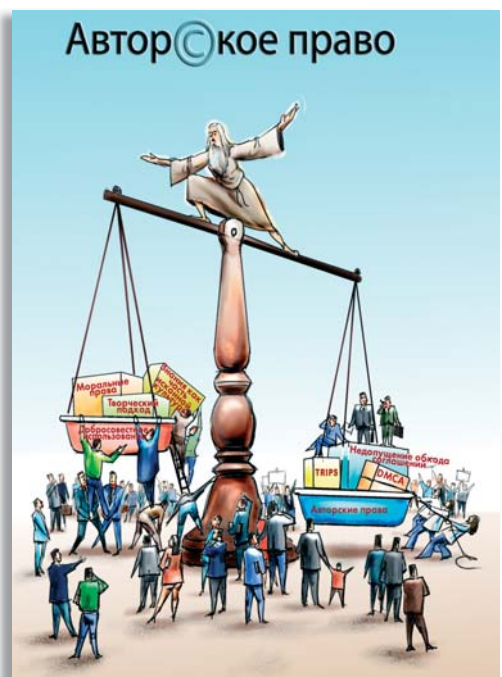
Усиление защиты авторских прав на национальном и международном уровнях

Компании индустрии звукозаписи и развлечений проводят активную лоббистскую деятельность на национальном и международном

уровнях в пользу усиления защиты авторских прав. В США защита интеллектуальной собственности была усилена Законом об авторских правах в цифровую эпоху (DMCA) 1998 г. На международном уровне защита цифровых материалов была включена в Договор о защите авторских прав ВОИС 1996 г. Этот договор также предусматривает ужесточение режима защиты авторских прав, в частности, более строгие условия для случаев ограничения эксклюзивных прав на интеллектуальную собственность, запрет на обход технической защиты авторских прав и другие подобные меры.

Возрастающее количество судебных дел

Только в 2003 г. интернет-провайдерам было направлено приблизительно 1000 повесток в суд с требованием прекратить обмен файлами между их клиентами и было возбуждено более 500 уголовных дел против индивидуальных пользователей. Дело против компаний Grokster и StreamCast, производящих программное обеспечение для обмена файлами в пиринговых сетях, является особенно важным с точки зрения будущего авторских прав в Интернете. В соответствии с Законом об авторских правах в цифровую эпоху Звукозаписывающая ассоциация США потребовала, чтобы эти компании прекратили разработку технологий, позволяющих пользователям обмениваться файлами в нарушение закона. Изначально суды США решили не признавать, в разумных пределах, такие компании, как Grokster и StreamCast, ответственными за возможные нарушения авторских прав. Однако в июне 2005 г. Верховный суд США постановил, что разработчики программного обеспечения несут ответственность за любое неправомерное использование их продукта.



Программное обеспечение против нарушения авторских прав

Инструменты, используемые нарушителями закона, могут также использоваться и его защитниками. Государственные власти и бизнес-структуры традиционно осуществляли свои функции с опорой на правовые механизмы. Однако активно набирает обороты использование «альтернативного» программного обеспечения для борьбы с нарушением авторских прав.

Статья в «International Herald Tribune» перечисляет следующие варианты использования программного обеспечения звукозаписывающими и развлекательными компаниями для защиты своих прав:

- программы-«трояны», перенаправляющие пользователей на вебсайты, где они могут законным образом купить песню, которую пытались загрузить нелегально;
- программное обеспечение, на некоторое время блокирующее компьютер и выводящее на экран предупреждение о скачивании пиратских музыкальных файлов;
- «тихое» ПО, незаметно сканирующее жесткий диск и предпринимающее попытки удалить с него любые пиратские файлы;
- «запрещающее» ПО, блокирующее доступ в Интернет при попытке загрузить пиратские файлы.

Профессор юридического факультета Стэндфордского университета Лоренс Лессиг предупреждает, что подобные меры, в свою очередь, могут оказаться противозаконными. Он обращает внимание на то, что вышеназванные инструменты не были включены в список «официальных» мер по борьбе с нарушением авторских прав. Означает ли это, что компании, самостоятельно использующие такие меры, нарушают закон?

Технологии «управления цифровыми правами»

В качестве долговременного и более структурного подхода к решению проблемы бизнес внедряет различные технологии управления доступом к материалам, защищенным авторским правом. Компания Microsoft создала программное обеспечение для «управления цифровыми правами» с целью регулирования загрузки звуковых файлов, фильмов и других материалов, защищенных авторским правом. Подобные системы были созданы компаниями Xerox (ContentGuard), Philips и Sony (InterTrust).

Использование технологических инструментов для защиты авторских прав получило поддержку как на международном уровне (Договор по авторскому праву ВОИС), так и в Законе об авторских правах в цифровую

эпоху, принятом в США. Последний, кроме того, придал противозаконный статус попыткам обойти технологическую защиту авторских прав.

ВОПРОСЫ

Усовершенствовать существующие или создавать новые механизмы защиты авторских прав?

Каким образом необходимо изменить механизмы защиты авторских прав, чтобы они отражали глубокие перемены, произошедшие под влиянием цифровых технологий и достижений в области Интернета? По мнению авторов «Белой книги» правительства США «Об интеллектуальной собственности и национальной информационной инфраструктуре», необходимо произвести самые минимальные перемены, главным образом путем «дематериализации» таких базовых концепций авторского права, как фиксация, распространение, передача и публикация. Этот подход поддержан в основных международных соглашениях в области защиты авторских прав, включая Соглашение по торговым аспектам прав интеллектуальной собственности (TRIPS) и Конвенцию об авторских правах ВОИС.

Однако приверженцы другой точки зрения считают, что изменения в правовой системе должны быть глубокими, поскольку авторское право в цифровую эпоху подразумевает не только «право предотвращать копирование», но и «право предотвращать доступ». В итоге, учитывая всевозрастающие возможности ограничения доступа к цифровым материалам, возникает вопрос, нужна ли защита авторского права вообще. Необходимо понять также, как будет осуществляться защита общественных интересов — второго неизвестного в уравнении о защите авторских прав.

Защита общественных интересов — «добросовестное использование» материалов, защищенных авторским правом

Изначально целью защиты авторского права было поощрение творчества и изобретений. Именно по этой причине в понятие были включены два элемента: защита прав авторов и защита общественных интересов. Основная сложность заключалась в том, что нужно было предусмотреть возможность для широкой аудитории обращаться к материалам, защищенным авторским правом, в интересах поощрения творчества, получения знаний и обеспечения всеобщего благосостояния. С точки зрения функционирования этого механизма, общественные интересы защищались с помощью концепции «добросовестного использования» защищенных материалов. «Добросовестное использование» обычно понимается как использование для исследований и других некоммерческих целей.

Защита авторских прав и развитие

Любые ограничения «добросовестного использования» могут ухудшить положение развивающихся стран. Интернет предоставляет исследователям, студентам и другим пользователям, особенно из развивающихся стран, мощный инструмент для участия в глобальном научном обмене. Ограничительный режим защиты авторских прав может вызвать негативные последствия для потенциала развивающихся стран.

Другой аспект — рост масштабов оцифровывания предметов культуры и искусства развивающихся стран. Как ни парадоксально, развивающимся странам, в конце концов, возможно, придется платить за свое культурное и художественное наследие, когда оно будет оцифровано, помещено в новую «упаковку» и станет собственностью иностранных развлекательных и медиакомпаний.

Всемирная организация интеллектуальной собственности и Соглашение по торговым аспектам прав интеллектуальной собственности

Существуют два основных международных режима защиты прав интеллектуальной собственности (ИС). Всемирная организация интеллектуальной собственности (ВОИС) координирует режим защиты ИС в традиционном понимании, основанный на Бернской и Парижской конвенциях. Другой, еще только складывающийся режим координируется Всемирной торговой организацией (ВТО) и основывается на Соглашении по торговым аспектам прав интеллектуальной собственности (TRIPS). Координация вопросов интеллектуальной собственности на международном уровне была передана от ВОИС к ВТО с целью усиления защиты ИС, особенно с точки зрения правоприменения. Это обстоятельство стало основным достижением развитых стран во время Уругвайского раунда переговоров ВТО.

Многие развивающиеся страны обеспокоены этими событиями. Строгие правоприменительные механизмы, существующие в рамках ВТО, могут ограничить пространство для маневров, имеющееся у развивающихся стран, и возможности нахождения равновесия между потребностями развития и защитой международных (в основном американских) прав интеллектуальной собственности. До сих пор в фокусе ВТО и TRIPS были различные толкования прав интеллектуальной собственности в отношении фармацевтических товаров. Весьма вероятно, что в будущем темой дискуссий станет интеллектуальная собственность и Интернет.

Ответственность интернет-провайдеров за нарушение авторского права

Еще одним шагом в направлении ужесточения международных правоприменительных механизмов в сфере интеллектуальной собственности стало возложение на интернет-провайдеров ответственности за размещенные на их серверах материалы, нарушающие авторское право (если такие материалы не были удалены после уведомления о подобном нарушении). Благодаря этому появилась возможность непосредственно обеспечивать защиту прав интеллектуальной собственности в Интернете.

ЗАЩИТА ТОРГОВЫХ МАРОК

С точки зрения защиты торговых марок, главной проблемой является регулирование регистрации доменных имен. На ранних стадиях развития Интернета доменное имя предоставлялось тому, кто первым подал заявку на него. Это привело к практике так называемого киберсквоттинга, то есть регистрации названий компаний в качестве доменных имен и их последующей перепродаже по более высокой цене.

Подобная ситуация заставила представителей бизнеса сделать вопрос о защите торговых марок центральным в реформе управления Интернетом, что привело к созданию в 1998 г. Корпорации по присвоению имен и номеров в Интернете (ICANN). В «Белой книге», на основании которой была создана ICANN, правительство США поставило перед организацией задачу разработать и применять механизм защиты торговых марок в области доменных имен. Вскоре после своего создания ICANN представила Единую политику рассмотрения споров о доменных именах (UDPR), разработанную Всемирной организацией интеллектуальной собственности [17].

ПАТЕНТЫ

В традиционном понимании патент защищает новый процесс или продукт, главным образом в технической или производственной сфере.

Лишь недавно стали выдавать патенты на программное обеспечение. По мере роста количества зарегистрированных патентов появляется все больше связанных с огромными деньгами судебных дел с участием американских компаний — производителей ПО.

Среди патентов, зарегистрированных для защиты бизнес-процессов, некоторые были довольно спорными; например, требование компании British Telecom о выплате ей лицензионных вознаграждений по патенту на гипертекстовые ссылки, зарегистрированному в 1980 г. В августе 2002 г. иск был отклонен [18]. Если бы British Telecom удалось выиграть это дело, то пользователям Интернета пришлось бы платить за каждый переход по ссылке. Важно подчеркнуть, что практика выдачи патентов на ПО и связанные с Интернетом процедуры не поддерживается ни Европейским Союзом, ни большинством других стран [19].

КИБЕРПРЕСТУПНОСТЬ

Противостояние между «реальным» и «виртуальным» правом существует и в этой плоскости. Сторонники «реального» права подчеркивают, что киберпреступность аналогична преступлениям в «офлайновом» мире, только совершается, как правило, с помощью компьютера, обычно подключенного к Интернету. Преступления остаются теми же, отличаются только средства их совершения. В соответствии с «киберподходом» уникальные элементы киберпреступности требуют особого обращения, особенно когда речь идет о применении законов и профилактике преступности.

Составители Конвенции Совета Европы по киберпреступности склонялись к «реальному» праву, подчеркивая, что единственным специфическим аспектом киберпреступности является использование коммуникационных технологий как средства совершения преступления. Конвенция вступила в силу 1 июля 2004 г. и является основным инструментом в данной области [20].

ВОПРОСЫ

Определение киберпреступности

Определение понятия «киберпреступность» является одним из ключевых вопросов «киберправа», имеющим практическое правовое зна-

чение. Именно от определения зависит, какие правонарушения будут отнесены к киберпреступлениям. Если определение будет сосредоточено на преступлениях, совершенных против компьютерных систем, киберпреступность будет включать: неавторизованный доступ, нанесение ущерба компьютерным данным или программам, саботаж с целью нарушения нормального функционирования компьютерной системы или сети, неавторизованный перехват данных, передаваемых, получаемых системой или хранящихся в ней, а также компьютерный шпионаж. Определение киберпреступления как любого преступления, совершенного с помощью Интернета или компьютерных систем, охватывает более широкий спектр правонарушений, в том числе и обозначенных в Конвенции о киберпреступности, таких как компьютерное мошенничество, нарушение авторских прав, детская порнография, а также нарушение безопасности сетей.

Киберпреступность и защита прав человека

Конвенция о киберпреступности обострила дискуссию о равновесии между безопасностью и правами человека. Существуют опасения, главным образом со стороны представителей гражданского общества, что конвенция предоставляет властям слишком много полномочий, включая право проверять компьютеры хакеров, следить за обменом информацией и т. д. Эти широкие полномочия могут поставить под угрозу некоторые права человека, в частности, право на частную жизнь и свободу выражения убеждений [21]. Конвенция о киберпреступности была принята Советом Европы, одной из наиболее активных международных организаций, выступающих в защиту прав человека. Это обстоятельство может способствовать нахождению необходимого равновесия между борьбой с киберпреступностью и защитой прав человека.

Сбор и хранение улик

Одной из основных сложностей в борьбе с киберпреступностью является сбор данных для ведения судебных дел. Скорость современных коммуникаций требует быстрой реакции со стороны правоохранительных органов. Одним из возможных способов хранения улик является ведение провайдерами электронных протоколов («логов»), в которые заносится информация о том, кто и когда получал доступ к тем или иным ресурсам. Некоторые положения Конвенции о киберпреступности устанавливают обязательство хранить данные об интернет-трафике. Эта правовая норма может оказать влияние на роль интернет-провайдеров в обеспечении правопорядка в Интернете.

ТРУДОВОЕ ЗАКОНОДАТЕЛЬСТВО

Часто говорят о том, что Интернет меняет характер трудовой деятельности. Хотя это явление требует более подробного рассмотрения, для управления Интернетом имеют непосредственную важность следующие аспекты.

- Благодаря Интернету стало больше временных и краткосрочных работников. Появился термин «постоянно временный» для обозначения сотрудников, которых постоянно держат на краткосрочных, но регулярно обновляемых контрактах. Это приводит к снижению уровня социальной защищенности работников.
- С постоянным развитием телекоммуникаций и с распространением широкополосного доступа к Интернету все большее распространение получает работа на расстоянии (так называемая телеработа).
- Все более значимой тенденцией становится передача части работы в секторе обслуживания, связанной с информационными технологиями (call-центры, отделы обработки данных), на подряд в другие страны. Большой объем подобной работы уже был переведен в страны Азии и Латинской Америки, где стоимость рабочей силы невысока.

Развитие информационных технологий нарушило привычное чередование работы, свободного времени и сна (8 + 8 + 8 часов). Все сложнее становится определить, где начинается и где заканчивается работа. Эти перемены в привычках могут потребовать создания нового трудового законодательства, которое регулировало бы такие аспекты, как продолжительность рабочего дня, защита интересов работников и заработная плата.

В области трудового законодательства важным аспектом является вопрос о тайне частной жизни на рабочем месте. Имеет ли работодатель право следить за тем, как его сотрудники пользуются Интернетом (проверять содержание электронных сообщений или контролировать доступ к сайтам)? Законодательство развивается и в этой области, появляется множество разнообразных новых решений.

Во Франции, Португалии и Великобритании правовые нормы и некоторое количество судебных прецедентов защищают работника, ограничивая право работодателя следить за электронной перепис-

кой сотрудников. Работодатель обязан предварительно предупреждать своих сотрудников о проведении подобных мероприятий. В Дании суд рассматривал дело, связанное с увольнением работника за пересылку личных электронных писем и участие в чатах сексуальной тематики. Суд постановил, что увольнение было незаконным, поскольку у работодателя не было официальной политики, запрещающей использование Интернета на рабочем месте в личных целях. Другим доводом в пользу сотрудника послужил тот факт, что использование им Интернета никак не повлияло на качество его работы.

Трудовое законодательство традиционно относится к внутригосударственной сфере. Однако глобализация и развитие Интернета привели к интернационализации вопросов, связанных с трудовым законодательством. Принимая во внимание рост количества людей, работающих в иностранных организациях и осуществляющих взаимодействие на международном уровне, следует признать, что назрела необходимость создания адекватных международных механизмов регулирования. Этот аспект был признан в Декларации WSIS, которая в §47 призывает к уважению соответствующих международных норм на рынке труда, связанного с информационно-коммуникационными технологиями.

ПРИМЕЧАНИЯ

[1] Одним из убежденных сторонников реального подхода является американский судья Фрэнк Истербрук, которому приписывают слова: «Успокойтесь, киберправа не существует!». В статье «Киберпространство и лошадиное право» он заявляет, что, несмотря на значимость лошадей, лошадиного права как отдельной отрасли никогда не существовало. Судья Истербрук утверждает, что необходимо сосредоточиться на базовых юридических инструментах, таких как контракты, обязательства и т. п. См.: Frank H. Easterbrook. Cyberspace and the Law of the Horse. University of Chicago Legal Forum Issue 207, 1996 (адрес в Интернете: http://www.law.upenn.edu/law619/f2001/week15/easterbrook.pdf). Аргументы судьи Фрэнка Истербрука имели широкий резонанс, в том числе в спор вступил Лоренс Лессиг. См.: Lawrence Lessig. The Law of the Horse: What Cyberlaw Might Teach (адрес в Интернете: http://www.lessig.org/content/articles/works/finalhls.pdf).

[2] К настоящему времени было предпринято несколько попыток гармонизовать международное частное право. Основным глобальным форумом является Гаагская конференция по международному частному праву, которая разработала и приняла множество конвенций в данной области.

[3] В документах WSIS очень часто встречается слово «следует», что является отличительной чертой инструментов «мягкого права». Для получения более подробной информации, см.: Jovan Kurbalija, The Emerging Language of ICT Diplomacy—Qualitative Analysis of Terms and Concepts, DiploFoundation.

[4] Статья 53 Венской конвенции о праве международных договоров 1969 г.

[5] Ian Brownlie, Principles of Public International Law, 5th Ed. (Oxford: Oxford University Press, 1999), p. 513.

[6] Для получения более подробной информации см.: Richard Paul Salis, A Summary of the American Bar Association's (ABA) Jurisdiction in Cyberspace Project: "Achieving Legal and Business Order in Cyberspace: A Report on Global Jurisdiction Issues Created by the Internet," (адрес в Интернете: http://www.lex-electronica.org/articles/v7-1/Salis.htm); Jonathan Zittrain, Jurisdiction in Cyberspace, Internet Law Program (адрес в Интернете: http://cyber.law.harvard.edu/ilaw/mexico_2006_module_9_jurisdiction); Jurisdiction Over Internet Disputes: Different Perspectives Under American and European Law in 2002, ABA Section on International Law and Practice. Annual Spring Meeting, New York City, May 8, 2002 (адрес в Интернете: http://www.howardrice.com/uploads/content/jurisdiction_internet.pdf).

[7] К наиболее важным ресурсам в этой области относятся «Принстонские принципы универсальной юрисдикции» (Princeton Principles on Universal Jurisdiction) 2001 г. (адрес в Интернете: http://www1.umn.edu/humanrts/instree/princeton.html).

[8] Peter Malanczuk, Akehurst's Modern Introduction to International Law (London: Routledge, 1997), p. 113.

[9] Обзор судебных дел с экстратерриториальной юрисдикцией, имеющих отношение к содержанию материалов Интернета, см.: Yulia A. Timofeeva, Worldwide Prescriptive Jurisdiction in Internet Content Controversies: A Comparative Analysis, Connecticut Journal of International Law, 20, p. 199, 2005 (адрес в Интернете: http://ssrn.com/abstract=637961).

[10] Кроме того, судебные иски включают дело Федерального суда Германии против Фредерика Тобена, гражданина Австрии, в прошлом гражданина Германии, который разместил материалы, оспаривавшие существование Холокоста, на веб-сайте, расположенном в Австрии. См.: http://www.ihr.org/jhr/v18/v18n4p-2_Toben.html.

[11] Информацию о дальнейшем ходе судебного процесса см.: http://www.eff.org/legal/Jurisdiction_and_sovereignty/LICRA_v_Yahoo.

[12] Спорные ситуации связаны не только с расистскими или порнографическими материалами; наряду с ними неоднозначное отношение вызывают нелегальные азартные игры, реклама табачной продукции и торговля наркотиками.

[13] Полный текст Конвенции см.: http://www.uncitral.org/uncitral/en/uncitral_texts/arbitration/NYConvention.html.

[14] Инструменты UNCITRAL также включают в себя Арбитражный регламент UNCITRAL 1976 г., Согласительный регламент UNCITRAL 1980 г., Комментарии UNCITRAL об организации арбитражного разбирательства 1996 г., Модельный закон UNCITRAL о международной коммерческой согласительной процедуре 2002 г.

[15] Uniform Domain Name Dispute Resolution Policy, The Internet Corporation for Assigned Names and Numbers, 26 August 1999 (адрес в Интернете: http://www.icann.org/udrp/udrp-policy-24oct99.htm).

[16] Кроме того, права на интеллектуальную собственность распространяются на промышленные образцы, полезные модели, торговые секреты, географические обозначения и сорта растений.

[17] Комплексный анализ основных проблем, с которыми сталкивается UDPR, см.: "WIPO's Overview of WIPO Panel Views on Selected UDRP Questions" (адрес в Интернете: http://arbiter.wipo.int/domains/search/overview/index.html).

[18] CNET News.com. Loney, M., "Hyperlink patent case fails to click" (адрес в Интернете: http://news.com.com/2100-1033-955001.html).

[19] Более подробную информацию о дискуссиях по вопросу патентования ПО в Европе см.: http://swpat.ffii.org и http://www.eubusiness.com/Rd/patents.2006-02-02.

[20] Полный текст Конвенции см.: http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm.

[21] Критические мнения о киберпреступности, выражающие озабоченность организаций гражданского общества и движений, выступающих в защиту прав человека, см.: The Association for Progressive Communication Report on the Cybercrime Convention: http://rights.apc.org/privacy/treaties_icc_bailey.shtml; веб-сайт TreatyWatch.org http://www.treatywatch.org.

Раздел 4

Экономические аспекты

ЭКОНОМИЧЕСКИЕ АСПЕКТЫ

ЭЛЕКТРОННАЯ КОММЕРЦИЯ

На протяжении последних десяти лет электронная коммерция была одной из основных движущих сил развития Интернета. Важность экономического аспекта управления Интернетом может проиллюстрировать название документа, положившего начало реформе управления Интернетом и учредившего ICANN — «Основы глобальной электронной коммерции» (1997). В этом документе указано, что «частный сектор должен возглавить» процесс управления Интернетом и основная функция такого управления заключается в обеспечении «предсказуемой, минималистичной, непротиворечивой и простой правовой среды для электронной коммерции». Эти принципы являются фундаментом режима управления Интернетом, в центре которого находится ICANN.

ОПРЕДЕЛЕНИЕ

Четкое определение понятия «электронная коммерция» имеет множество практических и юридических последствий [1]. В случае признания сделки электронной применяются особые нормы регулирования этого вида деятельности (в частности, в сфере налогообложения и таможенных пошлин).

С точки зрения правительства США, основным критерием, отличающим традиционную торговлю от электронной, является обязательство продать товары и услуги, данное в режиме онлайн. Это означает, что любая коммерческая сделка, заключенная онлайн, рассматривается как электронная, даже если ее осуществление предполагает физическую доставку товара. Например, приобретение книги на сайте Amazon.com является электронной сделкой, несмотря на то, что книга доставляется обычной почтой. Определение, даваемое ВТО, существенно у́же: «производство, распространение, реклама, продажа и доставка товаров и услуг электронным способом». Всемирная таможенная организация определяет электронную коммерцию таким образом: «способ ведения бизнеса, основанный на использовании компьютерных и телекоммуникационных технологий для обмена данны-

ми между независимыми компьютерными информационными системами организаций с целью совершения деловой транзакции».

Электронная коммерция существует в различных формах:

- business-to-consumer (B2C) — продажа фирмой товара или услуги частному лицу. Наиболее распространенный вид электронной коммерции (например, Amazon.com);
- business-to-business (B2B) — торговля между фирмами. Наиболее экономически важный вид электронной коммерции, составляющий более 90 % от общего объема электронных сделок;
- business-to-government (B2G) — электронные госзакупки. Наиболее важный вид с точки зрения политики госзакупок;
- consumer-to-consumer (C2C) — продажа товаров и услуг частными лицами другим частным лицам; например, электронные аукционы (такие как eBay).

Многие страны развивают правовую среду для регулирования электронной коммерции. Уже приняты законы, касающиеся электронной цифровой подписи, разрешения споров, киберпреступности, защиты прав потребителей и налогообложения. На международном уровне также возрастает число инициатив и режимов, связанных с электронной коммерцией.

ВТО И ЭЛЕКТРОННАЯ КОММЕРЦИЯ

Ключевой игрок в современной международной торговле, Всемирная торговая организация регулирует многие важные для электронной коммерции вопросы, в том числе либерализацию телекоммуникаций, защиту прав интеллектуальной собственности и некоторые аспекты развития ИКТ. Следующие виды деятельности и инициативы ВТО имеют непосредственное отношение к электронной коммерции.

- Временный мораторий на обложение электронных транзакций таможенными пошлинами, введенный в 1998 г. В соответствии с ним все сделки, совершаемые в Интернете, были освобождены от уплаты таможенных пошлин.
- Создание Рабочей программы ВТО по электронной коммерции, в рамках которой продолжается дискуссия по связанным с этим видом коммерции вопросам [2].
- Механизм разрешения споров. Ярким примером, имеющим непосредственное отношение к электронной коммерции, является дело «США против Антигуа», связанное с азартными играми онлайн [3].

Хотя вопросы электронной коммерции до сих пор оставались на периферии деятельности ВТО, в данной области было предложено много

инициатив и обозначен ряд ключевых вопросов. Два примера рассматриваются ниже.

Является ли электронная коммерция торговлей товарами (регулируемой в рамках GATT[1]) или торговлей услугами (регулируемой в рамках GATS[2])?

Меняется ли, например, классификация аудиопродукции (товар это или услуга) в зависимости от того, как она доставляется покупателю — на компакт-дисках (материальная форма) или через Интернет (нематериальная форма)? В конечном счете, одна и та же песня может иметь различный торговый статус (и подлежать обложению разными налогами и таможенными пошлинами) в зависимости от способа ее доставки потребителю. Проблема классификации очень важна, поскольку к торговле товарами и услугами применяются разные правовые нормы.

Какой должна быть связь между TRIPS и защитой прав интеллектуальной собственности в Интернете?

Поскольку Соглашение по торговым аспектам прав интеллектуальной собственности (TRIPS), заключенное в рамках ВТО, предоставляет гораздо более мощные правоприменительные механизмы в области прав интеллектуальной собственности, чем конвенции ВОИС, развитые страны пытались распространить сферу применения TRIPS на электронную коммерцию и Интернет в целом, используя при этом два подхода. Во-первых, апеллируя к принципу «технологической нейтральности», они указывали, что TRIPS, как и другие нормы ВТО, необходимо распространить на любые средства телекоммуникации, включая Интернет. Во-вторых, некоторые развитые страны потребовали более тесной интеграции так называемых цифровых договоров ВТО в систему TRIPS. Оба вопроса остаются открытыми, их важность для переговоров в рамках ВТО в будущем возрастет. На текущей стадии переговоров маловероятно, что в повестке дня ВТО электронной коммерции будет уделено значительное внимание. Отсутствие глобальных соглашений по электронной торговле частично компенсируется некоторыми конкретными инициативами (касающимися, например, контрактов и подписей) и разнообразными региональными соглашениями, в основном в ЕС и Азиатско-Тихоокеанском регионе.

[1] Генеральное соглашение по тарифам и торговле (General Agreement on Tariffs and Trade).

[2] Генеральное соглашение по торговле услугами (General Agreement on Trade in Services).

ДРУГИЕ МЕЖДУНАРОДНЫЕ ИНИЦИАТИВЫ В ОБЛАСТИ ЭЛЕКТРОННОЙ ТОРГОВЛИ

Одной из наиболее успешных и широко поддерживаемых международных инициатив в области электронной коммерции является Типовой закон об электронной торговле, подготовленный Комиссией ООН по праву международной торговли (UNCITRAL). Закон в первую очередь посвящен механизмам интеграции электронной коммерции и традиционного торгового законодательства. Этот документ стал основой законодательства об электронной коммерции во многих странах. Другой инициативой, направленной на развитие электронной коммерции, является разработка Центром ООН по упрощению торговых процедур и электронному бизнесу (UN/CEFAT) набора стандартов e-business XML (ebXML). Этот набор стандартов, основанный на языке XML, в недалеком будущем может стать основой для обмена электронной торговой документацией, вытеснив используемый сейчас стандарт EDI (Electronic Data Interchange).

Европейский Союз также предпринял ряд мер в области электронной коммерции, в основном сосредоточившись на проблемах малого и среднего бизнеса [4]. Множество вопросов, связанных с электронной торговлей, в том числе защита прав пользователей и использование электронной цифровой подписи, затрагиваются и в деятельности ОЭСР. Эта организация способствует развитию электронной коммерции и исследованию связанных с ней вопросов путем публикации рекомендаций и директив. Конференция ООН по торговле и развитию (UNCTAD) наиболее активна в области исследований и развития потенциала; в основном она занята вопросами связи между электронной коммерцией и развитием. Каждый год UNCTAD публикует доклад «Электронная коммерция и развитие», который содержит как обзор текущей ситуации, так и рекомендации на будущее.

В секторе бизнеса самыми активными организациями являются Международная торговая палата, которая выпускает большое количество рекомендаций и аналитических докладов по вопросам электронной коммерции, а также ассоциация «Глобальный диалог бизнеса по электронному обществу», содействующая развитию электронной торговли, как на национальном, так и на международном уровнях.

РЕГИОНАЛЬНЫЕ ИНИЦИАТИВЫ

ЕС принял стратегию развития электронной торговли на так называемом Саммите Dot.Com лидеров стран ЕС в Лиссабоне (март, 2000 г.). Несмотря на то, что в отношении электронной торговли акцент был сделан

на частные и ориентированные на рынок инициативы, в рамках ЕС были также приняты некоторые коррекционные меры, направленные на защиту государственных и общественных интересов (содействие предоставлению универсального доступа, конкурентная политика, принимающая во внимание государственные интересы, ограничение распространения вредоносных материалов). ЕС принял Директиву по электронной коммерции, а также ряд других документов по использованию электронной цифровой подписи, защите данных и электронным финансовым транзакциям.

В Азиатско-Тихоокеанском регионе центром взаимодействия в сфере электронной торговли является международная организация Азиатско-Тихоокеанское экономическое сотрудничество (АТЭС). Руководящая группа по электронной коммерции, созданная в рамках АТЭС, исследует различные вопросы, связанные с электронной коммерцией, в том числе вопросы защиты прав потребителей, защиты данных, противодействия спаму и киберпреступности. Последней и наиболее значимой законодательной инициативой является Индивидуальный план действий АТЭС по развитию безбумажной торговли, нацеленный на создание в регионе к 2010 г. системы торговли с полностью безбумажным документооборотом.

ЗАЩИТА ПРАВ ПОТРЕБИТЕЛЕЙ

Доверие потребителей является одним из основных условий успешного развития электронной коммерции. Этот вид деятельности является относительно новым, поэтому потребители еще не доверяют электронной коммерции так, как традиционной торговле. Защита прав потребителей является важным правовым инструментом укрепления доверия к электронной торговле. Регулирование электронной коммерции должно защищать потребителей в различных сферах: от недобросовестной рекламы, от некачественных товаров и услуг, от кражи или незаконной передачи личных финансовых данных (например, информации о платежных картах). Новой характерной особенностью электронной коммерции становится необходимость защиты прав потребителей на международном уровне, что не является приоритетом для традиционной торговли. В прошлом потребители редко нуждались в международной защите, так как в основном приобретали товары и услуги в своей стране. С развитием электронной коммерции все больше сделок выходит за пределы государственных границ.

Важным вопросом с точки зрения защиты прав потребителей является проблема юрисдикции, к которой существует два основных подхода. Первый подход более выгоден для продавцов (преимущественно компаний, осуществляющих электронную торговлю) и основывается на принципе «страны происхождения», или принципе «предписано продавцом». При таком сценарии компании, занимающиеся электронной коммерцией, имеют преимущество, поскольку всегда действуют в рамках предсказуемой и хорошо знакомой им правовой среды. Другой подход, защищающий в первую очередь покупателя, основывается на принципе «страны назначения». Здесь главной проблемой для компаний становится возможность столкновения с множеством разнообразных правовых систем. Одним из предлагаемых механизмов разрешения этой проблемы является гармонизация законодательства различных стран в сфере защиты прав потребителей, что делает менее актуальным сам вопрос о юрисдикции.

В области защиты прав потребителей, как и в других вопросах, связанных с электронной коммерцией, ведущую роль на международной арене играет ОЭСР. В рамках этой организации были приняты Директива по защите прав потребителей в контексте электронной коммерции (2000) и Директива по защите потребителей от мошеннических и обманных действий на трансграничном уровне (2003). Основные принципы, разработанные ОЭСР, были заимствованы другими бизнес-ассоциациями, включая Международную торговую палату и Совет агентств по улучшению деловой практики.

Высокая степень защиты прав потребителей обеспечивается в ЕС. В частности, вопросы юрисдикции разрешаются в рамках Брюссельской конвенции по выполнению решений судов в странах ЕС, которая требует, чтобы потребители всегда могли обратиться к местному законодательству и местным судам для защиты своих прав. На глобальном уровне какие-либо действенные международные правовые инструменты созданы не были. Один из наиболее значимых документов — Конвенция ООН о договорах международной купли-продажи товаров (1980) — не затрагивает вопросы заключения потребительских договоров и защиты прав потребителей.

Ряд частных ассоциаций и неправительственных организаций также работает в сфере защиты прав потребителей при электронных сделках, к ним относятся такие организации, как «Международные потребители», «Технологический проект потребителей», «Международная сеть защиты потребителей» и «Потребительский мониторинг сети».

Дальнейшее развитие электронной коммерции потребует либо гармонизации законодательства различных стран, либо создания нового международного режима для защиты прав потребителей в контексте электронной коммерции.

НАЛОГООБЛОЖЕНИЕ

После того, как в 1831 г. Фарадей открыл основные принципы электричества (электромагнитную индукцию), скептически настроенный политик спросил его, какая польза может быть от электричества. Фарадей ответил: «Сэр, не знаю, какая от него польза. В одном я уверен: когда-нибудь вы будете брать с него налог» [5].

Возникший в управлении Интернетом спор о том, должны ли вопросы киберпространства рассматриваться как отличные от явлений реального мира, находит свое отражение и в вопросе о налогообложении [6]. США с самого начала пытались объявить Интернет зоной, свободной от налогов. В 1998 г. Конгресс США принял «Акт о свободе от налогов», продленный в декабре 2004 г. еще на три года. В октябре 2007 г. Акт был продлен до 2014 г., несмотря на опасения, что это может привести к снижению поступлений в бюджет [7].

ОЭСР и ЕС отстаивают противоположную позицию: с точки зрения налогообложения для Интернета не должно делаться каких-либо исключений. В Оттавских принципах ОЭСР отмечается, что между традиционным и «электронным» налогообложением не существует различий, которые потребовали бы введения специального регулирования. На этом принципе основывается принятый в Евросоюзе в 2003 г. закон, согласно которому расположенные не в ЕС компании электронной коммерции обязаны платить налог на добавленную стоимость при продаже товаров на территории Европейского Союза. Основным мотивом в пользу принятия этого закона было то, что компании за пределами ЕС (в основном в США) имели преимущество перед европейскими компаниями, которые должны платить НДС при всех сделках, в том числе электронных.

Еще одной проблемой в области налогообложения интернет-коммерции, по которой позиции США и ЕС расходятся, является вопрос, в казну какого государства должны уплачиваться соответствующие налоги. США крайне заинтересованы в том, чтобы налоги уплачивались в соответствии с «принципом происхождения» товара, поскольку большинство компаний, занимающихся интернет-торговлей, зарегистрированы в США.

В противоположность этому в Оттавских принципах используется критерий «страны назначения», что соответствует интересам ЕС, где с точки зрения электронной коммерции больше покупателей, чем продавцов.

ЭЛЕКТРОННЫЕ ЦИФРОВЫЕ ПОДПИСИ

Говоря в общем, электронные цифровые подписи — это инструмент, позволяющий идентифицировать человека в Интернете. Потому они связаны со многими аспектами Интернета, включая юрисдикцию, киберпреступность и электронную коммерцию. Использование цифровых подписей должно способствовать складыванию отношений доверия в Интернете. Цифровая идентификация является важным компонентом электронной коммерции. Она должна облегчать заключение электронных сделок за счет использования электронных контрактов. Например, не прост вопрос о действительности соглашения, заключенного посредством электронной почты или на веб-сайте. Ведь во многих странах закон требует, чтобы любой договор был «в письменном виде» или «подписан». Что это означает применительно к Интернету? Столкнувшись с подобными проблемами и необходимостью создать благоприятную для электронной коммерции правовую среду, многие правительства начали принимать законы об электронной цифровой подписи (ЭЦП).

Что касается ЭЦП, то основная сложность состоит в том, что правительства не пытаются решить существующую проблему (например, в случае противодействия киберпреступности или защиты авторского права), а создают новую среду, не имея в этой области практического опыта. Это привело к появлению разнообразных решений и к общей неоднозначности документов, касающихся электронной цифровой подписи. В области регулирования цифровых подписей сложились три главных подхода [8].

Первый подход — «минималистский», согласно которому электронным подписям нельзя отказать в существовании на том основании, что они существуют в электронном виде. Этот подход предусматривает множество вариантов использования электронных подписей и принят в странах с прецедентной системой права (США, Канада, Австралия, Новая Зеландия).

Второй подход — «максималистский», определяющий структуру и процедуру использования цифровых подписей, включая криптографию и использование идентификаторов «открытых ключей». Этот подход обычно предусматривает создание особых уполномоченных органов, которые смогут сертифицировать будущих пользователей цифровой подписи. Этот подход превалирует в законодательстве европейских стран — таких как Германия и Италия.

Третий подход, примером которого является Директива ЕС о цифровых подписях, сочетает в себе вышеупомянутые подходы [9]. Минимализм в нем проявляется в части, касающейся признания подписей, существующих в электронном виде. Элементы максималистского подхода находят отражение в том, что «усовершенствованные» цифровые подписи имеют больший вес с точки зрения права (например, их правомерность легче доказать в суде). Нормы ЕС о цифровых подписях являются примером решения проблемы на многостороннем уровне. Хотя эти предписания были приняты всеми государствами — членами ЕС, различия в правовом статусе цифровых подписей сохраняются.

На глобальном уровне Комиссия ООН по праву международной торговли (UNCITRAL) приняла в 2001 г. Типовой закон по электронным цифровым подписям, который придает таким подписям равный статус с обыкновенными при условии соблюдения определенных технических требований. Международная торговая палата подготовила документ под названием «Общие методы осуществления международных торговых операций, заверенных в цифровой форме» (GUIDEC), который содержит обзор имеющегося положительного опыта, норм и вопросов сертификации [10]. В непосредственной связи с электронной цифровой подписью находятся инициативы, связанные с инфраструктурой «открытого ключа» (PKI). Созданием стандартов этой инфраструктуры занимаются две организации — МСЭ и IETF.

ВОПРОСЫ

Защита тайны частной жизни и цифровые подписи

Электронные цифровые подписи являются частью более широкой проблемы: баланса между конфиденциальностью и удостоверением личности в Интернете. ЭЦП — всего лишь одна из важных технологий (но не единственная), позволяющих удостоверить личность пользователя в Интернете [11]. Например, в некоторых странах, где законодательство или стандарты и процедуры, касающиеся ЭЦП, еще не разработаны, для одобрения онлайн-транзакций банки используют подтверждение личности с помощью мобильных телефонов (по SMS).

Необходимость создания подробных стандартов правоприменения

Хотя многие развитые страны приняли законодательные акты по поводу ЭЦП, в этих документах зачастую отсутствует подробное описание стандартов и процедур применения этих законов. Принимая во внимание новизну проблемы, многие страны заняли выжидательную позицию, пытаясь понять, в каком направлении будут развиваться стандарты.

Инициативы по стандартизации проявляются на разных уровнях, включая международные организации (МСЭ) и профессиональные ассоциации (IETF).

Опасность несовместимости

Разнообразие подходов и стандартов в области цифровых подписей может привести к несовместимости разных национальных систем. Решение проблемы «лоскутным» способом может ограничить развитие электронной коммерции на глобальном уровне. Необходимая гармонизация может быть достигнута при помощи региональных и глобальных организаций.

ЭЛЕКТРОННЫЕ ПЛАТЕЖИ: ИНТЕРНЕТ-БАНКИНГ И ЭЛЕКТРОННЫЕ ДЕНЬГИ

Общим компонентом различных определений электронных платежей является то, что финансовые транзакции происходят в интернет-среде с использованием онлайновых платежных систем. Наличие системы электронных платежей является предпосылкой успешного развития электронной торговли. Сфера электронных платежей требует разграничения понятий «электронные деньги» и «интернет-банкинг».

Предоставление банковских услуг в режиме онлайн (интернет-банкинг, или электронный банкинг) предполагает использование подключенного к Интернету персонального компьютера для осуществления традиционных банковских операций — таких как денежные переводы и оплата кредитными картами. Новым становится только инструмент совершения операций, тогда как сами они остаются теми же. Интернет-банкинг снижает издержки на осуществление сделок и предоставляет потребителям новые возможности. Так, клиентская транзакция, которая в традиционной форме обходится банку в 1 доллар, в форме интернет-банкинга стоит лишь 0,02 доллара [12]. С точки зрения регулирования интернет-банкинг порождает новые проблемы в том, что касается лицензирования банков государственными финансовыми органами. Как лицензировать виртуальные банки? Второй вопрос из области регулирования, уже освещавшийся в этой книге — защита прав потребителей на международном уровне.

По сравнению с интернет-банкингом электронные деньги представляют собой значительное нововведение. Правление Федеральной резерв-

ной системы США определяет их как деньги, находящиеся в электронном обращении. Электронные деньги обычно ассоциируются с так называемым смарт-картами, выпускаемыми компаниями Mondex, Visa Cash и Cyber Cash. Все электронные деньги имеют следующие черты:

- хранятся в электронном виде, чаще всего на электронной карте с магнитной полосой или микропроцессорным чипом;
- обращаются в электронном виде. В большинстве случаев используются для расчетов между фирмой-продавцом и покупателем, однако возможно и осуществление денежных переводов между физическими лицами;
- осуществление сделок с использованием электронных денег представляет собой сложную систему, включающую в себя эмитента электронных денег, сетевых операторов и банк, проводящий клиринговые операции.

На сегодняшний день использование электронных денег находится на ранней стадии своего развития. Электронные деньги не получили широкого распространения главным образом из-за недостаточного уровня безопасности и конфиденциальности. Развитие электронных денег возможно в двух направлениях:

1) эволюционное, которое потребует усовершенствования средств осуществления электронных сделок, в частности, развития эффективной системы микроплатежей. Но в итоге основой всех сделок по-прежнему будут существующие банковская и денежная системы;

2) революционное, которое выведет электронные деньги из-под контроля центральных банков стран. Банк международных расчетов уже обратил внимание на такие связанные с развитием электронных денег риски, как сокращение возможностей контроля над движением капитала и денежной массой. В концептуальном плане эмиссия электронных денег будет означать отсутствие контроля над ними со стороны центрального банка страны. Подобный подход даст возможность частным организациям выпускать собственные деньги для использования в электронной коммерции. В контексте недавнего финансового кризиса и попыток правительств вернуть себе контроль над финансовой системой маловероятно, что эксперименты с электронными деньгами получат поддержку.

ВОПРОСЫ

1. Дальнейшее распространение электронных денег и банковских услуг онлайн может *изменить всемирную банковскую систему,* предоставив потребителям дополнительные возможности и одновременно снизив стоимость банковских операций. Экономически

эффективные банковские услуги онлайн бросят серьезный вызов методам традиционных банков «из стекла и бетона» [13]. Стоит отметить, что многие традиционные финансовые институты уже активно используют интернет-банкинг. В 2002 г. в США было всего 30 «виртуальных» банков. Сегодня сложно найти банк, не предоставляющий услуги в электронной форме.

2. *Кибербезопасность* является одной из основных проблем на пути более широкого распространения электронных платежей. Как можно гарантировать безопасность финансовых транзакций в Интернете? Кибербезопасность обсуждается в другом разделе данной книги. Здесь лишь стоит подчеркнуть ответственность банков и других финансовых институтов за безопасность онлайн-транзакций. Важным событием с этой точки зрения является принятие Конгрессом США в ответ на финансовые скандалы с участием компаний Enron, Arthur Andersen и WorldCom так называемого Акта Сарбанеса-Оксли. Этот закон усиливает финансовый контроль и повышает ответственность финансовых институтов за безопасность онлайн-транзакций. Он также делит ответственность за безопасность между клиентами, которые должны проявлять определенное благоразумие, и финансовыми институтами [14].
3. Согласно опросам, *отсутствие средств платежа* (например, электронных карт) является третьей по значимости причиной того, что потенциальные покупатели не участвуют в электронной коммерции. На сегодняшний день электронная коммерция в основном осуществляется с применением кредитных карт. Это — существенное препятствие для тех стран, где рынок кредитных карт не развит. Правительствам этих стран придется внести необходимые поправки в законодательство, чтобы ускорить внедрение карточных платежных систем.
4. Чтобы способствовать развитию электронной торговли, правительствам всех стран необходимо поощрять все формы *безналичных платежей*, включая кредитные карты и электронные деньги. Быстрое внедрение электронных денег потребует дополнительных мер государственного регулирования. После того, как Гонконг первым принял комплексное законодательство в области электронной коммерции, в ЕС в 2000 г. была принята Директива об электронных деньгах [15]. Правительства неохотно внедряют электронные деньги, поскольку опасаются рисков, связанных с ограничением власти центрального банка страны. Об этом предупреждают и многие экономисты. Так, по словам Дэвида Сакс-

тона, «цифровая наличность представляет собой угрозу любому правительству на этой планете, желающему управлять собственной национальной валютой». Правительства также обеспокоены возможностью использования электронных средств платежа для отмывания денег.

5. По мнению некоторых аналитиков, перспективы действительно масштабного развития электронной коммерции во многом связаны с введением *эффективных и надежных сервисов микроплатежей*. Например, пользователи Интернета до сих пор неохотно применяют кредитные карты для совершения небольших платежей (несколько долларов или евро), которые обычно взимаются за доступ к каким-либо статьям или за другие онлайн-услуги. Схема микроплатежей, основанная на электронных деньгах, может стать необходимым решением данной проблемы. Интересно отметить, что W3C, ведущая организация в области стандартов Интернета, прекратила свои разработки в области электронной коммерции и микроплатежей, что явилось шагом назад в глобальных усилиях по стандартизации этого направления [16].
6. Учитывая саму природу Интернета, весьма вероятно, что электронные деньги станут глобальным явлением — и это даст повод *рассматривать вопрос на международном уровне*. Одним из действующих лиц в сфере предоставления банковских услуг онлайн является Группа по электронным банковским услугам Базельского комитета. Она уже начала заниматься проблемами удостоверения личности, стандартов проверки благонадежности, прозрачности, конфиденциальности, отмывания денег и трансграничного надзора над банковской деятельностью — ключевыми вопросами с точки зрения внедрения электронных денег [17].
7. Недавнее обращение генерального прокурора штата Нью-Йорк к системе Paypal и банку Citibank с требованием не осуществлять платежи в пользу интернет-казино *напрямую связывает электронные платежи и обеспечение правопорядка* [18]. То, чего правоохранительные органы не могут достигнуть с помощью правовых механизмов, они могут добиться с помощью контроля над электронными платежами.

ПРИМЕЧАНИЯ

[1] Значимость четкого определения с правовой точки зрения открыто объяснена на интерактивной странице ЕС, посвященной электронной коммерции: «Обычно мы избегаем определения электронной коммерции, за исключением нечеткого определения, что электронная коммерция связана с ведением бизнеса в электронной форме. Однако для юридических документов необходимо юридическое определение…» (адрес в Интернете: http://ec.europa.eu/archives/ISPO/ecommerce/drecommerce/answers/000025.html).

[2] Этот раздел сайта ВТО посвящен электронной коммерции: http://www.wto.org/english/tratop_e/ecom_e/ecom_e.htm.

[3] Дополнительную информацию о деле «США против Антигуа» в связи с азартными играми онлайн можно получить по адресу в Интернете: http://www.wto.org/english/tratop_e/dispu_e/cases_e/ds285_e.htm.

[4] Дополнительную информацию об инициативах ЕС в области электронной коммерции можно получить по адресу в Интернете: http://europa.eu.int/information_society/eeurope/2002/action_plan/ecommerce/index_en.htm.

[5] Maastricht Economic Research Institute on Innovation and Technology (MERIT) (адрес в Интернете: http://www.merit.unimaas.nl/cybertax/).

[6] Обсуждение различных аспектов налоговой политики применительно к Интернету см.: Arthur J. Cockfield, Transforming the Internet into a Taxable Forum: A Case Study in E-Commerce Taxation, 85 MINN. L. REV. 1171, 1235-36 (2001); Edward A. Morse, State Taxation of Internet Commerce: Something New under the Sun?, 30 CREIGHTON L. REV. 1113, 1124-27 (1997); W. Ray Williams, The Role of Caesar in the Next Millennium? Taxation of E-Commerce: An Overview and Analysis, 27 WM. MITCHELL L. REV. 1703, 1707 (2001).

[7] "Making the 'Internet Tax Freedom Act' Permanent Could Lead to a Substantial Revenue Loss for States and Localities" by Michael Mazerov (адрес в Интернете: http://www.cbpp.org/7-11-07sfp.htm).

[8] Более подробное объяснение этих трех подходов см. в: Survey of Electronic and Digital Signature Initiatives provided by the Internet Law & Policy Forum (адрес в Интернете: http://www.ilpf.org/groups/survey.htm#IB).

[9] Directive 1999/93/EC by the European Parliament and Council on 13 December 1999 on a Community Framework for Electronic Signatures.

[10] GUIDEC (General Usage for International Digitally Ensured Commerce) by the International Chamber of Commerce (адрес в Интернете: http://www.iccwbo.org/home/guidec/guidec_one/guidec.asp).

[11] Gavin Longmuir, "Privacy and Digital Authentication" (адрес в Интернете: http://caligula.anu.edu.au/~gavin/ResearchPaper.htm). Статья посвящена личным, общественным и государственным аспектам удостоверения личности в цифровом мире.

[12] Saleh M. Nsouli and Andrea Schaechter, "Challenges of the 'E-Banking Revolution'," Finance and Development, September 2002, Volume 39, Number 3, International Monetary Fund (адрес в Интернете: http://www.imf.org/external/pubs/ft/fandd/2002/09/nsouli.htm).

[13] Следующая статья посвящена введению в интернет-банкинг и обзору его преимуществ и недостатков по сравнению с традиционным банковским обслуживанием: http://www.bankrate.com/brm/olbstep2.asp.

[14] Дополнительную информацию можно получить из статьи: Edwin Jacobs, "Security as a Legal Obligation: About EU Legislation Related to Security and Sarbanes-Oxley in the European Union" (адрес в Интернете: http://www.arraydev.com/commerce/JIBC/2005-08/security.htm).

[15] Directive 2000/46/EC of the European Parliament and Council of 18 September 2000 on the taking up, pursuit of, and prudential supervision of the business of electronic money institutions.

[16] Аргументацию против микроплатежей см. в статье: "The Case against Micropayments" by Clay Shirky (адрес в Интернете: http://www.openp2p.com/pub/a/p2p/2000/12/19/micropayments.html).

[17] Группа Базельского комитета работает при Банке международных расчетов. Она публикует регулярный «Обзор новостей по электронным деньгам и интернет- и мобильным платежам» ("Survey of Developments in Electronic Money and Internet and Mobile Payments"). См.: http://www.bis.org/publ/cpss62.pdf.

[18] См.: http://www.oag.state.ny.us/press/2002/aug/aug21a_02.html.

Раздел 5

Вопросы развития

ВОПРОСЫ РАЗВИТИЯ

Технология не бывает нейтральной. История человечества знает множество примеров того, как технические достижения давали власть и могущество одним людям или даже целым сообществам и странам, оставляя в стороне других. Интернет в этом смысле не является исключением. С его распространением произошло значительное перераспределение богатства и власти как на уровне отдельных индивидов, так и в масштабе всего мира. То воздействие, которое Интернет и информационно-коммуникационные технологии оказали на распределение власти и на развитие, породило много вопросов, например:

- каким образом изменения, ускоренные развитием Интернета/ИКТ, повлияют на уже существующий разрыв между Севером и Югом? Увеличат ли Интернет/ИКТ этот разрыв или помогут сократить его?
- как и когда развивающиеся страны смогут достичь уровня информационных технологий индустриально развитых стран?

Для ответа на эти и другие вопросы необходим анализ проблем, связанных с развитием управления Интернетом.

Почти каждый аспект управления Интернетом тем или иным образом связан с развитием. Например:

- наличие телекоммуникационной инфраструктуры является основой для предоставления доступа в Интернет, первой предпосылки для преодоления разрыва в цифровых технологиях;
- текущая экономическая модель доступа к Интернету возлагает несоразмерно тяжелое бремя на развивающиеся страны, которым приходится оплачивать доступ к интернет-магистралям, расположенным в развитых странах;
- спам оказывает большее негативное воздействие на развивающиеся страны в силу небольшой пропускной способности их каналов связи и ограниченной возможности борьбы с ним;
- международное регулирование в области прав интеллектуальной собственности непосредственным образом влияет на развитие вследствие того, что доступ развивающихся стран к знаниям и информации в Интернете ограничен.

Важность вопросов развития для деятельности WSIS отмечается во многих документах, начиная с резолюции Генеральной Ассамблеи ООН по WSIS, в которой подчеркивалось, что саммит должен «способствовать развитию, в особенности с точки зрения доступа к технологиям и их передачи». Женевская декларация и План действий WSIS ставят развитие во главу угла и увязывают его реализацию с Декларацией тысячелетия, которая постулирует необходимость «доступа всех стран к информации, знаниям и коммуникационным технологиям в целях развития». Будучи связанным с «Целями развития тысячелетия», WSIS играет важную роль в этой области.

В настоящей главе рассматриваются лишь основные вопросы, связанным с развитием: разрыв в цифровых технологиях и обеспечение всеобщего доступа. Именно эти проблемы часто обсуждаются в контексте развития. Здесь также анализируются основные факторы, влияющие на Интернет и развитие: инфраструктура, финансовая поддержка, политические вопросы и социокультурные аспекты.

Каким образом ИКТ влияют на развитие общества?

Основные вопросы, связанные с информационными технологиями и развитием, кратко изложены в статье журнала «The Economist» «Проваливаясь сквозь Сеть?» (сентябрь 2000 г.) [1]. Статья приводит доводы как за, так и против тезиса о том, что информационные технологии являются движущей силой развития.

ИКТ не способствуют развитию	ИКТ способствуют развитию
• «Сетевые эффекты» помогают «пионерам» ИКТ удерживать доминирующую позицию, благодаря чему американские компании-гиганты вытесняют из электронной коммерции небольшие фирмы развивающихся стран. • Утеря продавцом главенствующей позиции и повышение значимости покупателя (в Интернете «другой поставщик всегда рядом — только мышкой щелкнуть») вредит более бедным странам, в первую очередь производителям сырьевых товаров в развивающихся странах. • Привлекательность «высокотехнологичных» акций стран с развитой экономикой снижает интерес инвесторов к развивающимся странам.	• ИКТ снижают расходы на оплату труда, становится дешевле инвестировать в развивающиеся страны. • ИКТ быстро преодолевают границы по сравнению с более ранними технологиями. Другим технологиям (например, железным дорогам и электричеству) потребовались десятилетия, чтобы достичь развивающихся стран, тогда как ИКТ распространяются стремительно. • Возможность «перепрыгнуть» устаревшие технологии, пропустить такие переходные стадии, как провода и аналоговая телефония, ускоряет темп развития. • Способность ИКТ уменьшить оптимальный размер фирмы во многих отраслях производства больше соответствует потребностям развивающихся стран.

РАЗРЫВ В ЦИФРОВЫХ ТЕХНОЛОГИЯХ

Разрыв в цифровых технологиях («цифровой разрыв») можно определить как водораздел между теми, кто в силу технических, политических, социальных или экономических причин может использовать Интернет/ИКТ, и теми, кто такой возможности не имеет. Существуют различные точки зрения на масштабы и важность разрыва в цифровых технологиях.

«Цифровой разрыв» (или разрывы) существует на разных уровнях: внутри стран и между странами, между городским и сельским населением, между молодыми и пожилыми людьми, а также между мужчинами и женщинами. «Цифровые разрывы» не существуют изолированно. Они отражают сложившееся социально-экономическое неравенство в области образования и здравоохранения, зависят от материального положения, качества жилья, наличия работы, чистой воды и еды. Вот к какому выводу пришла Целевая группа по цифровым возможностям «Большой восьмерки» (DOT Force): «Не существует никакого противоречия между “цифровым разрывом” и более широкими социальными и экономическими расколами, которые должны преодолеваться в процессе развития; “цифровой разрыв” следует понимать и преодолевать в контексте этих более широких расколов» [2].

Увеличивается ли цифровой разрыв?

Интернет/ИКТ развиваются намного быстрее, чем другие области (например, сельское хозяйство или медицина), и в силу того, что в развитых странах, в отличие от развивающихся, созданы все условия для эффективного использования достижений ИКТ, создается впечатление, что «цифровой разрыв» увеличивается постоянно и с довольно внушительной скоростью. Данная точка зрения представлена во многих авторитетных источниках, например в Докладе о развитии человека Программы развития ООН и в докладах Международной организации труда об уровне занятости. Противоположная же точка зрения основана на том, что статистика, оценивающая разрыв в цифровых технологиях, часто обманчива и «цифровой разрыв» на деле отнюдь не увеличивается. В соответствии с этой позицией традиционное внимание к количеству компьютеров, веб-сайтов и имеющейся пропускной способности нужно заменить оценкой воздействия, которое оказывают Интернет/ИКТ на общество — на людей, живущих в развивающихся странах. Примером могут послужить успехи Индии и Китая в области цифровых технологий.

ВСЕОБЩИЙ ДОСТУП

Помимо «цифрового разрыва», другой часто упоминаемой концепцией в дискуссиях о развитии является всеобщий доступ, то есть доступ для всех. Хотя этот аспект должен быть краеугольным камнем любой политики в отношении информационных технологий, существуют различные мнения и различное понимание сущности и масштаба политики всеобщего доступа. Частое упоминание этой концепции в преамбулах международных деклараций и резолюций при отсутствии необходимой политической и финансовой поддержки превращает это понятие в достаточно абстрактный, не имеющий практического значения принцип. Вопрос всеобщего доступа на международном уровне остается во многом вопросом политическим, который, в конечном счете, зависит от готовности развитых стран осуществлять инвестиции для достижения этой цели.

В отличие от международного уровня, в некоторых странах концепция всеобщего доступа подробно разработана с экономической и правовой точек зрения. Предоставление всем гражданам доступа к телекоммуникациям было положено в основу политики США в области телекоммуникаций. В результате появилась хорошо развитая система различных политических и финансовых механизмов, целью которых является финансирование доступа в отдаленных регионах и областях, где связь дорога. Субсидии предоставляются регионами с низкими расценками на связь — главным образом, большими городами. ЕС также предпринял ряд конкретных мер, направленных на обеспечение всеобщего доступа [3].

СТРАТЕГИИ ПРЕОДОЛЕНИЯ «ЦИФРОВОГО РАЗРЫВА»

Сосредоточенная на технологии теория развития, доминирующая в политике и академических кругах на протяжении последних 50 лет, гласит, что развитие зависит от доступности технологии. Чем больше технологий, тем больше развития. Однако во многих странах (главным образом, в бывших социалистических государствах) такой подход не оп-

равдал себя. Как оказалось, развитие общества является гораздо более сложным процессом, и технология является необходимой, но не единственной его предпосылкой. Другие элементы включают в себя нормативные рамки, финансовую поддержку, наличие людских ресурсов, а также иные социокультурные условия. Даже при наличии всех этих составляющих необходимо знать, как и когда они должны использоваться, сочетаться и взаимодействовать.

РАЗВИТИЕ ТЕЛЕКОММУНИКАЦИЙ И ИНФРАСТРУКТУРЫ ИНТЕРНЕТА

Возможность подключения к глобальной сети является необходимым условием для знакомства отдельных лиц и организаций с Интернетом и, в итоге, для преодоления «цифрового разрыва». Существуют различные способы установления подключения и улучшения его качества.

Быстрый рост беспроводной связи создает новые возможности для многих развивающихся стран [4]. Патрик Гельсингер, сотрудник компании Intel, считает целесообразным для развивающихся стран отказаться от проводных коммуникаций и применять беспроводные способы связи на участке «провайдер-пользователь», а также оптоволоконные сети для общенациональных информационных магистралей. Беспроводные коммуникации могут помочь решить проблему развития традиционной инфраструктуры наземных коммуникаций (избавить от необходимости прокладки кабелей через огромные расстояния многих азиатских и африканских стран). Таким способом можно преодолеть проблему «последней мили» (местной линии связи) — одну из основных преград на пути ускорения развития Интернета. Традиционно инфраструктурные аспекты цифрового разрыва находятся в центре внимания Международного союза электросвязи (МСЭ).

ФИНАНСОВАЯ ПОДДЕРЖКА

Развивающиеся страны получают финансовую поддержку по различным каналам, включая двусторонние и многосторонние агентства

содействия развитию (например, Программу развития ООН или Всемирный банк), а также через региональные инициативы по развитию и региональные банки. По мере либерализации рынка телекоммуникаций соответствующая инфраструктура все больше создается за счет прямых иностранных инвестиций. Многие развивающиеся страны ведут постоянную борьбу за привлечение частных инвестиций.

В настоящий момент большинство западных телекоммуникационных компаний находится на стадии консолидации в связи со значительными долгами, появившимися в результате чрезмерных инвестиций 1990-х годов. Хотя они еще не готовы к инвестициям, ожидается, что в недалеком будущем компании будут вкладывать деньги в развивающиеся страны, поскольку рынок развитых стран перенасыщен мощностями, созданными в конце 1990-х гг.

Важность финансового аспекта была особо подчеркнута в ходе Всемирной встречи на высшем уровне по вопросам информационного общества. Некоторые ее участники выступали за создание Фонда цифровой солидарности при ООН, в задачи которого входила бы помощь малообеспеченным странам в создании телекоммуникационной инфраструктуры. Однако это предложение не получило широкой поддержки развитых стран, по мнению которых прямые инвестиции предпочтительнее централизованного фонда развития. После WSIS в Женеве был создан Фонд цифровой солидарности. Это независимое учреждение, финансируемое преимущественно городскими и местными властями по всему миру.

СОЦИОКУЛЬТУРНЫЕ АСПЕКТЫ

Социокультурная составляющая «цифрового разрыва» включает в себя целый набор вопросов — таких как грамотность, навыки использования ИКТ, образование, сохранение лингвистического разнообразия.

Для развивающихся стран одной из основных проблем является «утечка умов», под которой подразумевают отток высококвалифицированной рабочей силы из развивающихся стран в развитые. Из-за этого развивающиеся страны проигрывают одновременно по нескольким показателям. Основной из них — утечка квалифицированной рабочей силы. Развивающиеся страны также теряют средства, вложенные в обучение покинувших страну специалистов. Вполне вероятно, что «утечка умов» продолжится, в особенности с учетом различных иммиграционных программ и облегченных схем трудоустройства, внедренных в США, Германии и других странах с целью привлечения квалифицированных специалистов в области ИКТ.

Передача (аутсорсинг) некоторых задач в области ИКТ в развивающиеся страны может остановить «утечку умов» или даже повернуть ее

вспять. Удачный пример — создание центров по разработке программного обеспечения в Бангалоре и Хайдарабаде (Индия).

На международном уровне ООН основала Сеть цифровых диаспор для ускорения темпов развития в Африке посредством мобилизации технологических, деловых и профессиональных знаний и ресурсов африканских диаспор в области ИКТ [5].

ПОЛИТИКА И РЕГУЛИРОВАНИЕ В ОБЛАСТИ ТЕЛЕКОММУНИКАЦИЙ

Политика в области телекоммуникаций тесно связана с преодолением «цифрового разрыва». Во-первых, финансовые доноры — как частные, так и государственные — не готовы инвестировать в страны, не обладающие необходимой для развития Интернета институциональной и правовой средой. Во-вторых, развитие национальных секторов ИКТ зависит от создания необходимых правовых рамок. В-третьих, существование национальных телекоммуникационных монополий является одной из причин более высокой стоимости доступа к Интернету.

Создание условий для развития ИКТ является сложной задачей, предполагающей постепенную демонополизацию рынка телекоммуникаций, разработку законодательства, связанного с Интернетом (по вопросам авторского права, права на частную жизнь, электронной коммерции и т. д.), а также обеспечение всеобщего доступа без политических, религиозных и других ограничений.

Дискуссии о влиянии либерализации рынка телекоммуникаций на развитие обращаются вокруг двух превалирующих точек зрения. Сторонники первой утверждают, что либерализация не пошла на пользу развивающимся странам. С потерей телекоммуникационных монополий правительства развивающихся стран утратили важный источник доходов для своих бюджетов. Сокращение бюджетов приводит к изменениям в других сферах общественной и экономической жизни. Согласно этой точке зрения, в проигрыше остались правительства развивающихся государств, а в выигрыше — телекоммуникационные компании из развитых стран. Вторая точка зрения заключается в том, что открытие рынка телекоммуникаций привело к усилению конкуренции, в результате чего повысился уровень обслуживания и снизились цены. В конечном итоге, будет сформирован эффективный и доступный сектор телекоммуникаций, что является необходимым условием для развития общества.

ПРИМЕЧАНИЯ

[1] “Falling through the Net?”, The Economist, 21 September 2000.

[2] Digital Opportunities for All: Meeting the Challenge. Report of the Digital Opportunity Task Force (DOT Force) including a proposal for a Genoa Plan of Action. 11 May 2001 (адрес в Интернете: http://www.g8italia.it/_en/docs/STUWX141.htm).

[3] European Union. Directive 2002/22/EC on universal service and users’ rights relating to electronic communications networks and services (Universal Service Directive) (адрес в Интернете: http://ec.europa.eu/information_society/topics/telecoms/regulatory/new_rf/documents/l_10820020424en00510077.pdf).

[4] См.: United Nations. Press Release PI/1490. Development Potential of Wireless Internet Technology Explored at Headquarters Conference Resolution adopted by the General Assembly 56/183. World Summit on the Information Society. 27 June 2003 (адрес в Интернете: http://www.un.org/news/Press/docs/2003/pi1490.doc.htm;); Larry Press. Wireless Internet Connectivity for Developing Nations// First Monday. Volume 8, number 9, September 2003 (адрес в Интернете: http://www.firstmonday.org/issues/issue8_9/press/).

[5] Больше информации о Сети цифровых диаспор см. на сайте Целевой группы ООН по ИКТ: http://www.unicttaskforce.org/stakeholders/ddn.html.

Раздел 6

Социокультурные аспекты

СОЦИОКУЛЬТУРНЫЕ АСПЕКТЫ

Интернет оказал значительное влияние на общественную и культурную ткань современного общества. Сложно назвать область общественной жизни, на которую он бы не повлиял. Интернет привносит в нашу жизнь новые модели социальной коммуникации, разрушает языковые барьеры и создает новые формы творческого самовыражения — и это лишь некоторые примеры его влияния. Сегодня Интернет становится все в большей степени социальным, а не только технологическим явлением. Корзина «Социокультурные аспекты» включает в себя такие вопросы управления Интернетом, как политика в отношении содержания материалов и многоязычие. Эти вопросы отражают наиболее яркие национальные, религиозные и культурные различия современного мира.

ПРАВА ЧЕЛОВЕКА

Интернет дал человечеству новые формы общения и взаимодействия и, в конечном счете, оказал влияние на традиционное понимание прав человека. Основной набор связанных с Интернетом прав человека включает в себя право на тайну частной жизни, на свободу выражения убеждений, на получение информации, на образование, различные права, защищающие культурное и языковое разнообразие, и права меньшинств. Неудивительно, что вопросы, связанные с правами человека, часто становились предметом жарких обсуждений в рамках как WSIS, так и IGF. Хотя вопросы прав человека обычно рассматриваются в явном виде, они также включены в такие «сквозные» темы, как сетевая нейтральность (право на доступ к информации, свобода выражения, анонимность), кибербезопасность (соблюдение прав человека при мероприятиях, направленных на обеспечение безопасности), контроль над содержанием материалов Интернета и т. д. WSIS признала важность прав человека, в особенности права на развитие и права на свободу выражения убеждений.

«Реальные права» и «киберправа»

Параллельно с концептуальными правовыми обсуждениями на тему достаточности существующего законодательства для регулирования Интернета и потребности в новом «киберправе» идут дискуссии о том, нуж-

но ли пересматривать традиционные концепции прав человека с учетом использования Интернета. Обсуждаются также и «новые» права человека, такие как право на коммуникацию.

Обзор инициатив по правам человека и Интернету

Наиболее актуальная в настоящее время инициатива в области «киберправ» — «Билль о правах в Интернете» (БПИ), в поддержку которого выступают Италия и представители гражданского общества. Движение «БПИ» стало началом процесса, поддержанного Динамической коалицией за интернет-права и принципы[1] и включающего на сегодняшний день такие инициативы, как «Мониторинг интернет-прав». «Билль о правах в Интернете» обсуждался на всех сессиях IGF. Стремясь определить «киберправа», Ассоциация прогрессивных коммуникаций подготовила проект Хартии интернет-прав [1]. Другая, академическая, инициатива — Хартия о свободе сетевых коммуникаций, разработанная на Факультете права Университета Торонто.

Google, Microsoft и ряд других интернет-компаний в ноябре 2008 г. создали Глобальную сетевую инициативу, основной целью которой является защита прав человека, в особенности права на свободу выражения убеждений и конфиденциальность. Эта инициатива особенно важна, поскольку коммерческая деятельность основных интернет-компаний может непосредственно влиять на то, как защищаются права человека [2].

Право на доступ в Интернет

Финляндия стала первой страной в мире, законодательно гарантирующей доступ в Интернет. С июля 2010 г. все жители Финляндии будут иметь право на 1-мегабитный широкополосный доступ в Интернет.

Деятельность Совета Европы в области прав человека в Интернете

Одним из основных игроков в области прав человека в Интернете является Совет Европы. Совет Европы — основной институт защиты прав человека на общеевропейском уровне, а главным его инструментом является Европейская конвенция о защите прав человека и основных свобод (1950) [3]. С 2003 г. Совет Европы принял несколько деклараций, подчеркивающих важность прав человека в Интернете [4]. Эта организация также является депозитарием Конвенции по киберпреступности — основного глобального инструмента в этой области. Это делает Совет

[1] Internet Rights and Principles Dynamic Coalition (http://internetrightsandprinciples.org/).

Европы одним из ключевых институтов с точки зрения поиска нужного баланса между правами человека и соображениями кибербезопасности в будущем.

Свобода выражения убеждений и право искать, получать и распространять информацию

В число наиболее спорных областей прав человека в Интернете входит свобода выражения убеждений. Это одно из основополагающих прав человека, которое обычно рассматривают в рамках обсуждения политики в отношении материалов Интернета и цензуры. Во Всеобщей декларации прав человека ООН свободе выражения убеждений (ст. 19) противопоставляется право государства ограничивать такую свободу в интересах удовлетворения справедливых требований морали, общественного порядка и общего благосостояния (ст. 29).

Таким образом, и обсуждение, и претворение в жизнь статьи 19 следует рассматривать в контексте достижения должного баланса между двумя этими потребностями. Такая двусмысленная ситуация делает возможным неоднозначное толкование норм и их различное применение. Конфликт между статьями 19 и 29 в «реальном» мире находит отражение и в дискуссиях о поиске правильного баланса в Интернете.

Свобода выражения убеждений привлекает особенное внимание неправительственных организаций, связанных с правами человека, в том числе Amnesty International и Freedom House. Недавнее исследование Freedom House оценивает уровень свободы при использовании Интернета и мобильных телефонов обычными пользователями в 15 странах из 6 регионов. Исследование, проведенное в 2007—2008 гг., учитывает ряд факторов, которые могут влиять на свободу выражения, в частности, состояние телекоммуникационной инфраструктуры, ограничения, вводимые правительством на доступ к технологии, нормативную среду деятельности провайдеров, цензуру и контроль над содержанием материалов, правовое окружение, слежку и незаконные нападения на пользователей и производителей материалов. Названные индикаторы включают не только действия правительства, но и активность и разнообразие сферы новых медиа в каждой стране, независимо от попыток правительства ограничить их использование либо вопреки таким попыткам [5].

Другие права человека

Право на конфиденциальность обсуждается на страницах 144–149.

Права людей с ограниченными возможностями обсуждаются на страницах 152–153.

ПОЛИТИКА В ОТНОШЕНИИ СОДЕРЖАНИЯ МАТЕРИАЛОВ ИНТЕРНЕТА

Одним из основных вопросов в рамках социокультурных аспектов управления Интернетом является политика в отношении содержания информационных материалов (контента), которая часто рассматривается с точки зрения соблюдения прав человека (свобода выражения убеждений и право на коммуникацию), деятельности правительств (контроль над содержанием) и технологии (инструменты контроля над содержанием). Дискуссии о содержании материалов Интернета обычно сводятся к обсуждению трех видов материалов.

Первая группа включает в себя материалы, необходимость контролировать распространение которых ни у кого не вызывает сомнений. Среди них детская порнография, материалы, оправдывающие геноцид и связанные с организацией террористических актов или призывами к ним, а также другая информация, запрещенная международным правом (ius cogens) [6].

Вторая группа представлена материалами, которые могут оказаться оскорбительными для определенных стран, регионов или этнических групп в силу их религиозных или культурных особенностей. Глобальные онлайн-коммуникации являются вызовом культурным и религиозным ценностям многих групп людей. Контроль над материалами Интернета, осуществляемый на Ближнем Востоке и в азиатских странах, официально объясняется необходимостью защиты специфических культурных ценностей. Обычно под этим подразумевается запрещение доступа к порнографическим сайтам и сайтам, связанным с азартными играми [7].

Третья группа состоит из примеров политической цензуры в Интернет. В 2007 г. в списке организации «Репортеры без границ» числилось 13 стран, которые осуществляют политическую цензуру в Интернете [8].

КАКИМ ОБРАЗОМ ОСУЩЕСТВЛЯЕТСЯ ПОЛИТИКА В ОТНОШЕНИИ МАТЕРИАЛОВ ИНТЕРНЕТА?

«Меню» политики в отношении материалов Интернета включает в себя следующие правовые и технические возможности, используемые в разных сочетаниях.

Фильтрация материалов правительством

Распространенным способом правительственной фильтрации является «интернет-индекс» веб-сайтов, доступ к которым граждан запрещен [9]. Если веб-сайт включен в такой индекс, доступ к нему не предоставляется. С технической точки зрения, фильтрация в основном осуществляется посредством блокировки IP-адресов на уровне маршрути-

заторов, прокси-серверов и переназначения при обращении к DNS [10]. Фильтрация материалов применяется во многих странах. Помимо государств, которые обычно ассоциируются с этой практикой — Китай, Саудовская Аравия и Сингапур, — она получает распространение и в других странах. Например, в Австралии есть система фильтрации для отдельных страниц внутри страны (но не для зарубежных сайтов) [11].

Частные системы рейтингов и фильтрации

Столкнувшись с риском дезинтеграции Интернета в связи с появлением различных государственных барьеров (систем фильтрации), W3C и другие подобные институты «сработали на опережение», предложив использовать *системы рейтингов и фильтрации,* контролируемые конечными пользователями [12]. В системах такого рода фильтрующие механизмы встраиваются в интернет-браузеры. Доступность определенных материалов на определенном сайте обозначается специальным значком. Использование подобной фильтрации особенно распространено на сайтах «для детей».

Геолокационное программное обеспечение

Еще одним техническим решением, связанным с материалами Интернета, является *геолокационное программное обеспечение*, которое фильтрует доступ пользователей к определенным материалам в зависимости от их географического местонахождения. С этой точки зрения значительным прецедентом стало дело Yahoo!, поскольку занимавшаяся им группа экспертов, в состав которой входил Винт Серф, заявила, что в 70—90 % случаев Yahoo! имела возможность определить, находится ли пользователь, пытающийся зайти в раздел сайта с нацистскими памятными материалами, во Франции [13]. Подобная техническая оценка помогла суду принять окончательное решение — от Yahoo! потребовали фильтровать доступ к из Франции к размещенным на портале нацистским материалам. Компании, занимающиеся геолокационным ПО, заявляют, что они могут определить страну без ошибки, а город — примерно в 85 % случаев, особенно если это большой город [14]. С распространением протокола IPv6, в котором каждое устройство имеет уникальный адрес в Интернете, геолокация станет еще проще.

Контроль над материалами с помощью поисковых систем

«Мостиком» между размещенным в Интернете материалом и пользователем обычно является поисковая система. Одним из первых появившихся в прессе примеров контроля над материалами с помощью поисковых систем стали действия китайских властей в отношении по-

исковой системы Google. Если пользователь вводил запрещенные слова в поисковую систему, компьютер на несколько минут терял связь с Интернетом [15]. Представитель министерства информации Китая заявил: «Вполне нормально, что иногда невозможно получить доступ к некоторым интернет-сайтам. Министерство не получало никакой информации о том, что Google блокируется» [16].

Чтобы приспособиться к местным законам, в Google решили ограничить доступ к некоторым материалам на своих региональных веб-сайтах. Например, в немецких или французских версиях Google невозможно найти веб-сайты, содержащие нацистские материалы. В определенной степени это самоцензура во избежание возможных судебных исков [17].

Вызов Веб 2.0: пользователи как авторы

С развитием платформ Веб 2.0 — блогов, форумов, сервисов обмена документами и виртуальных миров — различия между пользователем и создателем контента стираются. Пользователи Интернета могут сами создавать значительную часть материалов: сообщения блогов, видео на YouTube, фотогалереи.

Выявление, фильтрация и маркировка «неподходящих» сайтов становятся все сложнее. Несмотря на существование технологий автоматической фильтрации, автоматическое распознавание, фильтрация и категоризация изображений и видео пока недоступны. Просматривать и отмечать все материалы вручную невозможно — по некоторым оценкам, к середине 2006 г. на YouTube было размещено более 6 миллионов видеороликов, а общее время, потраченное пользователями на их просмотр, составило более 9000 лет! [18]

Одним из возможных решений, применявшимся в Марокко, Пакистане, Турции и Тунисе, является полное блокирование доступа к YouTube в стране. Однако результатом подобного «максималистского» подхода становится недоступность материалов, не вызывающих возражений, в том числе образовательных.

Необходимость создания соответствующей правовой базы

Правовой вакуум в отношении материалов Интернета дает правительствам возможность блокировать материалы по собственному усмотрению. Поскольку регулирование контента является важным вопросом для каждого общества, существует насущная необходимость выработки правовых инструментов в этой области. Государственная политика в отношении материалов Интернета может обеспечить лучшую защиту прав человека и прояснить иногда двусмысленную роль провайдеров интернет-услуг, правоохранительных органов и других лиц. В последние годы

во многих странах было принято законодательство, определяющее политику в отношении материалов Интернета.

Международные инициативы

На международном уровне основные инициативы исходят от европейских стран с мощной правовой базой, касающейся проявлений различных форм нетерпимости, включая расизм и антисемитизм. Европейские региональные институты пытались ввести эти правила и в киберпространство. Основным правовым инструментом, регулирующим вопросы содержания материалов Интернета, является Дополнительный протокол к Конвенции по киберпреступности Совета Европы.

Первой инициативой Европейского Союза в области контроля над материалами Интернета стало принятие «Рекомендации Европейской комиссии против расизма в Интернете». В качестве практического шага в этом направлении был разработан План действий по созданию безопасного Интернета, который включает в себя следующие основные пункты:

- создание в Европе единой «горячей линии», по которой можно сообщить о выявленных незаконных материалах;
- поощрение саморегулирования;
- создание рейтинга содержания, систем фильтрации, в том числе на основе эталонных критериев;
- разработка программного обеспечения и сервисов;
- популяризация знаний о безопасном использовании Интернета [19].

Организация по безопасности и сотрудничеству в Европе (ОБСЕ) также ведет активную деятельность в этой области. С 2003 г. она организовала несколько конференций и встреч, посвященных свободе выражения убеждений и возможным негативным вариантам использования Интернета (например, в целях пропаганды расизма, ксенофобии и антисемитизма).

ВОПРОСЫ

Контроль над материалами Интернета и свобода выражения убеждений

В сфере контроля над контентом обратной стороной медали является ограничение свободы выражения убеждений. Это особенно важно в США, где Первая поправка к Конституции гарантирует свободу выражения в самом широком смысле, включая право публиковать нацистские материалы и подобную им информацию.

Свобода выражения убеждений во многом определяет позицию США в международной полемике по вопросам управления Интернетом. Так, хотя США и подписали Конвенцию о киберпреступности, они не могут подпи-

сать Дополнительный протокол к ней, посвященный нетерпимым высказываниям и контролю над материалами. Свобода выражения убеждений также рассматривалась в контексте дела Yahoo!. В ходе международных переговоров США не пойдут на компромисс, который может поставить под вопрос свободу выражения убеждений, защищаемую Первой поправкой.

«Незаконно в офлайне — незаконно в онлайне»

Дискуссия о содержании материалов Интернета, так или иначе, затрагивает различия между реальным миром и «кибермиром». Существующие законы, которые регламентируют содержание распространяемых материалов, могут быть применены и в Интернете. Этот факт часто подчеркивается в Европе. Рамочное решение Совета ЕС по борьбе с расизмом и ксенофобией явно указывает: «То, что незаконно в офлайне, должно оставаться незаконным в онлайне». Один из аргументов, выдвигаемых сторонниками «киберподхода» к управлению Интернетом, заключается в том, что количество (интенсивность коммуникации, количество сообщений) влияет на качество. Согласно этой точке зрения, проблема нетерпимых высказываний состоит не в том, что отсутствуют соответствующие нормативные акты, а в том, что масштабы распространения информации и обмена ей в Интернете придают правовой проблеме новые черты. Все большее число людей имеет доступ к противозаконным материалам, поэтому обеспечить соблюдение существующих норм сложно. Следовательно, уникальность Интернета с правовой точки зрения заключается не в законах, а в их применении и соблюдении.

Эффективность контроля над материалами Интернета

При обсуждении политики в отношении материалов Интернета одним из ключевых аргументов является децентрализованная природа глобальной сети, дающая пользователям возможность обходить цензуру. Интернет включает в себя различные решения, позволяющие осуществлять эффективный контроль, однако с технической точки зрения их можно обойти. В странах, где контроль над материалами Интернета ведется на государственном уровне, технически продвинутые пользователи сумели найти обходные пути. Тем не менее, контроль над контентом направлен не на эту небольшую группу пользователей, а на более широкие слои населения. Как писал Р.Г. Коуз, «регулирование не должно быть абсолютно эффективным, чтобы быть достаточно эффективным».

Кто несет ответственность за политику в отношении материалов?

В первую очередь, содержание материалов Интернета регулируют правительства. Они определяют, что подлежит контролю и каким обра-

зом контроль должен осуществляться. На провайдеров, как основных «посредников» в Интернете, обычно возлагается ответственность за осуществление фильтрации контента — либо в соответствии с указаниями правительства, либо на основе саморегулирования (по крайней мере, в отношении материалов, не вызывающих дискуссий, таких как детская порнография). Некоторые группы пользователей, например родители, стремятся усилить контроль, чтобы обезопасить своих детей. С целью помочь родителям отфильтровывать не подходящие для детей веб-страницы, созданы различные системы рейтингов. Новые версии интернет-браузеров обычно включают в себя разнообразные возможности фильтрации. Контроль над материалами Интернета также осуществляется частными компаниями и университетами. В некоторых случаях содержание контролируется через пакеты программного обеспечения. Например, среди членов движения саентологов распространялся пакет ПО Scienositter, который блокировал доступ к сайтам, критикующим саентологию [20].

ТАЙНА ЧАСТНОЙ ЖИЗНИ И ЗАЩИТА ДАННЫХ [21]

Защита тайны частной жизни и защита данных — аспекты управления Интернетом, тесно связанные между собой. Защита данных является правовым механизмом, обеспечивающим защиту частной жизни. Что же такое «частная жизнь» (privacy)? Обычно ее определяют как право любого гражданина контролировать личную информацию и принимать решения относительно нее (раскрывать либо не раскрывать эту информацию). Право на частную жизнь является неотъемлемым правом человека. Оно признается во Всеобщей декларации прав человека, в Международном пакте о гражданских и политических правах и многих других международных и региональных конвенциях по вопросам прав человека.

Границы понятия «частная жизнь» зависят от различий в национальной культуре и образе жизни. Проблема соблюдения конфиденциальности, приватности, столь важная для западных обществ, может иметь меньшую значимость в других культурах. Современные определения этого понятия делают акцент на тайне коммуникации (отсутствие слежки за перепиской) и защите частной информации (нераскрытие информации о частных лицах). Защита тайны частной жизни, традиционно касавшаяся в основном действий государства, сегодня расширилась и, как показано на рисунке ниже, включает в себя также деловой сектор [22].

Защита тайны частной жизни: частные лица и государство

Информация всегда была для органов власти крайне важным инструментом контроля над территорией и населением. Правительства собирают большие объемы личной информации (данные регистрации рождений и браков, номера паспортов, данные о голосовании, судимости, налоговую информацию, данные учета жилых помещений, регистрации автомобилей и т. д.).

Граждане не имеют возможности отказаться от предоставления этой информации, если только не эмигрируют в другую страну, где им все равно предстоит встретиться с подобными проблемами. Информационные технологии, используемые для глубинной обработки данных, позволяют интегрировать данные из разных систем (например, налоговой, учета жилья и автомобилей) для проведения сложных аналитических процедур, поиска повторяющихся моделей и выявления несоответствий. Одной из основных сложностей для любых инициатив в области электронного правительства является обеспечение надлежащего равновесия между модернизацией правительственных функций и обеспечением гарантий прав граждан на частную жизнь.

Принятый в США после 11 сентября 2001 г. «Патриотический акт» (Patriot Act) и аналогичные законы в других странах расширили полномочия правительственных органов в области сбора информации, включая право на законный перехват информации [23]. Концепция законного перехвата с целью сбора улик также включена в Конвенцию по киберпреступности (ст.ст. 20 и 21) Совета Европы.

Защита тайны частной жизни: частные лица и бизнес

Второй стороной треугольника, иллюстрирующего различные компоненты защиты частной жизни (см. рисунок выше), являются взаимоот-

ношения между частными лицами и бизнес-сектором. Человек сообщает личную информацию о себе, открывая счет в банке, бронируя авиабилеты или отель, расплачиваясь в Интернете кредитной картой и просто работая в Интернете. В каждой из этих ситуаций остаются многочисленные «следы».

В информационной экономике сведения о клиентах, в том числе их предпочтения и особенности совершения покупок, становятся важным товаром. Для некоторых компаний — таких, как Google и Amazon — информация о предпочтениях клиентов является краеугольным камнем бизнес-модели. Успех и стабильность электронной коммерции, как между организациями, так и между организациями и частными лицами, зависит от доверия к политике обеспечения защиты частной жизни, принятой компанией, и к мерам безопасности, предпринимаемым для защиты конфиденциальной информации о клиентах от кражи и злоупотреблений [24]. С распространением социальных сетей появляются опасения, что хранящиеся в них личные данные однажды могут быть использованы не по назначению — не только владельцами сервисов или их администраторами, но и другими пользователями этих сетей.

Защита тайны частной жизни: государство и бизнес

О третьей стороне треугольника (см. рисунок на стр. 145) известно меньше всего, хотя это, может быть, самый значимый аспект, связанный с защитой тайны частной жизни. Обе стороны — и государство, и бизнес — собирают значительный объем информации о частных лицах. Часть данных они передают другим государствам и компаниям с целью предотвращения террористической деятельности. Однако в некоторых ситуациях, например, предусмотренных в Европейской директиве о защите данных, государство защищает информацию о гражданах, находящуюся в распоряжении коммерческих структур.

Защита тайны частной жизни: граждане

Последним аспектом защиты тайны частной жизни, не вошедшим в треугольник на стр. 145, становится потенциальная угроза приватности, исходящая от отдельных граждан. Сегодня любой человек, располагающий достаточными средствами, может приобрести мощные инструменты для слежки. Даже простые мобильные телефоны с камерами могут стать средствами слежения. Технология, по выражению одного из авторов журнала «The Economist», «демократизировала слежку». Известно много случаев нарушения неприкосновенности частной жизни одних людей другими — от простого подглядывания за соседями до более изощренного использования камер с целью записи номеров банковских карт и электронного шпионажа. Основная проблема с точки зрения защиты от

подобных нарушений заключается в том, что большая часть законодательных норм касается защиты тайны частной жизни от действий государства. Столкнувшись с новыми явлениями, подобными приведенным выше, некоторые страны стали предпринимать соответствующие шаги. Конгресс США принял Акт о предотвращении видеовуайеризма, запрещающий фотографировать обнаженных людей без их согласия. Германия и ряд других стран также приняли аналогичные законы, ограничивающие возможности слежки одних частных лиц за другими.

Международное регулирование защиты тайны частной жизни и конфиденциальных сведений

Одним из основных международных документов, регулирующих защиту частной жизни и конфиденциальных данных, является Конвенция о защите физических лиц при автоматической обработке персональных данных, принятая Советом Европы в 1981 г. [25] Конвенция открыта для подписания и другими государствами, в том числе не входящими в Совет Европы. Поскольку Конвенция является технологически нейтральной, она выдержала испытание временем. В последнее время ее рассматривают на предмет применимости к сбору и обработке биометрических данных.

В Европейском Союзе правовая основа для обработки личных данных заложена Директивой ЕС о защите данных (Directive 45/46/EC), которая оказала значительное влияние на национальные законодательства не только в ЕС, но и за его пределами.

Еще одним ключевым международным документом по вопросам защиты тайны частной жизни и личных данных, не носящим обязательный характер, являются «Основные принципы защиты тайны частной жизни и трансграничных потоков личных данных», подготовленные Организацией экономического сотрудничества и развития (ОЭСР) в 1980 г. Эти принципы и последующая работа ОЭСР способствовали созданию многих международных и региональных норм в этой области. На сегодняшний день почти все страны ОЭСР приняли законодательство в области защиты тайны частной жизни и наделили свои властные органы соответствующими полномочиями. Хотя предложенные ОЭСР принципы были приняты во многих странах и регионах, в способе их применения кроются различия.

Так, европейский и американский подход к этой теме значительно отличаются друг от друга. В Европе законодательство по защите данных является всеобъемлющим, в то время как в США правовые нормы, касающиеся конфиденциальности, разрабатываются отдельно для каждой сферы деятельности. В области финансовой тайны это Акт Грэмма-Лича-Блайли [26], в сфере конфиденциальности в отношении детей — Акт о защите частной жизни детей онлайн [27], конфиденциальность меди-

цинской информации призван обеспечить недавно предложенный пакет законов о здравоохранении и социальном обеспечении [28].

Другое важное отличие заключается в том, что в Европе за соблюдением законов следят государственные органы, а в США их выполнение обеспечивается частным сектором и на основе саморегулирования. Политика обеспечения конфиденциальности определяется компаниями, а частные лица самостоятельно решают, принимать ее или нет. Главным аргументом против подхода США является то, что потребители оказываются в невыгодном положении. Частные лица, как правило, не отдают себе отчета, насколько важны условия, перечисленные в политиках конфиденциальности, и принимают их, не читая.

Соглашение о «безопасной гавани» между США и ЕС

Между двумя этими подходами — американским и европейским — возникли противоречия. Основным источником проблемы стало использование личных данных коммерческими структурами. Каким образом ЕС может обеспечить соблюдение своих норм, скажем, компанией по производству программного обеспечения, расположенной в США? Каким образом Европейский Союз может гарантировать, что информация о гражданах ЕС защищается в соответствии с принципами, изложенными в Директиве по защите данных? В соответствии с какими предписаниями (американскими или европейскими) нужно обращаться с информацией, переправляемой внутри компании по корпоративным сетям из ЕС в США? Евросоюз угрожал заблокировать передачу данных в страны, не способные обеспечить уровень защиты информации, соответствующий директиве. Такая позиция неизбежно вела к конфликту с американским подходом.

Глубинные различия в подходах препятствовали достижению какого-либо соглашения. Более того, адаптация американских законов к европейским не представлялась возможной, поскольку это потребовало бы изменения некоторых фундаментальных принципов американской правовой системы. Выход из этой ситуации был найден, когда посол США Дэвид Аарон предложил формулу «безопасной гавани». Это предложение представило проблему в новом свете и позволило выйти из дипломатического тупика.

Было найдено решение, при котором нормы ЕС могут применяться к компаниям США в правовой «гавани». Американские компании, работающие с данными о гражданах стран Евросоюза, могут добровольно принять на себя обязательства выполнять требования по защите конфиденциальности, принятые в ЕС. Подписав соответствующие соглашения, компании должны следовать формальным механизмам их выполнения, согласованным между США и ЕС.

В 2000 г., когда соглашение о «безопасной гавани» было подписано, на него возлагались большие надежды как на инструмент, который поможет решить сходные проблемы в отношениях с другими странами. Однако пока эффективность соглашения не очень впечатляет. Оно подверглось критике со стороны Европейского парламента как не обеспечивающее должную степень конфиденциальности данных о гражданах ЕС. Американские компании также не слишком заинтересованы в этом подходе. Согласно недавнему исследованию компании Galexia, из 1597 компаний, участвующих в соглашении по «безопасной гавани», лишь 348 соответствуют его базовым требованиям (например, политике конфиденциальности) [29]. С учетом важности для Европейского Союза вопросов конфиденциальности и защиты данных европейским политикам, вероятно, придется найти замену неработающему соглашению о «безопасной гавани».

МНОГОЯЗЫЧИЕ И КУЛЬТУРНОЕ РАЗНООБРАЗИЕ

С первых дней своего существования Интернет был преимущественно англоязычной средой. По статистике, приблизительно 80 % содержания Интернета составляют материалы на английском языке, в то время как 80 % населения Земли говорит на других языках. Такая ситуация побудила многие страны принять согласованные меры с целью сохранения многоязычия и защиты культурного разнообразия. Задача поддержания многоязычия связана не только с сохранением культурных особенностей, но и с перспективами дальнейшего развития Интернета [30]. Чтобы Интернетом могли пользоваться более широкие слои населения, а не только элита, материалы должны быть доступны на различных языках.

ВОПРОСЫ

Во-первых, развитие многоязычия требует наличия технических стандартов, позволяющих использовать иные, чем латиница, алфавиты. Одну из первых инициатив в этой области предпринял Консорциум Unicode — некоммерческая организация, разрабатывающая стандарты для использования символов различных алфавитов. В свою очередь, ICANN и IETF предприняли важные меры, направленные на продвижение международных доменных имен (IDN) на китайском, арабском и других языках.

Во-вторых, неоднократно предпринимались попытки улучшить машинный перевод. Согласно правилам Евросоюза, официальные документы должны переводиться на языки всех государств-членов; в связи

с этим ЕС поддерживал различные проекты, направленные на усовершенствование машинного перевода. Несмотря на несомненные успехи, в основном результаты в этой области достаточно ограничены.

В-третьих, развитие многоязычия требует создания соответствующих нормативных рамок. Важным игроком в этой области является ЮНЕСКО, которая инициировала несколько проектов по развитию многоязычия и приняла ряд ключевых документов, в частности, Всеобщую декларацию по культурному разнообразию. Другой организацией, активно работающей в этой области, является Европейский Союз, провозгласивший многоязычие одним из своих главных политических и рабочих принципов.

Развитие и широкое использование инструментов Веб 2.0, которые позволяют обычным пользователям вносить вклад в создание материалов Интернета, открывает перспективы увеличения количества и объема материалов местного содержания на различных языках. Однако без общей политики продвижения многоязычия и при отсутствии положительной «обратной связи» эти возможности могут, напротив, привести к увеличению языкового разрыва. «Новые пользователи Интернета видят, насколько полезно знать английский язык и использовать его для онлайн-коммуникации, что повышает престиж языка и заставляет последующие поколения пользователей изучать его» [31].

ГЛОБАЛЬНЫЕ ОБЩЕСТВЕННЫЕ БЛАГА

Концепция глобальных общественных благ связана со многими аспектами управления Интернетом. Она имеет непосредственное отношение к таким аспектам, как доступ к инфраструктуре Интернета, защита знаний, созданных в результате взаимодействия в Интернете, защита открытых технических стандартов и доступ к онлайн-образованию.

Инфраструктура Интернета контролируется преимущественно частными компаниями. Одной из текущих задач является поиск гармоничного сочетания частной собственности на инфраструктуру Интернета и его статуса глобального общественного блага. Государственные законы дают возможность ограничивать право частной собственности с помощью определенных требований в интересах общества — таких как предоставление равных прав всем потенциальным пользователям и невмешательство в содержание передаваемых материалов.

Важной особенностью Интернета является создание новых знаний и информации в результате взаимодействия пользователей по всему миру.

Значительный объем знаний был создан в ходе обмена электронными сообщениями, через социальные сети и блоги. За исключением лицензии «Creative Commons» не существует правовых механизмов защиты этих знаний. Без надлежащего правового регулирования эти знания могут превратиться в товар, предмет продажи. Таким образом, общий фонд знаний, важная основа для творческой деятельности, может быть исчерпан. По мере того, как материалы Интернета становятся источником прибыли, все сложнее становится осуществлять свободный обмен информацией, что может привести к сокращению творческого взаимодействия.

Концепция глобального общественного блага, вкупе с такими инициативами, как «Creative Commons», может предоставить решения, способные защитить творческий потенциал Интернета и сохранить созданные в нем знания для будущих поколений.

В области стандартов также предпринимаются многочисленные попытки заменить общественные, открытые стандарты частными и проприетарными. Так было с компаниями Microsoft (применительно к браузерам и ASP) и Sun Microsystems (например Java). Стандарты Интернета (главным образом TCP/IP) считаются открытыми и общественными. Режим управления Интернетом должен обеспечить защиту основных стандартов Интернета как глобальных общественных благ.

ВОПРОСЫ

Баланс между частными и общественными интересами

Одна из основополагающих проблем, связанных с будущим развитием Интернета — поиск баланса между частными и общественными интересами. Вопрос заключается в том, как создать для частного сектора благоприятную среду, одновременно обеспечив развитие Интернета как глобального общественного блага. Во многих случаях это не «игра с нулевой суммой», а ситуация, в которой выиграть могут все. Google и многие другие компании Веб 2.0 смогли разработать бизнес-модели, которые одновременно приносят прибыль и предоставляют возможности для творческого развития Интернета.

Защита Интернета как глобального общественного блага [32]

Некоторые решения могут быть разработаны на основе существующих экономических и правовых концепций. Например, в экономической теории существует хорошо развитая концепция общественных благ, которая на международном уровне была расширена до концепции глобальных общественных благ. Общественное благо имеет две важные характеристики: неконкурентное потребление и неисключительность. Первая

подразумевает, что потребление блага одним индивидом никаким образом не умаляет потребление этого блага другим; вторая означает, что помешать какому-либо лицу пользоваться благом сложно, если вообще возможно. Доступ к материалам Интернета и многим интернет-сервисам соответствует обоим критериям: неконкурентности в потреблении и неисключительности в предоставлении.

ПРАВА ЛЮДЕЙ С ОГРАНИЧЕННЫМИ ФИЗИЧЕСКИМИ ВОЗМОЖНОСТЯМИ [33]

По оценкам ООН, в мире насчитывается 500 миллионов людей с ограниченными возможностями. Это число постоянно возрастает из-за войн, неблагоприятныхе условия жизни, отсутствия знаний о болезнях, их причинах, предотвращении и лечении [34]. Интернет дает новые возможности для включения инвалидов в жизнь общества. Чтобы максимизировать потенциал технологий с точки зрения помощи людям с ограниченными возможностями, необходима разработка соответствующей модели управления Интернетом. Основным международным инструментом в этой области является Конвенция о правах инвалидов, принятая ООН в 2006 г. и уже подписанная 139 странами. Закрепленные в этой Конвенции права сейчас включаются в национальные системы законодательства, что через несколько лет сделает возможным обеспечение их соблюдения [35].

Осознание необходимости учитывать потребности людей с ограниченными возможностями при проектировании технологических решений постепенно растет благодаря работе таких организаций, как Динамическая коалиция IGF по вопросам доступа и ограниченных возможностей [36] и Секция по ограниченным возможностям и специальным потребностям Общества Интернета [37].

Инвалиды часто лишены способностей, необходимых для использования оборудования, программного обеспечения и материалов Интернета. Создать соответствующие возможности можно за счет работы в двух направлениях. Во-первых, необходимо включать стандарты доступности в требования к дизайну оборудования, ПО и материалов. Во-вторых, нужно повышать доступность дополнительного оборудования и ПО, усиливающих или заменяющих определенные физические способности пользователя.

С точки зрения управления Интернетом в центре внимания находятся контент и сервисы, поскольку их объем и количество быстро увеличиваются и в совокупности они создают своего рода инфраструктуру. Многие веб-приложения не соответствуют стандартам доступности из-за низкой осведомленности их разработчиков и не соответствующих сегодняшним реалиям представлений о якобы высокой цене и сложности необходимых

решений. Международные стандарты доступности для Интернета были разработаны Консорциумом «всемирной паутины» (W3C) и называются «Руководство по доступности веб-контента» [38].

Одна из инициатив, призванных расширить доступ людей с ограниченными возможностями к материалам и сервисам глобальной сети — «Универсальный дизайн Интернета», предложенный Обществом Интернета (Internet Society) и определяемый так: «Универсальный дизайн Интернета означает обеспечение достаточной гибкости с точки зрения представления материалов и технологического дизайна, чтобы учитывались потребности максимально широкой пользовательской аудитории, независимо от возраста, языка, физических способностей» [39].

ОБРАЗОВАНИЕ

Интернет открыл новые возможности для образования. Постоянно появляются разнообразные инициативы в области электронного образования, онлайн-образования, дистанционного образования, основной целью которых является использование Интернета как средства обучения. Хотя онлайн-образование не может заменить традиционного обучения, оно предоставляет новые возможности в тех случаях, когда время или расстояние затрудняют непосредственное (очное) посещение занятий. По некоторым оценкам, рынок онлайн-образования будет расти и к 2010 г. достигнет приблизительно 10 млрд долларов США.

Традиционно нормативные рамки в сфере образования устанавливались государственными структурами. Аккредитация образовательных учреждений, признание степеней и обеспечение качества образования регулируются на государственном уровне. Однако международное образование требует создания новых режимов управления. Многие международные инициативы стремятся заполнить существующий вакуум в области управления, особенно в части контроля качества и признания дипломов и степеней.

ВОПРОСЫ

ВТО и образование

Одним из противоречивых аспектов переговоров в рамках ВТО является интерпретация статей 1(3) (b) и (c) Генерального соглашения по

торговле услугами (GATS), которое предусматривает исключения из режима свободной торговли для услуг, предоставляемых государством. В соответствии с точкой зрения, поддерживаемой в основном США и Великобританией, эти исключения должны трактоваться в узком смысле и де-факто в области высшего образования должна осуществляться свободная торговля. Подобный подход продиктован главным образом заинтересованностью образовательного сектора США и Великобритании в формировании глобального рынка образовательных услуг, и он вызывает целый ряд возражений со стороны других стран.

Будущие дискуссии в рамках ВТО и других международных организаций, вероятно, будут вестись о сути образования: является ли оно товаром или общественным благом? Если рассматривать образование как товар, то правила свободной торговли, принятые ВТО, можно будет применять и в этой сфере. Если же относиться к образованию как к общественному благу, то сохранится ныне существующая модель образования, в соответствии с которой государственные университеты имеют особый статус учреждений, значимых для национальной культуры.

Обеспечение качества

Доступность инструментов, необходимых для предоставления услуг в области электронного образования, и легкость входа на этот рынок ставят целый ряд вопросов, связанных с контролем качества. Стремление представить как можно больше материалов онлайн может привести к пренебрежению качеством учебных материалов и дидактических методов. Кроме того, негативно повлиять на качество образования может целый ряд факторов. Одним из них является появление на рынке большого числа новых, главным образом коммерчески ориентированных образовательных учреждений, в большинстве своем не располагающих необходимыми академическим и дидактическими возможностями. Другая проблема обеспечения качества кроется в том, что при простом переносе существующих материалов с бумажных носителей в онлайн-среду ее дидактический потенциал не используется.

Признание академических степеней и создание общей системы зачетных единиц

Применительно к области онлайн-обучения особую значимость имеет вопрос о признании степеней. Основной задачей здесь выступает обеспечение признания дипломов и степеней за пределами конкретного региона, в первую очередь на глобальном уровне.

ЕС начал разработку такой нормативной базы в виде Европейской системы взаимозачета кредитов. Азиатско-Тихоокеанский регион следу-

ет примеру Европы, создавая свою собственную региональную модель для обмена студентами и систему зачетных единиц (UCTS).

Стандартизация онлайн-обучения

Начальный этап развития онлайн-обучения характеризовался быстрым развитием и большим разнообразием материалов с точки зрения технических платформ, содержания и дидактики. Однако существует необходимость выработки общих стандартов с целью облегчения обмена онлайн-курсами и внедрения определенного стандарта качества.

Наибольший объем работы по стандартизации выполняется в США частными и профессиональными учреждениями. Другие инициативы, включая международные, гораздо менее масштабны.

БЕЗОПАСНОСТЬ ДЕТЕЙ В ИНТЕРНЕТЕ [40]

Дети часто оказываются в роли жертв. Большинство вопросов, связанных с безопасностью в Интернете, в значительной степени касаются молодежи, особенно несовершеннолетних. Граница между допустимым и недопустимым становится особенно очевидной, когда речь заходит о безопасности детей.

«*Киберзапугивание*». Домогательство является особенно значительной проблемой, когда его объектом становятся несовершеннолетние. Дети и молодежь, наиболее активные пользователи разнообразных средств коммуникации, таких как системы обмена сообщениями, чаты и социальные сети, оказываются наиболее уязвимыми. Дети легко становятся жертвами запугивания в Интернете — особенно часто со стороны сверстников, использующих в качестве инструментов различные информационно-коммуникационные технологии.

Насилие и сексуальная эксплуатация. Эти действия, направленные на несовершеннолетних, особенно опасны, если их совершают взрослые. Наиболее часто интернет-педофилы скрывают свою истинную личность и, притворяясь сверстниками, собирают информацию и постепенно стараются завоевать доверие ребенка и даже договориться о реальной встрече. Таким образом, виртуальные действия превращаются в реальный контакт и могут привести к таким последствиям, как насилие и эксплуатация детей, педофилия, вовлечение несовершеннолетних в сексуальные связи и даже торговля детьми.

Жестокие игры. Игры, основанные на насилии (обычно сетевые, многопользовательские), быстро занимают место «пассивных» жестоких фильмов. Влияние игр, основанных на насилии, на поведение молодежи является предметом жарких споров. Наиболее известные игры демонс-

трируют разнообразные виды оружия (как настоящие, так и вымышленные), кровопролитие и обычно считаются средством «снять стресс». Наиболее популярными играми для различных платформ, включая Microsoft Xbox, Nintendo DS, Nintendo Wii, PC, Playstation, PSP чаще всего оказываются «стрелялки» и другие жестокие игры.

Варианты решения проблем

Главная проблема, с которой сталкиваются педагоги и родители в контексте защиты детей в Интернете, заключается в том, что «цифровое поколение» гораздо больше знает об информационных технологиях — и при этом гораздо хуже понимает их возможные последствия. В этих условиях возрастает значение сотрудничества сверстников, родителей, педагогов и сообщества в целом. Родители, лица, принимающие решения, и представители общественности по всему миру постепенно признают наличие вышеназванных проблем и инициируют различные шаги, направленные на защиту детей в «цифровой окружающей среде».

Чтобы повысить уровень осведомленности различных заинтересованных сторон, Европейская комиссия реализует проект InSafe по созданию общеевропейской сети центров по вопросам безопасности в Интернете (e-safety). В рамках проекта подготовлено большое количество образовательных и информационных материалов на различных языках для родителей и педагогов; все этим материалы доступны для скачивания и свободного распространения. Польские СМИ провели кампанию против запугивания в Интернете, результатом которой стала серия видеоклипов и дистанционный обучающий курс для детей по безопасности в Интернете. Одной из первых инициатив по безопасности в Интернете на национальном уровне является проект NetSafe, реализуемый в Новой Зеландии с 1998 г. с участием министерств, бизнеса и СМИ.

Одной из наиболее успешных моделей информационно-образовательных кампаний на национальном уровне является инициатива «Кибермир» (Cyber-Peace Initiative), созданная в Египте под эгидой Международного движения женщин за мир, председателем которого является Сюзанна Мубарак. Была создана и обучена проведению и управлению соответствующими проектами группа молодых энтузиастов под названием «Net-Aman», а также группа, в состав которой вошли родители. Совместно с партнерами, в том числе Министерством телекоммуникаций Египта, местным подразделением Microsoft, а также международными организациями (ChildNet International), за последние несколько лет они провели работу с десятками тысяч молодых людей и их родителей по всей стране. Кроме того, они подготовили несколько наборов информационно-образовательных материалов на арабском языке для детей, их родителей и педагогов.

С учетом встречи IGF в Египте в 2009 г. вполне вероятно, что эта модель получит широкую известность и будет использована в других странах.

Помимо обучения молодежи, родителей и педагогов, необходимо повышение квалификации лиц, принимающих решения по обеспечению интернет-безопасности: чиновников, сотрудников частных компаний, неправительственных организаций и СМИ, представителей академического сообщества и «мозговых центров». Различные международные организации, в том числе Совет Европы, МСЭ, «Кибермир» и DiploFoundation, обсуждают возможные модели сотрудничества по созданию таких программ.

В долгосрочной перспективе также необходимо обновление учебных планов и программ и включение в процесс обучения на уровне школ таких вопросов безопасности в Интернете, как защита личных данных, обеспечение безопасности, внимание к собственной и чужой репутации онлайн, вопросы этики, реагирование на преступное поведение и т. д. Ряд подобных инициатив уже существуют — в их числе Cyber Smart!, iKeepSafe, i-Safe и NetSmartz.

Неотъемлемым компонентом обеспечения безопасности детей в Интернете является координация национальных и международных правовых и политических механизмов. Недавним примером является успех общеевропейской «Пражской декларации за безопасный Интернет для детей», принятой на конференции министров ЕС в апреле 2009 г. МСЭ включило инициативу по защите детей онлайн в свою «Глобальную повестку дня в области кибербезопасности». Кроме того, защита детей входит в повестку дня и активно обсуждается на многих международных форумах, включая IGF, в рамках которого функционирует Динамическая коалиция по безопасности детей онлайн.

Успешным примером международного сотрудничества в области защиты детей также являются давно существующие международные «горячие линии», среди которых:

- проект по борьбе с распространением в Интернете материалов, связанных с эксплуатацией детей (CIRCAMP), инициированный Целевой группой руководителей полицейских сил стран Евросоюза;
- деятельность и сотрудничество с государственными органами неправительственных организаций, таких, как Internet Watch Foundation, Perverted Justice Foundation, ICMEC, ECPAT, Save the Children, Internet Content Rating Association, Child Exploitation and Online Protection Centre;
- частно-государственные партнерства, примером которых является сотрудничество между компанией Norway Telecom и полицией Норвегии.

ПРИМЕЧАНИЯ

[1] Хартия АПК включает следующие положения: доступ к Интернету для всех; свобода собраний и выражения убеждений; доступ к знаниям; сотрудничество в обучении и творчестве — разработка свободного программного обеспечения и других технологий с открытым кодом; защита частной жизни, защита от слежки, шифрование данных; управление Интернетом; знание, защита и реализация своих прав. Дополнительную информацию см.: http://www.apc.org/en/node/5677

[2] Более подробную информацию см.: http://www.globalnetworkinitiative.org

[3] Адрес в Интернете: http://conventions.coe.int/treaty/EN/Treaties/html/005.htm

[4] Совет Европы принял следующие основные декларации, связанные с правами человека и Интернетом: Декларация о свободе коммуникаций в Интернете (28 мая 2003 г.), Декларация о правах человека и верховенстве закона в информационном обществе (13 мая 2005 г.)

[5] Больше информации можно получить на сайте: http://www.freedomhouse.org/uploads/specialreports/NetFreedom2009/FreedomOnTheNet_FullReport.pdf

[6] Timothy Zick (1999). Congress, the Internet, and the intractable pornography problem: the Child Online Protection Act of 1998, Creighton Law Review, 32, pp. 1147, 1153, 1201.

[7] Обсуждение проблемы азартных игр в Интернете, см.: Jenna F. Karadbil (2000), Note: Casinos of the next millennium: a look into the proposed ban on internet gambling, Arizona Journal of International and Comparative Law, 17, 413, 437-38.

[8] См. доклад «Интернет под наблюдением» (“Internet Under Surveillance”). Адрес в Интернете: http://www.rsf.org/rubrique.php3?id_rubrique=433.

[9] Jonathan Zittrain and Benjamin Edelman, Documentation of Internet filtering worldwide (Open Net Initiative): http://cyber.law.harvard.edu/filtering/.

[10] Власти Китая используют блокирование IP-адресов. Официальная фильтрация материалов Интернета в Саудовской Аравии осуществляется через систему прокси-серверов. Дополнительную информацию см.: http://www.isu.net.sa/saudi-internet/contenet-filtring/filtring-mechanism.htm.

[11] См.: Electronic Frontiers, Australia, “Internet censorship in Australia” (20 December 2002), http://www.efa.org.au/Issues/Censor/cens1.html.

[12] Дополнительную информацию об «интернет-платформе для выбора контента» (Platform for Internet Content Selection, PICS), см.: http://www.w3.org/PICS/iacwcv2.htm.

[13] Хотя Винт Серф являлся участником группы экспертов, он выразил несогласие с итоговым докладом, который, по его словам «не уделил внимания проблемам, связанным с использованием онлайн-фильтров, и глобальным последствиям этих действий». Источник: “Welcome to the world wide web, passport, please?”, New York Times, 15 March 2001 (адрес в Интернете: http://www.quova.com/page.php?id=33&coverage_id=86).

[14] По словам представителей компании Akamai, ее программное обеспечение может определить географическое положение пользователя с точностью до почтового индекса. Бóльшая точность технологически невозможна. Информацию об адресе пользователя нельзя получить на основе IP-адреса. «Silicon Valleys Quova Inc., один из ведущих поставщиков такого рода технологий, заявляет, что может определить страну пользователя в 98 % случаев, а город — если это большой город — в 85 % случаев. Независимые исследования оценивают точность таких программ, также поставляемых компаниями InfoSplit, Digital Envoy, Netgeo и др., на уровне 70—90 %». См.: "Rise of internet borders prompts fears of web's future" by Arianna Eunjung Cha, Washington Post, January 4, 2002, p. E01.

[15] Обзор публикаций по теме см.: http://searchenginewatch.com/sereport/article.php/2165031.

[16] Опубликовано в интернет-версии журнала New Scientist: http://www.newscientist.com/news/news.jsp?id=ns99992797.

[17] См. Jonathan Zittrain and Benjamin Edelman, Localised Google search result exclusions: statement of issues and call for data (адрес в Интернете: http://cyber.law.harvard.edu/filtering/google/).

[18] "Will all of us get our 15 minutes on a YouTube video?" by Lee Gomes. The Wall Street Journal. August 30, 2006 (адрес в Интернете: http://online.wsj.com/public/article/SB115689298168048904-5wWyrSwyn6RfVfz9NwLk774VUWc_20070829.html?mod=rss_free).

[19] EU Information Society, "Safer internet action plan" (адрес в Интернете: http://europa.eu.int/information_society/programmes/iap/index_en.htm).

[20] См.: Church of Scientology censors net access for members (адрес в Интернете: http://www.xenu.net/archive/events/censorship).

[21] Ценные комментарии и идеи для этого раздела предоставила Катитца Родригес (Katitza Rodriguez).

[22] Доклад Американского союза за гражданские права (American Civil Liberties Union): Jay Stanley (2004). The surveillance-industrial complex: How the American government is conscripting businesses and individuals in the construction of a) surveillance society (адрес в Интернете: http://www.aclu.org/FilesPDFs/surveillance_report.pdf).

[23] Текст «Патриотического акта» см.: http://www.epic.org/privacy/terrorism/hr3162.html.

[24] Обсуждение проблемы доверия пользователей с точки зрения защиты личных данных компаниями см. в: Rick Whiting. Wary customers don't trust business to protect privacy, Information Week, August 19, 2002 (адрес в Интернете: http://www.informationweek.com/shared/printableArticle.jhtml?articleID=6503045).

[25] Council of Europe, Convention for the protection of individuals with regard to the automatic processing of personal data, ETS No. 108 (адрес в Интернете: http://conventions.coe.int/Treaty/en/Treaties/Html/108.htm).

[26] Gramm-Leach-Bliley Act, Public Law (адрес в Интернете: http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=106_cong_public_laws&docid=f:publ102.106).

[27] Children's Online Privacy Protection Act (адрес в Интернете: http://www.ftc.gov/ogc/coppa1.pdf U.S.C. §§ 6501-6505).

[28] Health Insurance Portability and Accountability Act of 1996, Public Law 104-191, § 264; Department of Health and Human Services, Standards for Privacy of Individually Identifiable Health Information; Proposed Rule, 64 Fed. Reg. 59917, (адрес в Интернете: http://www.epic.org/privacy/medical/HHS_medical_privacy_regs.html).

[29] Galexia, the US Safe Harbour — Fact or Fiction?, 2008

[30] Дополнительную информацию о многоязычии в Интернете см.: Qusai AlShatti, Raquel Aquirre and Veronica Cretu. Multilingualism — the communication bridge. DiploFoundation's Internet Governance Research Project, 2006/2007 (адрес в Интернете: http://textus.diplomacy.edu/thina/TxFsetW.asp?tURL=http://textus.diplomacy.edu/thina/txgetxdoc.asp?IDconv=3241).

[31] См.: http://en.wikipedia.org/wiki/English_in_computing#English_on_the_World_Wide_Web.

[32] Дополнительную информацию об Интернете как глобальном общественном благе см.: Seiiti Arata and Stephanie Psaila. Protection of Public Interest on the Internet. DiploFoundation's Internet Governance Research Project, 2005/2006 (адрес в Интернете: http://www.diplomacy.edu/ig/Research/display.asp?Topic=Research%20Themes%20II#Protection).

[33] Ценные комментарии и идеи для этого раздела предоставил Хорхе Плано (Jorge Plano).

[34] См.: http://www.hrea.org/index.php?base_id=152

[35] См.: http://www.un.org/disabilities/

[36] См.: http://www.intgovforum.org/cms/index.php/dynamic-coalitions/80-accessibility-and-disability and http://www.itu.int/themes/accessibility/dc/

[37] См.: http://www.isocdisab.org

[38] См.: http://www.w3.org/TR/WCAG10/

[39] См.: http://www.isoc.org/briefings/002/isocbriefing02.txt

[40] Этот текст был подготовлен Владимиром Радуновичем (Vladimir Radunovic) для курса по кибербезопасности и безопасности в Интернете DiploFoundation (Advanced Course on Cybersecurity and Internet Safety, Internet Governance Capacity Building Program).

Раздел 7

Участники процесса управления Интернетом

УЧАСТНИКИ ПРОЦЕССА УПРАВЛЕНИЯ ИНТЕРНЕТОМ

Отличительной чертой управления Интернетом всегда было участие в нем различных заинтересованных сторон. Такая «многосторонность» вполне естественна — ведь негосударственные субъекты принимали основное участие в создании и поддержании функционирования Интернета. Гражданское общество и особенно академические круги играли ключевую роль в становлении Интернета, включая разработку протоколов, создание контента и построение онлайн-сообществ. Усилиями бизнеса в ответ на растущие потребности создавалась технологическая инфраструктура: компьютеры, сети, программное обеспечение. Правительства же оказались на поле управления Интернетом новичками [1].

Основные отличие между переговорами по управлению Интернетом и другими глобальными переговорами, например, в сфере охраны окружающей среды, заключается в том, что если в других случаях межправительственные режимы постепенно «открывались» для негосударственных игроков, в переговорах по управлению Интернетом правительствам пришлось включаться в уже существующий неправительственный режим, центром которого была ICANN. Когда вопросы управления Интернетом вышли на глобальный уровень, появилась необходимость интеграции этих двух режимов (неправительственного и традиционного дипломатического) путем создания многосторонней модели выработки политики.

Первым успешным экспериментом в этом направлении была Рабочая группа по управлению Интернетом (WGIG), созданная в процессе подготовки WSIS (2003—2005). WGIG представляла собой экспертную, совещательную группу, но не структуру, принимающую решения [2]. Она не готовила официальные документы ООН, однако существенно повлияла на переговоры по управлению Интернетом в ходе WSIS. WGIG была создана в результате компромисса между правительствами, поддерживающими ICANN, которые официально допустили появление вопросов управления Интернетом в многосторонней дипломатической

повестке дня, и другими правительствами — в основном развивающихся стран, — которые согласились с участием в процессе неправительственных субъектов. Результатом этого компромисса стал успех WGIG.

Уже после завершения WSIS управление Интернетом остается на глобальной повестке дня в виде Форума по управлению использованием Интернета, четвертая встреча которого состоялась в ноябре 2009 г. в Шарм-эш-Шейхе (Египет). Первая встреча прошла в Афинах (Греция) в 2006 г., вторая — в Рио-де-Жанейро (Бразилия) в 2007 г., третья — в Хайдарабаде (Индия) в 2008 г. Структура участия в IGF сходна с WGIG; эти структуры они остаются примерами многосторонних партнерств на международном уровне.

В этой главе обсуждается роль основных заинтересованных сторон в процессе управления Интернетом. Мы начнем с субъектов, официально признанных в процессе WSIS и WGIG, включая правительства, международные организации, гражданское общество и бизнес. Мы также кратко проанализируем роль других ключевых участников, в первую очередь интернет-сообщества и ICANN.

Управление Интернетом — подход с «переменной геометрией»

Управление Интернетом требует участия различных заинтересованных сторон, отличающихся по многим параметрам, включая международную правоспособность, заинтересованность в конкретных вопросах управления Интернетом и наличие экспертных знаний. Такое разнообразие можно интегрировать в единую модель управления Интернетом за счет использования подхода «с переменной геометрией». Этот подход, учитывающий интересы, приоритеты и возможности заинтересованных сторон в области решения вопросов управления Интернетом, нашел отражение в статье 49 Декларации принципов WSIS, определяющей следующие роли для основных заинтересованных сторон [3]:

- государства — «политические полномочия по связанным с Интернетом вопросам государственной политики» (включая международные аспекты);
- частный сектор — «развитие Интернета как в технической, так и в экономической сфере»;
- гражданское общество — «важная роль в относящихся к Интернету вопросах, в особенности на уровне общин»;
- межправительственные организации — «координация связанных с Интернетом вопросов государственной политики»;
- международные организации — «разработка относящихся к Интернету технических стандартов и соответствующей политики».

ГОСУДАРСТВА

Последние шесть лет — после появления вопросов управления Интернетом в политической повестке дня в 2003 г. — были для многих государств временем обучения. Даже для крупных и богатых стран участие в решении вопросов управления Интернетом связано с многочисленными

сложностями, в том числе из-за междисциплинарной природы управления Интернетом (технологические, социальные, экономические аспекты) и большого разнообразия участвующих в этом процессе субъектов. Многим государствам пришлось постигать этот новый для них вопрос «на ходу»: обучать чиновников, вырабатывать политику и активно участвовать в различных форумах по управлению Интернетом. В этой главе мы рассмотрим основные проблемы в области управления Интернетом с точки зрения государств.

Координация на уровне государства

В 2003 г., в начале процесса WSIS, в большинстве стран вопросами управления Интернетом занимались «технические» министерства, обычно те, в чьем ведении находились отношения с Международным союзом электросвязи (МСЭ). Постепенно, по мере осознания того, что управление Интернетом — это больше, чем «провода и кабели», правительства начали включать в него представителей других министерств, например, культуры, СМИ, юстиции. Разнообразие вопросов управления Интернетом также обусловило то, что ими занимались самые разные субъекты, такие как ICANN и организации технической стандартизации.

Основной сложностью для многих государств стала разработка стратегии, направленной на получение и координацию поддержки негосударственных субъектов, обладающих необходимыми для решения вопросов управления Интернетом знаниями — университетов, частных компаний, неправительственных организаций. В ходе WSIS большинству крупных и средних государств удалось приобрести необходимый институциональный потенциал для мониторинга глобальных переговоров по управлению Интернетом. Некоторые из них, такие как Бразилия, создали инновационные национальные структуры, следящие за дискуссиями по управлению Интернетом [4].

Согласованность политических курсов

Учитывая многодисциплинарную природу управления Интернетом и высокую степень разнообразия участников и площадок обсуждения, достижение согласованности политических курсов в этой сфере является крайней сложным. Это управленческая проблема, требующая от правительств гибкого подхода к координации процесса выработки политики, включая горизонтальную коммуникацию между различными министерствами, бизнес-кругами и другими субъектами. Традиционная правительственная структура, построенная по иерархическому принципу, может быть препятствием для такой гибкой координации.

«Телеграфная геостратегия» и политическая (не)согласованность

Англо-французский союз (Антанта) был создан в 1904 г. Однако французское Министерство телеграфов не последовало общему политическому курсу страны, установив тесное сотрудничество с Германией. Основной целью этого было уменьшить британское доминирование в глобальной «телеграфной геостратегии» за счет сотрудничества с Германией в прокладке телеграфных кабелей. Французский историк Шарль Лезаж так прокомментировал эту политическую (не)согласованность: «Длительное расхождение между общими принципами французской дипломатии и действиями в области телеграфа, на мой взгляд, является следствием того, что в этой стране у каждого министерства своя внешняя политика: одна у Министерства иностранных дел, другая — у Министерства финансов… У Администрации почт и телеграфов тоже время от времени имеется своя внешняя политика; и получилось так, что в эти последние годы, не будучи враждебной к Англии, она продемонстрировала сильную склонность к Германии» [5].

Помимо чисто управленческих сложностей возможность согласовать политические курсы часто ограничена существованием конкурирующих политических интересов. Это особенно справедливо в отношении стран с развитой и разнообразной интернет-экономикой. Недавний пример — дискуссии по вопросу о сетевой нейтральности, в которых правительству США пришлось балансировать между активными сторонниками сетевой нейтральности из числа интернет-компаний (Google, Yahoo!) и сектором телекоммуникаций/развлечений (Verizon, AT&T, голливудское лобби), который рассматривает сетевую нейтральность как препятствие на пути создания более быстрого Интернета для доставки пользователям мультимедийных материалов.

Конвергенция различных медиа дает еще один стимул к достижению согласованности политических курсов. Различным областям регулирования (телекоммуникации, теле- и радиовещание) придется прийти к «общему знаменателю», чтобы не отстать от процесса сближения технологий.

Важность постоянных миссий в Женеве

Для многих государств постоянные миссии в Женеве были важными, если не сказать ключевыми, игроками в процессе WSIS и управления Интернетом в целом. Большая часть активности происходила в Женеве, где расположена штаб-квартира МСЭ, игравшего основную роль в процессе. Первый саммит WSIS в 2003 г. состоялся в Женеве, и все, кроме одной, подготовительные встречи прошли там же, благодаря чему постоянные миссии в Женеве все время были вовлечены в процесс. На сегодняшний день секретариат IGF располагается в Женеве; здесь же проходят все подготовительные встречи IGF.

Для крупных развитых стран постоянные миссии были частью широкой сети организаций и индивидов, участвовавших во WSIS и

процессе управления Интернетом. Для небольших и развивающихся государств постоянные миссии были основными — а иногда и единственными — участниками процесса. «Портфель» WSIS добавился к повестке дня обычно маленьких и без того перегруженных миссий развивающихся стран. Нередко один и тот же дипломат был вынужден выполнять задачи, связанные с WSIS, наряду с другими обязанностями в таких областях, как права человека, здравоохранение, торговля, охрана труда.

«Дипломатизация» процесса управления Интернетом

Важным для позиции правительств в ходе WSIS было и то, что этот саммит включил Интернет в глобальную повестку дня. До WSIS Интернет обсуждался преимущественно в неправительственных кругах или на внутригосударственном уровне. «Дипломатизация» политических аспектов Интернета вызвала различную реакцию. Кеннет Нил Кукьер, технологический обозреватель журнала «The Economist», подчеркивал негативный аспект «дипломатизации» дискуссий по управлению Интернетом: «…повышение уровня обсуждения проблемы до формального саммита ООН естественно повышает важность темы в правительственных кругах. В результате тематика информационного общества, которой — как вопросами научно-технической политики, СМИ или культуры — занимались менее политизированные и менее заметные правительственные структуры, была передана министерствам иностранных дел и опытным дипломатам, более привыкшим к силовой политике и менее осведомленным о технических аспектах и внутренне присущей Интернету необходимости сотрудничества и взаимозависимости» [6].

Дипломатизация процесса имела и определенные положительные последствия для дискуссий в ходе WSIS. Например, дипломаты высказали непредвзятые комментарии по таким давним проблемам, связанным с Корпорацией по присвоению имен и номеров в Интернете, как доменные имена, IP-адреса и корневые серверы. Вклад дипломатов был особенно заметен в дебатах WGIG. Дипломаты-лидеры WGIG (председатель Нитин Десаи и исполнительный директор Маркус Куммер) создали атмосферу участия, в которой различия между членами группы, включая представителей технического сообщества, не блокировали процесс. Результатом работы WGIG стал Итоговый отчет, в котором отмечались разногласия, но предлагалось и решение относительно процесса будущих дискуссий в виде Форума по управлению использованием Интернета.

ПОЗИЦИЯ ПРАВИТЕЛЬСТВА США

Интернет был разработан в рамках проекта, финансировавшегося правительством США. Со времени появления глобальной сети до сегодняшнего дня правительство США участвовало в управлении Интернетом через различные министерства и ведомства: сначала Министерство обороны, затем Национальный фонд науки, и, наконец, Министерство торговли. Федеральная комиссия по связи также сыграла важную роль в создании нормативно-правовой базы для развития Интернета.

Одной из отличительных черт участия правительства США была политика невмешательства, обычно называемая «отдаленный опекун». Американские власти задавали лишь общие рамки, оставляя управление Интернетом в ведении тех, кто с ним непосредственно работает, в первую очередь интернет-сообщества. Однако в некоторых случаях правительство США вмешивалось в процесс более явным образом — например, как это случилось в середине 1990-х гг., когда в рамках проекта CORE[1] корневые серверы и управление ключевыми ресурсами Интернета могли быть перенесены из США в Женеву. Этот процесс был остановлен знаменитой, по крайней мере в истории Интернета, дипломатической нотой, направленной государственным секретарем США Мадлен Олбрайт Генеральному секретарю МСЭ [7]. Параллельно с остановкой инициативы CORE правительство США начало консультации, результатом которых стало создание ICANN.

С момента создания ICANN правительство США заявляло о своем намерении прекратить контролировать ICANN, как только эта организация станет институционально и функционально устойчивой. Этот процесс был начат в октябре 2009 г. с подписания Министерством торговли США «Подтверждения обязательств». Согласно этому документу, ICANN станет независимой организацией. Другой элемент особых отношений между Министерством торговли и ICANN — так называемое соглашение по IANA[2] — будет пересмотрен в 2011 г.

На глобальном уровне в ходе WSIS США возражало против возможной передачи функций ICANN межправительственной структуре. Однако тогда же американское правительство сделало первые шаги в сторону интернационализации ICANN, признав право правительств государств

---

[1] CORE — неправительственная организация, ассоциация регистраторов доменных имен (http://www.corenic.org/). — ***Примеч. перев.***

[2] Internet Assigned Numbers Authority (Администрация присвоения номеров в Интернете) — контролируемая ICANN структура, занимающаяся решением отдельных технических вопросов, связанных с доменными именами, IP-адресами и интернет-протоколами (http://www.iana.org). — ***Примеч. перев.***

на соответствующие доменные имена и согласившись с продолжением международных дискуссий в форме создания IGF.

ПОЗИЦИЯ ДРУГИХ ГОСУДАРСТВ

Политический спектр управления Интернетом начал формироваться недавно, по мере того, как правительства разных стран формулировали свои позиции. Согласно одной из крайних точек зрения, Интернетом должна управлять такая межправительственная организация, как МСЭ. Такова была изначальная позиция развивающихся стран. Наиболее активно за укрепление роли МСЭ выступали Китай, Иран, Россия и Бразилия. Некоторые развивающиеся страны предлагали создать вместо МСЭ новую международную организацию («Международную организацию Интернета»), возможно, даже на основе нового международного договора. Другие страны подчеркивали, что Интернетом должна управлять организация нового типа, включающая различные заинтересованные стороны.

В центре политического спектра находятся государства, выступающие за сохранение технических функций за ICANN и создание новой международной структуры, осуществляющей контроль над политическими аспектами. Эту позицию постепенно занял Европейский Союз. Наконец, на другом конце спектра находятся США, утверждающие, что существующий режим, основанный на ICANN, не нуждается в изменении. Канада, Австралия и Новая Зеландия высказывали сходные мнения, выступая в то же время за бóльшую интернационализацию ICANN. Эти государства вместе с ЕС, Швейцарией и некоторыми развивающимися странами сыграли важную роль в достижении компромиссных решений по управлению Интернетом в рамках WSIS.

ПОЗИЦИЯ МАЛЫХ ГОСУДАРСТВ

Сложность вопросов и динамика деятельности в процессе управления Интернетом не позволяли небольшим государствам, в особенности развивающимся, следить за происходящим, а тем более оказывать на процесс сколько-либо значительное влияние. В результате, многие малые государства поддержали в отношении управления Интернетом принцип «одного окна» [8]. Количество пунктов повестки дня и ограниченный потенциал развивающихся стран (как в самой стране, так и в ее дипломатических представительствах) остаются важными препятствиями для их полноценного участия в процессе управления Интернетом. Необходимость развивать потенциал в данной сфере была признана в качестве приоритета в Тунисской программе для информационного общества WSIS.

БИЗНЕС [9]

Когда в 1998 г. была создана ICANN, одной из центральных проблем с точки зрения бизнес-сообщества была защита торговых марок. Многие компании сталкивались с проблемами киберсквоттинга и неправомерного использования своих торговых марок людьми, которые успели первыми зарегистрировать соответствующие доменные имена. В процессе создания ICANN бизнес-круги явно обозначили защиту торговых марок в качестве приоритета и, соответственно, сразу после своего появления эта организация занялась вопросами защиты торговых марок [10].

Сегодня по мере распространения Интернета возрос и интерес бизнеса к управлению глобальной сетью. С этой точки зрения компании можно разделить на следующие основные группы: компании, занимающиеся доменными именами; поставщики интернет-услуг; телекоммуникационные компании; разработчики программного обеспечения и компании, производящие контент для Интернета.

Компании, занимающиеся доменными именами, включают в себя регистраторов и регистратуры различного уровня, продающие доменные имена в Интернете (например, .com, .edu). Среди основных игроков в этом секторе — компании VeriSign и Affilias. На их деятельность непосредственно влияют политические решения, принимаемые ICANN в таких областях, как создание новых доменов верхнего уровня и разрешение споров. Поэтому эти компании наиболее заинтересованы в процессе выработки политики в ICANN. Они также участвовали в более широком процессе управления Интернетом (WSIS, WGIG, IGF), в основном для того, чтобы снизить риск присвоения функций ICANN другими участниками, особенно правительствами и международными организациями.

Поставщики интернет-услуг (провайдеры) — компании или организации, с помощью которых конечные пользователи получают доступ в Интернет. Поскольку провайдеры являются ключевыми посредниками при работе в сети, они особенно важны с точки зрения управления Интернетом. Их основное участие в этом процессе происходит на национальном уровне в виде взаимодействия с правительственными органами и ведомствами. На глобальном уровне некоторые провайдеры, особенно из США и Европы, активно участвовали в WSIS/WGIG/IGF как индивидуально, так и через посредников — Международную торговую палату, национальные, региональные и отраслевые бизнес-организации, такие как Европейская

Международная торговая палата (МТП) позиционировала себя как одного из ключевых представителей бизнеса в глобальных процессах управления Интернетом. МТП активно участвовала в переговорах WGIG и WSIS на ранних этапах и продолжает вносить активный вклад в процесс IGF.

ассоциация операторов телекоммуникационных сетей (ETNO), Американская ассоциация информационных технологий (ITAA) и др.

Телекоммуникационные компании обеспечивают передачу интернет-трафика и обслуживают интернет-инфраструктуру. Среди основных игроков в этом сегменте — такие компании, как Verizon и AT&T. Телекоммуникационные компании традиционно участвовали в выработке международной политики в области электросвязи через МСЭ. Они все более активно вовлекаются в деятельность ICANN и IGF. Их основной интерес с точки зрения управления Интернетом — гарантировать благоприятную среду для бизнеса, позволяющую развивать телекоммуникационную инфраструктуру Интернета.

Компании, производящие программное обеспечение, такие как Microsoft, Adobe и Oracle, в основном участвуют в деятельности различных организаций по стандартизации (W3C, IETF). На ранних этапах процесса WSIS основную озабоченность у них вызывала возможность начала дискуссий по правам интеллектуальной собственности в Интернете. Как выразился один из представителей этого сектора, их целью было «предупреждение аварий». Когда стало ясно, что WSIS не будет заниматься вопросами прав интеллектуальной собственности, интерес производителей ПО к участию в этом процессе снизился. Эта тенденция продолжилась и после WSIS.

Последняя группа участников, обозначенная как «*компании, производящие контент*», включает в себя основные бренды Интернета, такие как Google, Yahoo! и Facebook. Эта группа компаний становится все более важной по мере развития сервисов Веб 2.0. Их приоритеты тесно связаны с различными проблемами управления Интернетом, в частности, интеллектуальной собственностью, защитой конфиденциальности и кибербезопасностью, а их участие в процессе управления Интернетом становится все более заметным.

ГРАЖДАНСКОЕ ОБЩЕСТВО

Гражданское общество всегда было самим активным сторонником вовлечения различных участников в управление Интернетом. Традиционным поводом для критики участия гражданского общества на предыдущих многосторонних форумах было отсутствие надлежащей координации между его представителями и обилие разнообразных, часто противоречивых, позиций. Однако в процессе WSIS представители гражданского общества сумели справиться с присущей этому сектору сложностью и разнообразием, опираясь на несколько организационных форм, в том числе Бюро гражданского общества (Civil Society Bureau), Пленум гражданского общества (Civil Society Plenary) и тематические группы. Столкнувшись с

ограниченностью своих возможностей по влиянию на формальный процесс, группы гражданского общества разработали «двунаправленный» подход. Неправительственные организации (НПО) продолжали присутствовать в формальном процессе, используя имеющиеся возможности для участия и лоббирования правительств. Параллельно с этим они подготовили Декларацию гражданского общества — документ, альтернативный основной декларации, принятой на Женевской встрече WSIS.

Во WGIG гражданское общество было представлено более широко благодаря многосторонней природе Рабочей группы. Организации гражданского общества предложили восьмерых кандидатов для участия в WGIG, все из которых были впоследствии одобрены Генеральным секретарем ООН. Во время тунисского этапа WSIS основные усилия гражданского общества были перенесены на WGIG, где они сумели повлиять на многие принятые решения, в том числе, на решение создать Форум по управлению использованием Интернета (IGF) как пространство для обсуждения вопросов управления Интернетом с участием различных заинтересованных сторон.

Участие основных НПО (зарегистрированных при Экономическом и социальном совете ООН — ЭКОСОС) в работе WSIS было довольно ограниченным. Из почти 3000 НПО, имеющих консультативный статус при ЭКОСОС, лишь около 300 участвовали в WSIS.

МЕЖДУНАРОДНЫЕ ОРГАНИЗАЦИИ

МСЭ был основной международной организацией в процессе WSIS. Он организовывал работу Секретариата WSIS и участвовал в выработке политики по важнейшим вопросам. Участие МСЭ в процессе WSIS связано с активными попытками организации определить и укрепить свою позицию на быстро меняющейся арене глобальных телекоммуникаций, которая во все большей степени зависит от Интернета. Влиянию МСЭ в области глобальных телекоммуникаций угрожают, например, такие тенденции, как либерализация глобального рынка телекоммуникаций, проводимая в рамках ВТО, и перевод телефонного трафика с традиционных телекоммуникационных каналов в Интернет (с помощью технологии Voice over IP).

Возможность того, что по итогам WSIS МСЭ может де-факто стать «Международной организацией Интернета», вызвала озабоченность в США и ряде развитых стран, хотя получила поддержку некоторых развивающихся государств. На протяжении всего процесса WSIS эта перспектива создавала скрытое напряжение. В особенности это было заметно

в области управления Интернетом, где напряженность между ICANN и МСЭ существовала с момента создания ICANN в 1998 г. WSIS не ослабила эту напряженность. С учетом усиливающейся интеграции различных коммуникационных технологий, вполне вероятно, что вопрос о более значительной роли МСЭ в области управления Интернетом будет вновь появляться в политических дискуссиях.

Еще один вопрос касался «приземления» многодисциплинарной повестки дня WSIS в структуру специализированных агентств ООН. Нетехнические аспекты коммуникаций и интернет-технологий (социальные, экономические, культурные вопросы) входят в мандат других организаций ООН. Наиболее заметным игроком в этом контексте является ЮНЕСКО, которая занимается такими вопросами, как многоязычие, культурное разнообразие, общество знания и обмен информацией. В процессе WSIS значительные усилия были направлены на поддержание равновесия между МСЭ и другими организациями системы ООН. Оно сохраняется и в процессах, инициированных WSIS, основными участниками которых являются МСЭ, ЮНЕСКО и Программа развития ООН (ПРООН).

ДРУГИЕ УЧАСТНИКИ

Помимо формально признанных в рамках WSIS заинтересованных сторон, другие игроки — интернет-сообщество и ICANN — участвовали в процессе через механизмы гражданского общества и бизнес-сектора.

ИНТЕРНЕТ-СООБЩЕСТВО

Интернет-сообщество состоит из институтов и индивидов, развивавших и продвигавших Интернет с момента его появления. Исторически члены интернет-сообщества были связаны с вузами США, где они разрабатывали технические стандарты и основной функционал Интернета. В рамках этого сообщества также сложился традиционный «дух Интернета», основанный на принципах обмена ресурсами, открытого доступа и противодействия участию правительства в регулировании глобальной сети. Члены сообщества всегда защищали исконную концепцию Интернета от излишней коммерциализации и чрезмерного влияния правительства.

Наряду с термином «интернет-сообщество» для обозначения того же понятия используются и словосочетания «разработчики Интернета», «основатели Интернета», «отцы Интернета» и «технологи». Мы используем термин «интернет-сообщество», поскольку он предполагает более высокую степень согласия между членами относительно определенных ценностей. Эти разделяемые всеми ценности являются одной из отличительных черт сообщества.

В контексте международных отношений интернет-сообщество представляет собой эпистемическое сообщество [11]. На ранних этапах интернет-сообщество регулировалось несколькими, в основном неформализованными правилами и одной формальной процедурой — запросом комментариев (Request for Comments, RFC). Все основные стандарты Интернета описаны с помощью RFC. Несмотря на отсутствие строгих правил и формальной структуры, на ранних этапах интернет-сообщества регулировались силой традиций и влияния участников друг на друга. Большинство участников процесса разделяло общие ценности, приоритеты и отношение к ключевым проблемам.

Техническое регулирование глобальной сети силами интернет-сообщества было поставлено под вопрос в середине 1990-х гг., когда Интернет стал частью глобальной общественной и экономической жизни. Рост Интернета привел к появлению новых заинтересованных сторон (например бизнеса), которые привнесли иную профессиональную культуру и понимание того, что есть Интернет и как им управлять. Это привело к нарастанию напряженности. Так, в 1990-х годах интернет-сообщество и компания Network Solutions были вовлечены в так называемую войну DNS, конфликт по поводу контроля над корневыми серверами и системой доменных имен.

На сегодняшний день интернет-сообщество представлено Обществом Интернета (Internet Society, ISOC) и Рабочей группой по проектированию Интернета (Internet Engineering Task Force, IETF). ISOC сыграло важную роль в разработке и внедрении стандартов и продвижении ключевых ценностей Интернета, таких как открытость. Оно также активно участвует в развитии потенциала и помогает развивающимся странам, преимущественно африканским, создавать базовую интернет-инфраструктуру.

Интернет-сообщество было одним из важных участников процесса создания и функционирования ICANN. Один из создателей Интернета, Винт Серф, был председателем совета директоров этой организации. Члены интернет-сообщества занимают важные должности в различных структурах ICANN.

Однако сейчас модель выработки политики, ориентированная на интернет-сообщество, ставится под сомнение. Как указывают критики, по мере того как стирается грань между гражданами и пользователями Интернета, в управлении глобальной сетью требуется все большее участие правительств и других структур, представляющих граждан, а не только организаций пользователей — «интернет-сообщества». К этому аргументу особенно часто прибегают те, кто выступает за расширение роли правительств в управлении Интернетом.

Интернет-сообщество обычно обосновывает свою особую позицию в управлении Интернетом наличием специальных технических знаний. Его представители подчеркивают, что ICANN — в первую очередь техническая организация, поэтому ей должны управлять специалисты, опирающиеся на технические знания. Поскольку ограничить деятельность ICANN исключительно техническими вопросами становится все сложнее, это обоснование подвергается частой критике. Весьма вероятно, что члены интернет-сообщества постепенно включатся в другие ключевые группы участников, преимущественно гражданское общество и бизнес, но также и правительства. Хотя интернет-сообщество может исчезнуть как отдельная заинтересованная сторона, важно сохранить те ценности, которые оно продвигает: открытость, обмен знаниями и защиту интересов пользователей Интернета.

КОРПОРАЦИЯ ПО ПРИСВОЕНИЮ ИМЕН И НОМЕРОВ В ИНТЕРНЕТЕ (ICANN)

Корпорация по присвоению имен и номеров (ICANN) — основная структура управления Интернетом. В ее сферу ответственности входит управление системой доменных имен (DNS) — ключевой инфраструктурой Интернета, состоящей из IP-адресов, доменных имен и корневых серверов. Интерес к роли ICANN возрос вместе со стремительным ростом Интернета в 2000-е гг., и в ходе WSIS ICANN оказалась в поле внимания глобальных политических кругов.

Хотя ICANN является центральным участником процесса управления Интернетом, она не регулирует все аспекты Интернета, поэтому некорректно называть ее «правительством Интернета», как это иногда делают. ICANN управляет интернет-инфраструктурой, но не имеет полномочий в отношении других аспектов управления Интернетом, таких как кибербезопасность, контроль над контентом, защита авторских прав, защита конфиденциальности, поддержание культурного разнообразия или преодоление цифрового разрыва.

ICANN — некоммерческая корпорация, зарегистрированная в Калифорнии. Ее функциональные полномочия основаны на Меморандуме о взаимопонимании между Министерством торговли США и ICANN, подписанном в 1998 г. и дважды продленном (второй раз — с сентября 2006 г. по сентябрь 2009 г.). По состоянию на 1 октября 2009 г. формальной основой функционирования ICANN является «Подтверждение обязательств» (Affirmation of Commitments). Этот документ, подписанный ICANN и Министерством торговли США, служит основой превращения ICANN в независимую организацию.

ICANN является многосторонней организацией, включающей широкий спектр участников с разными полномочиями и ролями. Они делятся на четыре основные группы. Первая состоит из тех, кто участвовал в деятельности ICANN с момента ее создания: интернет-сообщества, бизнес-сообщества и правительства США. Вторая группа включает в себя межправительственные организации, среди которых наиболее важную роль играют Международный союз электросвязи и Всемирная организация интеллектуальной собственности. Третья группа состоит из национальных правительств, которые, начиная с WSIS в 2003 г., выражают желание играть более значимую роль в ICANN. Четвертая группа включает пользователей Интернета («сообщество всех»). ICANN экспериментировала с различными подходами, стараясь включить в процесс управления пользователей Интернета. На ранних этапах ее существования предпринимались попытки выбирать представителей пользователей в руководящие органы путем прямых выборов, что также было призвано укрепить правовую базу ICANN. Из-за низкой активности избирателей и нарушений в процессе прямые выборы не смогли обеспечить реальное представительство пользователей. В последнее время ICANN пытается вовлечь в свою деятельность пользователей Интернета через «представляющие всех» (at-large) структуры управления. Этот организационный эксперимент сейчас продолжается.

На процесс принятия решений в ICANN повлияли ранние модели управления Интернетом, основанные на принципах демократии, прозрачности, открытости и всеобщего участия. Основным различием между интернет-сообществом 1980-х гг. и сегодняшним контекстом принятия решения в ICANN является уровень «социального капитала». В прошлом интернет-сообщество обладало более высоким уровнем взаимного доверия и солидарности, что значительно упрощало процесс принятия решений и разрешения споров. Распространение Интернета привело к увеличению количества и разнообразия заинтересованных сторон; соответственно, уровень социального капитала среди этих участников весьма низок. Поэтому требование интернет-сообщества сохранить процедуры принятия решений, существовавшие на ранних этапах развития Интернета, по большей части утопично. Без опоры на социальный капитал единственным способом обеспечить функционирование процесса принятия решений является его формализация и разработка различных механизмов сдержек и противовесов.

Некоторые изменения процедур принятия решений, отражающие новые реалии, уже были сделаны. Наиболее важным из них является реформа ICANN в 2002 г., частью которой было усиление правительственного консультационного комитета и отказ от системы прямого голосования.

ВОПРОСЫ

Решение технических или политических вопросов?

Противоречие между решением технических и политических вопросов всегда создавало напряженность в деятельности ICANN. ICANN воспринимала себя как «техническую координационную структуру», которая занимается только техническими вопросами и не затрагивает политические аспекты Интернета. Официальные лица ICANN считали эту специфически техническую природу основным концептуальным аргументом в защиту уникального статуса и организационной структуры организации. Первый председатель ICANN Эстер Дайсон подчеркивала, что ICANN не стремится решать все вопросы управления Интернетом; по сути, она управляет инфраструктурой, а не людьми. Ее мандат жестко ограничен администрированием определенных (преимущественно технических) аспектов интернет-инфраструктуры в целом и DNS в частности [12].

Критики этого утверждения обычно указывают на то, что технически нейтральных решений не существует. В конечном итоге, каждое техническое решение продвигает определенные интересы, усиливает определенные группы и влияет на общественную, политическую и экономическую жизнь. Дебаты по поводу возможности создания домена «.xxx» (для «взрослых» материалов) явно демонстрируют, что ICANN придется заниматься политическими аспектами технических вопросов.

Международный статус ICANN

Особые связи между ICANN и правительством США всегда являлись объектом критики, ведущейся по двум направлениям. Первое связано с принципиальными соображениями и делает акцент на том, что важнейший элемент глобальной инфраструктуры Интернета, важный для всех стран, находится под контролем одного государства. Эта критика была очевидна в ходе WSIS и усиливалась из-за общей подозрительности в отношении внешней политики США после военного вторжения в Ирак. На этом уровне дискуссий ответом на критику чаще всего становится тот аргумент, что Интернет был создан при финансовой поддержке правительства США. Это дает правительству США моральные основания принимать решения по поводу формы и темпов интернационализации управления Интернетом. Этот аргумент нашел особенно широкую поддержку в Конгрессе США, который однозначно выступает против любой интернационализации управления Интернетом.

Второе направление аргументации в пользу интернационализации ICANN основано на практических и юридических соображениях. Так,

некоторые критики высказывают мнение, что если судебные власти США воспользуются своими полномочиями и в полной мере введут режим санкций против Ирана и Кубы, они могут обязать ICANN — как частную американскую компанию — удалить национальные домены этих двух государств из Интернета. Согласно этой аргументации, продолжая поддерживать доменные имена Ирана и Кубы, ICANN нарушает законы США относительно санкций. Хотя прецедентов с удалением национальных доменов еще не было, возможность такой ситуации при существующем правовом статусе ICANN сохраняется.

Сигналом к началу нового этапа в дискуссиях о статусе ICANN является подписание «Подтверждения обязательств» между Министерством торговли США и ICANN. Это событие закладывает основы для независимости ICANN и открывает новый блок вопросов, касающихся контроля, подотчетности, отношений с правительствами этой организации и т. д.

Оба ключевых вопроса — полномочия в отношении политических аспектов и интернационализация — могут быть решены изменением статуса ICANN, что позволит уменьшить неопределенность статуса и повысить прозрачность миссии организации. Развитие ICANN в будущем потребует инновационных решений. Возможным компромиссом может быть трансформация ICANN в особую международную организацию, которая сохранит преимущества существующей структуры ICANN, одновременно преодолев ее недостатки, в особенности проблему международной легитимности.

ПРИМЕЧАНИЯ

[1] Исключением являются США и ряд развитых стран (Австралия, Новая Зеландия и, наряду с ними, Европейская комиссия).

[2] Выбор членов WGIG основывался на критериях представительности и экспертных знаний. Структура представительства была основана на принципе равного количества участников (по 1/3 от общего числа) от правительств, гражданского общества и бизнеса. Представители правительств выбирались по обычным для региональных групп ООН критериям. Наряду с соображениями представительности требовалось, чтобы выбранные участники достаточно знали о предмете дискуссий WGIG, чтобы вносить в них содержательный вклад.

[3] См.: Всемирная встреча на высшем уровне по вопросам информационного общества. Декларация принципов. WSIS-03/GENEVA/DOC/4-R, 12 декабря 2003 г., ст. 49.

[4] Бразильская модель управления национальным доменом обычно приводится в качестве удачного примера многостороннего подхода. Организация, отвечающая за национальный домен Бразилии, открыта для всех пользователей, вклю-

чая правительственные ведомства, бизнес-сектор и гражданское общество. Бразилия постепенно распространила эту модель и на другие области управления Интернетом, особенно на процесс подготовки IGF-2007, прошедшего в Рио-де-Жанейро.

[5] Charles Lesage, La rivalite franco-britannique. Les cables sous-marins allemands (Paris, 1915) p. 257-258; цит. по: Daniel R. Headrick, The Invisible Weapon: Telecommunications and International Politics 1851-1945 (Oxford University Press: 1991), p. 110.

[6] Cukier, K. N. (2005). The WSIS wars: an analysis of the politicization of the Internet. In: B: D. Stauffacher and W. Kleinwachter (eds). The World Summit on the Information Society: moving from the past into the future. New York: United Nations ICT Task Force, p. 176.

[7] В телеграмме правительство США так критиковало участие МСЭ в проекте CORE: «Без одобрения правительствами государств-членов созвана глобальная встреча, предполагающая не одобренное расходование ресурсов и заключение "международных соглашений"».

[8] Удобство «одного окна» было одним из аргументов в пользу утверждения МСЭ в качестве центрального игрока управления Интернетом.

[9] Ценные комментарии по этому вопросу дала Аиша Хасан (Ayesha Hassan).

[10] Разработка Единой политики разрешения споров (Universal Dispute Resolution Procedures — UDRP).

[11] Интернет-сообщество соответствует всем критериям эпистемического сообщества, выдвинутым Питером Хаасом: «Профессиональная группа, члены которой имеют общие представления о причинах и следствиях, методах проверки истинности, разделяют общие ценности, имеют общее понимание проблемы и ее решений» (Peter Haas (1990), Saving the Mediterranean: the politics of international environmental co-operation (New York: Columbia University Press, p. 55).

[12] См.: Esther Dyson's Response to Ralph Nader's Questions. 15 June 1999 (адрес в Интернете: http://www.icann.org/correspondence/dyson-response-to-nader-15jun99.htm).

Приложения

ПРИЛОЖЕНИЕ 1. ЧЕТЫРНАДЦАТЬ УРОКОВ ФОРУМА ПО УПРАВЛЕНИЮ ИСПОЛЬЗОВАНИЕМ ИНТЕРНЕТА

В ходе Форума по управлению использованием Интернета (IGF) было представлено несколько инновационных подходов к управлению глобальными политическими процессами. Некоторые из них могут быть полезны и для других областей политики, затрагивающих интересы большого числа заинтересованных сторон (например, изменение климата, миграция, торговля, права человека). При обсуждении опыта IGF важно иметь в виду одно существенное различие между управлением Интернетом и другими глобальными политическими процессами. В то время как другие области регулирования, такие как изменение климата, традиционно контролировались государствами и медленно открывались для участия неправительственных игроков, в сфере управления Интернетом правительствам пришлось включаться в уже существующий неправительственный режим, центром которого является ICANN. IGF был одним из важных элементов в этом процессе. Соответствующий опыт IGF можно суммировать в следующих четырнадцати рекомендациях.

1. Будьте эффективным лидером: «Мудрец на сцене и проводник у дороги»

Одной из основных причин успеха IGF является исключительный уровень руководства Нитина Десаи, председателя IGF, и Маркуса Куммера, исполнительного координатора Секретариата IGF. Н. Десаи и М. Куммер вместе составляют высокоэффективную команду, дополняя взгляды и навыки друг друга. Оба обладают значительным дипломатическим опытом: первый отвечал за подготовку ряда важных встреч на высшем уровне в ООН, второй имеет в своем активе успешную карьеру в дипломатических структурах Швейцарии. Пока г-н Десаи руководил «главной сценой» мероприятий IGF, г-н Куммер помогал участникам достичь взаимопонимания и включиться в процесс, в нужный момент общаясь с ними за рамками официальных встреч, через Интернет, и участвуя в ключевых мероприятиях различных профессиональных сообществ, собравшихся вокруг IGF. Глубокое знание правил, процедур и практики ООН помогло этим дипломатам находить творческие ре-

шения и создавать эффективный, хотя и неформализованный, modus operandi[1]. Форума. Г-н Десаи объясняет одну из составляющих успеха IGF следующим образом: «Чтобы диалог состоялся, все участники должны признать, что ценность данного форума состоит в присутствии других участников; но для эффективного диалога каждый участник должен скорректировать свои ожидания относительно других и, прежде всего, слушать, а не говорить».

Новички в области управления Интернетом, Н. Десаи и М. Куммер не принадлежат к каким-либо «партиям» в давних дискуссиях по вопросам, связанным с ICANN (доменные имена, IP-адреса и корневые серверы). Их успех поставил под сомнение «дипломатический миф» о том, что технические вопросы должны решать технические эксперты. **Как показывает этот пример, иногда «дипломатизация» решения технических вопросов может помочь преодолеть традиционные споры в сообществе технических специалистов и способствовать успеху политического процесса.**

Нитин Десаи и Маркус Куммер

[1] Образ деятельности, образ действия (*лат.*).

2. Выстраивайте доверительные отношения, действуя вовремя и в нужной последовательности

Процесс IGF собрал за одним столом людей с самым разным профессиональным и культурным опытом. У участников нет опыта работы в одних и тех же организациях, учебы в одних и тех же университетах, вращения в тех же социальных кругах и прочих основных составляющих, на которых строится доверие. Доверительные отношения пришлось выстраивать в атмосфере, полной подозрений — либо из-за прошлых споров (например, между МСЭ и ICANN), либо из-за общей геополитической напряженности, вызванной войной в Ираке, либо из-за простого человеческого противопоставления «нас» и «их».

Выстраивание доверительных отношений требует терпения и правильно спланированной последовательности действий. Каждый этап процесса IGF был направлен на достижение взаимопонимания и на получение новых знаний и информации. Результатом стало постепенное укрепление доверия, а также содержательные обсуждения. Некоторые предложения, такие как прозвучавший в начале переговоров призыв к принятию рамочной конвенции об Интернете, были справедливо отвергнуты: время для дальнейшей формализации управления Интернетом еще не настало. Как показывает недавнее решение правительства США о будущем ICANN, некоторые проблемы теряют остроту с течением времени, если с ними обращаться осторожно и не позволять им перерасти в политический кризис. IGF был весьма успешным в этом отношении. **Дипломаты и политики могут поучиться у IGF эффективному выстраиванию отношений доверия за счет выбора правильного момента и последовательности действий, равно как и понять кое-что новое о времени и сроках в политическом процессе вообще.**

3. Позвольте политическому процессу развиваться своим чередом

С правильным выбором момента тесно связана другая рекомендация: важно позволять процессам развиваться за счет их собственной инерции, и не полагаться чрезмерно на детальное планирование. В сегодняшнем мире разработка логически последовательных схем и контроль по методу «вход/выход» является чем-то вроде навязчивой идеи. Такое чересчур детальное управление процессами может оказаться нерезультативным, поскольку социальная реальность слишком сложна, чтобы уложить ее в «прокрустово ложе» моделей и схем. Недавний глобальный финансовый кризис служит примером того, как система, основанная главным образом на науке и моделировании, может привести к краху, если в расчет не

берутся люди во всей их сложности, со всеми их слабыми и сильными сторонами.

В дипломатии риски, связанные с чрезмерно детальным управлением политическими процессами, хорошо иллюстрирует успех Венского конгресса (1814) и провал Версальского договора (1919). Венский конгресс заложил основу для одного из самых спокойных периодов европейской истории, не знавшего больших войн на протяжении почти 100 лет. Версальский мирный договор, напротив, потерпел крах уже через несколько лет после подписания. В Вене участники переговоров имели достаточно времени для работы, но не были исключены и социальные аспекты взаимодействия. Постепенно, без заранее определенного общего плана они выработали эффективное мирное соглашение, достижению которого помогли гении Меттерниха и Талейрана. В Версале, напротив, дипломаты участвовали в высокоорганизованном процессе, в котором сотни ученых, статистиков и картографов трудились вместе над созданием «мира, построенного по науке». Они даже попытались применить к поиску справедливого решения количественные методы. В конечном итоге, это создало неразбериху, приведшую ко Второй мировой войне. Конечно, на судьбу этих двух соглашений повлияли многие другие факторы, однако существенные различия в подходах к организации переговоров убедительно свидетельствуют против чрезмерного регулирования дипломатических процессов.

Непринужденная атмосфера Венского конгресса (1814)

Хотя IGF не может сравниться с этими великими событиями, его принципы ближе к Венскому конгрессу. Развлечений, к сожалению, было поменьше, чем в Вене, но общим является стремление не пытаться предопределять процессы, за исключением минимального планирования. Обсуждения IGF разворачиваются и принимают оптимальную форму путем «сплавления» мнений участвующих сторон, в том числе существенно различающихся.

4. Задействуйте разнообразные точки зрения за счет политического «длинного хвоста»

Концепция «длинного хвоста»[2] пришла в политику из маркетинга и относится к возможности задействовать самые разнообразные точки зрения, которые в обычных условиях потерялись бы в различных фильтрах традиционных межправительственных взаимодействий. **Отдельные лица и группы смогли высказать свои мнения непосредственно Форуму путем личного участия в мероприятиях, веб-коммуникации и удаленного участия.** Эти новые идеи и мнения, которые в большинстве случаев не достигают глобальных форумов на высшем уровне, значительно обогатили процесс IGF. Один из уроков заключается в том, что первым шагом на пути к большей открытости политического процесса является приглашение к свободному участию в нем. Полностью преимущества открытого и всестороннего участия достигаются тогда, когда собирается, рассматривается и, по возможности, включается в политические документы максимально большое количество точек зрения. Включение в процесс переговоров различных заинтересованных сторон повышает его легитимность и создает у участников чувство причастности результатам.

5. Расширяйте возможности страны «оставлять дипломатический след», привлекая различные заинтересованные стороны

С момента создания национальных государств и дипломатических служб в XVIII веке интересы жителей страны за рубежом традиционно представляли правительства. Когда Ришелье создал Министерство

[2] В маркетинге термин «длинный хвост» (введен Крисом Андерсом в статье в журнале «Wired» и затем в книге «Длинный хвост: новая модель ведения бизнеса») означает потребителей, которых интересуют специфические, нишевые, часто малоизвестные товары. Суммарный спрос на такие товары может значительно превышать общий объем продаж небольшого числа популярных товаров, однако до появления электронной торговли логистические расходы были слишком велики для того, чтобы продажа товаров «длинного хвоста» была экономически оправданной. — *Примеч. перев.*

иностранных дел Франции, письмо из Парижа в Москву шло месяц. Сегодня сообщение может покрыть такое же расстояние за доли секунды. Это заставляет задуматься над вопросом: может ли характер дипломатического представительства оставаться прежним несмотря на такие кардинальные изменения в области коммуникации?

Некоторые аспекты представительства, безусловно, остаются неизменными. На обозримую перспективу государства останутся основной формой организации человеческого общества, характеризующейся определенным населением, территорией и общей национальной идентичностью. Дипломатия сохраняет свое значение как главный канал для представления интересов общества за рубежом.

Однако в других отношениях концепцию представительства необходимо адаптировать. В условиях, когда на мировой арене стало больше игроков и увеличилось число сложных вопросов, традиционный дипломатический подход демонстрирует серьезную ограниченность. Даже самые эффективные дипломатические службы не обладают достаточной «пропускной способностью» (то есть квалифицированными человеческими ресурсами) для общения с иностранными субъектами. Более высокая «пропускная способность дипломатии» может быть обеспечена за счет включения представителей гражданского общества, деловых кругов, местных органов власти и других субъектов глобальных политических процессов. Уже сегодня многие негосударственные субъекты проводят собственную «дипломатию» — например, поддерживают контакты с иностранными организациями, участвуют в международных совещаниях и формируют глобальный политический дискурс.

Некоторые государства, например, Канада, Швейцария и страны Скандинавии, первыми признали эту тенденцию и включили негосударственных участников во внешнеполитический процесс с помощью таких инициатив, как «Команда Канады» (Team Canada) и назначения специальных послов по работе с НПО. К сожалению, эта практика не распространена во многих развивающихся странах, где «дипломатическая пропускная способность», как правило, очень низка и ограничивается небольшой дипломатической службой с ограниченными финансовыми и человеческими ресурсами. Во многих развивающихся странах многосторонние структуры на национальном уровне появились только в последние несколько лет.

Форум по управлению использованием Интернета внес практический вклад в повышение осведомленности правительственных кругов, в особенности в развивающихся странах, о преимуществах многостороннего подхода. Помимо общего принципа открытости участия, многосторонний подход в рамках IGF продемонстрировал

и практическое решение, которое помогает странам оставлять более заметный «дипломатический след» без необходимости вкладывать больше ресурсов. На национальном уровне появляются многосторонние органы IGF, и правительства чаще координируют свои действия с деловыми кругами и гражданским обществом. Некоторые малые и развивающиеся государства представлены в процессе управления Интернетом негосударственными субъектами.

Иногда внедрение такого открытого участия является в основном вопросом координации, выявления квалифицированных представителей своей страны и создания национального механизма многостороннего участия. Полезной оказывается также организация учебных программ по развитию потенциала с участием различных заинтересованных сторон, представляющих одну страну: среди участников таких программ, как правило, устанавливаются отношения доверия и командный дух.

6. Повышайте уровень политической согласованности, привлекая различные заинтересованные стороны

Сегодня одной из основных сложностей для любого глобального политического процесса, в том числе в таких областях, как изменение климата и миграция, является достижение политической согласованности в решении междисциплинарных вопросов. В области управления Интернетом IGF выступает в качестве «зонтика», под которым могут разместиться различные существующие режимы, включая информационные технологии, права человека, торговлю и интеллектуальную собственность. В процессе IGF различные политические группы обнаруживают, что ранее изолированные области их интересов являются частью управления Интернетом. В некоторых тематических областях, таких как многоязычие, IGF помог различным организациям, включая правительства, ICANN, ЮНЕСКО и МСЭ, скоординировать усилия в решении общей задачи. Как орган, *формирующий* решения, IGF больше способствует политической согласованности, чем некоторые *принимающие* решения органы. **Необычно широкое участие различных заинтересованных сторон ослабило традиционную «борьбу за сферы влияния» и дало возможность увязать разнообразные инициативы в согласованный политический процесс. Такой подход позволил также частично разрешить проблему дублирования, когда различные организации в конечном итоге занимались решением одних и тех же вопросов.**

7. Разрабатывайте функциональную взаимосвязь между национальным, региональным и глобальным уровнями выработки политики

Во все более взаимосвязанном мире трудно сохранить традиционную архитектуру международной политики, состоящую из международных организаций на региональном и глобальном уровнях. Мгновенная коммуникация и растущее влияние негосударственных субъектов стирают грань между национальными, региональными и глобальными пространствами политики. В этом едином глобальном политическом пространстве проблемы «мигрируют» с одного уровня на другой и с одной площадки на другую. Некоторые игроки, особенно неправительственные организации, используют эту возможность, чтобы внести свои политические инициативы на уровне, наиболее благоприятном для них. Правительства, например, в странах ЕС, порой используют так называемое отмывание политики: если инициатива не принимается на национальном уровне, она вносится на региональном уровне и вновь возвращается в страну уже в качестве «международных обязательств».

В области управления Интернетом сеть политических форумов очень сложна. Множество различных площадок существовало задолго до того, как был создан IGF (международные организации, ICANN, Общество Интернета, различные органы по стандартизации). Кроме того, субъекты управления Интернетом весьма динамичны и легко «мигрируют» с одного уровня политики или форума на другой с помощью современных коммуникационных технологий. **Форум по управлению использованием Интернета пытается максимизировать преимущества и сократить риски «многоуровневого» политического процесса. В его рамках глобальные, региональные и национальные мероприятия координируются как «снизу вверх» (в ходе подготовки Форума), так и «сверху вниз» (путем распространения знаний, созданных в процессе работы Форума). Высокая прозрачность IGF делает поиск «подходящего» форума и другие манипуляции с политическим процессом более сложными.** Хотя Форум достиг с этой точки зрения существенного прогресса, многое еще предстоит сделать.

8. Развивайте коммуникацию между различными профессиональными и организационными культурами

Сотни книг были написаны о том, как общаться с людьми из разных национальных культур: арабами, китайцами, американцами и т. д. Однако опыт IGF показывает, что в политическом процессе основная сложность часто заключается в налаживании коммуникации между

различными профессиональными культурами (например, юристы, инженеры) и различными организационными культурами (например, представители международных организаций, правительств, компаний). В сегодняшнем глобализованном мире, располагая средствами мгновенной коммуникации, нам зачастую легче общаться в рамках одной профессиональной среды, невзирая на национальные границы. Например, американский инженер-компьютерщик может обнаружить, что у него лучше складывается взаимодействие с другим инженером в Китае, чем с американским дипломатом.

Поскольку значение технической стороны глобальных вопросов возрастает (например, в изменении климата и здоровье человека), повышение эффективности межпрофессиональной коммуникации становится все более важным. Улучшения межпрофессионального общения можно достичь путем подготовки, обучения и контактов с другими культурами. Более эффективное общение между представителями разных профессий может также повысить согласованность политики различных министерств и международных организаций. **Форум по управлению использованием Интернета способствовал налаживанию межпрофессионального общения, обеспечивая эффективный обмен идеями между специалистами разных областей.** Ярким примером является значительное профессиональное и институциональное разнообразие участников на сессиях Форума.

9. Признайте, что технические и научные вопросы не являются политически нейтральными

Процесс IGF продемонстрировал, что любой технический вопрос имеет политический аспект; он усиливает позиции определенных групп и продвигает определенные интересы. На некотором этапе технические вопросы превращаются политические; вопросы политики, в свою очередь, требуют принятия решений о ценностях и интересах.

Выход технических вопросов на политический уровень происходит и в других сферах. Копенгагенская встреча на высшем уровне по вопросам изменения климата показала, что в составе национальных делегаций будет появляться все больше дипломатов и политиков и меньше ученых, специализирующихся на проблемах изменения климата. Поскольку дипломатические процессы все более пересекаются со сферами науки и техники, актуальность вопроса о разграничении двух этих областей будет возрастать.

10. Помните, что текст остается ключевым для дипломатии

Несмотря на потенциал виртуальных конференций и других технологий, сегодня — даже в большей степени, чем раньше — текст остается ключевым инструментом дипломатии [1]. Текст занимает центральное место в процессе IGF несмотря на то, что итогом деятельности Форума не является какой-либо официальный документ (например, конвенция, договор или декларация). Общение в промежутках между подготовительными сессиями осуществляется в основном с помощью списков рассылки и по электронной почте. Сайт IGF насыщен текстами, на нем представлено относительно мало фотографий или изображений. Текст также является ключевым для двух других видов деятельности, которые отдельно рассматриваются ниже: стенографические отчеты и дистанционное участие. Опыт IGF показывает, что многосторонний характер процессов не умаляет значения текста. В самом деле, стало очевидно, что основные процессы должны быть построены вокруг текста. Этот факт следует отразить в обучении и подготовке заинтересованных сторон к участию в глобальных политических процессах.

11. Оцените влияние дословных отчетов на дипломатию

Дословные отчеты в реальном времени — запись и представление в виде текста всех устных заявлений прямо по ходу совещания — являются процедурной и технической инновацией, которая может иметь существенное влияние на то, как осуществляется многосторонняя дипломатия. Опираясь на практику ICANN, секретариат Рабочей группы по управлению Интернетом (WGIG) начал внедрять дословные отчеты в апреле 2005 г. Эта практика была продолжена в ходе IGF, а недавно внедрена и в МСЭ. Все устные выступления записываются в

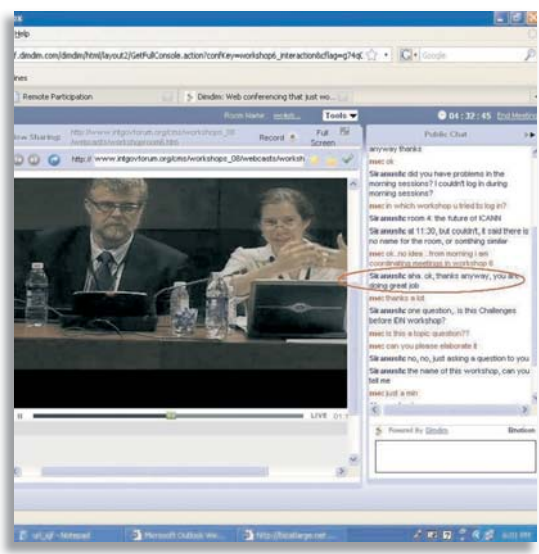
Экран с дословным отчетом на Форуме по управлению использованием Интернета в Рио-де-Жанейро. Фотограф Чарльз Мок (Charles Mok)

реальном времени специальными стенографистами и сразу же отображаются на большом экране в зале заседаний, а также транслируются через Интернет. Во время выступления делегатов на экране отображается текст их выступления.

Дословные отчеты значительно повлияли на то, как осуществляется дипломатия, на ее modus operandi. Осознание того, что все сказанное останется в письменной форме, заставляет многих делегатов быть более осторожными в выборе уровня и продолжительности их устных выступлений. Дословные отчеты также повысили прозрачность дипломатических переговоров.

12. Повышайте открытость и представительность с помощью центров дистанционного участия [2]

Одной из основных целей IGF было обеспечение участия в процессе самых разных стран и заинтересованных групп. Для форума, посвященного управлению Интернетом, было естественно использовать Интернет для расширения участия во встречах IGF, давая доступ к ним даже тем, кто не смог присутствовать физически. В ходе первого заседания IGF в Афинах секретариат Форума обеспечивал видео-, аудио- и текстовые трансляции как подготовительных, так и основных мероприятий. Эти материалы в основном смотрели те, кто и так интересовался IGF. В результате уровень удаленного участия был относительно скромным и не позволил вовлечь в процесс все стороны, заинтересованные в обсуждавшихся на IGF темах.



Удаленное участие в IGF 2008 г.

В качестве решения было предложено использовать «удаленные центры» («хабы»). Под ними понимаются встречи на местах, которые проводятся во время заседаний IGF и параллельно им; организаторами таких встреч выступают университеты, центры ИКТ, неправительственные организации и другие объединения и группы, занимающиеся вопроса-

ми управления Интернетом. В рамках встреч организуется трансляция заседания IGF в реальном времени, чтобы удаленные участники были в курсе обсуждаемого в данный момент вопроса. Они также могут отправлять текстовые и видеовопросы, на которые участники дискуссии IGF отвечают «в прямом эфире». Кроме того, «удаленные центры» собирают экспертные группы и круглые столы, на которых темы IGF рассматриваются с учетом местных реалий. В рамках этой деятельности удаленные центры позволяют более эффективно координировать политические процессы на глобальном и местном уровне. Например, в ходе IGF в 2008 г. центр в Мадриде транслировал сессии и организовывал обсуждение по вопросам кибербезопасности применительно непосредственно к Испании. Параллельно с IGF в 2008 г. в общей сложности работало восемь удаленных узлов (Мадрид, Лахор, Барселона, Белград, Буэнос-Айрес, Сан-Паулу, Богота и Пуна). За четыре дня Форума было транслировано более 450 часов мероприятий, дистанционное участие в обсуждениях приняли в общей сложности 522 посетителя [3].

После успешного тестирования в 2008 г. концепция удаленных центров была принята Секретариатом IGF. Ожидается, что дистанционное участие значительно расширится в ходе следующего IGF в Шарм-эш-Шейхе (ноябрь 2009 г.)[3].

Опыт Форума по управлению использованием Интернета показывает, что дистанционное участие значительно увеличивает открытость международных совещаний и представленность различных интересов, способствует формированию связи между глобальной и местными политическими аренами, часто отсутствующей в международной дипломатии.

13. Учитывайте взаимосвязь между формальным протоколом (или отсутствием такового) и равным участием

Одна из проблем, стоящих перед IGF — противопоставление культуры официальной дипломатии ООН и неофициальной культуры интернет-сообщества. После трех ежегодных встреч Форума кажется, что неофициальная культура возобладала. Но хотя эта культура создает атмосферу включенности, способствует участию молодежи и различных сообществ по всему миру, она может быть и источником некоторых проблем. В неформальной обстановке участники из стран, культура которых подчеркивает уважение к социальной иерархии, могут чувство-

[3] Текст данной книги был подготовлен осенью 2009 г., до проведения Форума в Шарм-эш-Шейхе. — *Примеч. перев.*

вать себя некомфортно и не решаться внести свой вклад в дискуссию. Кроме того, в дипломатической, правовой и других профессиональных культурах участие в обсуждении структурировано профессиональными протоколами. Поэтому неформальность рабочего процесса и обсуждений может препятствовать участию некоторых делегатов и стать источником неравенства. **IGF отвечает на такой риск, находя способы сочетать различные уровни формальности, предлагая несколько форматов работы, в которых все заинтересованные стороны могут участвовать, не испытывая дискомфорта.** Например, IGF повысил уровень формальности протокола на некоторых сессиях, в основном пленарных, введя более типичные для дипломатии правила процедуры (например, порядок выступлений, вопросов) и организовав специальные сессии для парламентариев.

14. Обеспечьте эффективное участие развивающихся стран: от формального равенства к функциональному

В структурах ООН малые и развивающиеся государства обычно обеспечивают себе равный статус, настаивая на формальных принципах и процедурах представительства. В отличие от развитых и крупных государств, малые и развивающиеся страны не обладают сетью параллельного представления интересов общества в целом силами бизнеса, гражданского общества и академических кругов. Поэтому неудивительно, что они могут испытывать сомнения относительно участия различных негосударственных субъектов. На заседаниях «большого масштаба», собирающих тысячи участников на равноправной основе, такая теряет «защиту» процедур ООН, согласно которым представители всех 194 государств имеют формально равный статус, независимо от их размера или мощи.

В начале процесса подготовки Всемирной встречи на высшем уровне по информационному обществу (WSIS) в 2002 г. многие малые и развивающиеся государства выступали решительно против предложений ввести равноправное участие деловых кругов и представителей гражданского общества. Некоторые из этих государств высказались за принцип «единого окна» в вопросах управления Интернетом, что дало бы им одну, предпочтительно межправительственную, «площадку» для обсуждения всех вопросов управления Интернетом [4].

С 2002 г. WSIS, WGIG и особенно IGF достигли значительного прогресса в деле укрепления ориентированных на развитие аспектов многостороннего процесса, в том числе обеспечив достаточное представительство малых и развивающихся государств.

1. На официальном уровне IGF гарантирует, что различные заинтересованные стороны из развивающихся государств адекватно представлены во всех заседаниях и экспертных группах. Повышение уровня участия развивающихся стран очевидно на примере встреч IGF в Рио-де-Жанейро и Хайдарабаде.
2. Процесс IGF помог многим малым и развивающимся государствам более эффективно использовать человеческие ресурсы. Речь идет не только о дипломатах, но и о других гражданах, имеющих опыт в области управления Интернетом, работающих в связанных с Интернетом организациях и университетах по всему миру. Использование потенциала экспертов, работающих за рубежом, для малых государств особенно важно.
3. Физическое участие, то есть присутствие на заседаниях, не обязательно означает равное участие. Равное участие требует от каждого делегата адекватных знаний, навыков и уверенности для участия в политическом процессе. IGF пытался обеспечить равное участие посредством мероприятий по развитию потенциала. С 2002 г. более 1000 должностных лиц и специалистов из малых и развивающихся государств были вовлечены в подготовку кадров и другие мероприятия по развитию потенциала. Эти мероприятия выходят за рамки традиционных академических курсов, обеспечивая уникальное сочетание обучения, исследований в области политики и погружения в политический процесс, чтобы

Формальное и функциональное равенство на переговорах

помочь участникам понять динамику IGF и обрести уверенность, необходимую для полного и эффективного участия в политических процессах. Вовлечение различных заинтересованных сторон (дипломатов, чиновников, инженеров) в процесс обучения позволило участникам понять преимущества многостороннего подхода, дало необходимую уверенность для участия в переговорах с представителями других профессиональных сообществ.

4. Процесс IGF также способствовал развитию «сообществ практики» в области управления Интернетом на «глобальном Юге» как на региональном (например, Западная Африка, Восточная Африка, Латинская Америка), так и на национальном уровне (например, Кения, Бразилия, Сенегал). Эти сообщества помогли многим малым и развивающимся государствам привлечь к процессу различные заинтересованные стороны, выявив экспертов в неправительственных кругах, которые уже участвуют в научных исследованиях и процессе управления Интернетом.

Расширяя масштаб участия, поощряя развитие потенциала и содействуя созданию сетей и сообществ, IGF помог развивающимся странам перейти от официального/пассивного к функциональному/активному участию в управлении Интернетом.

ПРИМЕЧАНИЯ

[1] Интересную параллель можно провести с использованием услуги SMS на мобильных телефонах: текст по-прежнему необходим в человеческом общении, несмотря на мощные инструменты, основанные на передаче голоса и видео.

[2] Значимые и содержательные замечания по этому пункту предоставили Джинджер Пак (Ginger Paque) и Марилия Марсель (Marilia Marcel), активные члены рабочей группы по удаленному участию (www.igfremote.com).

[3] Подробный отчет об удаленном участии в IGF-2008 доступен по адресу в Интернете: http://www.igfremote.com/ReportRPIGF-final.pdf.

[4] Предварительные исследования показывают, что различными аспектами управления Интернетом занимаются 80—100 международных организаций, органов по стандартизации, форумов и других организаций. Даже для крупных развитых государств охватить такое широкое поле почти невозможно. IGF пытался уменьшить эту сложность, «отфильтровывая» вопросы собственно управления Интернетом от других политических вопросов (тайна частной жизни, интеллектуальная собственность, права человека, развитие, электронная коммерция и т. д.).

ПРИЛОЖЕНИЕ 2

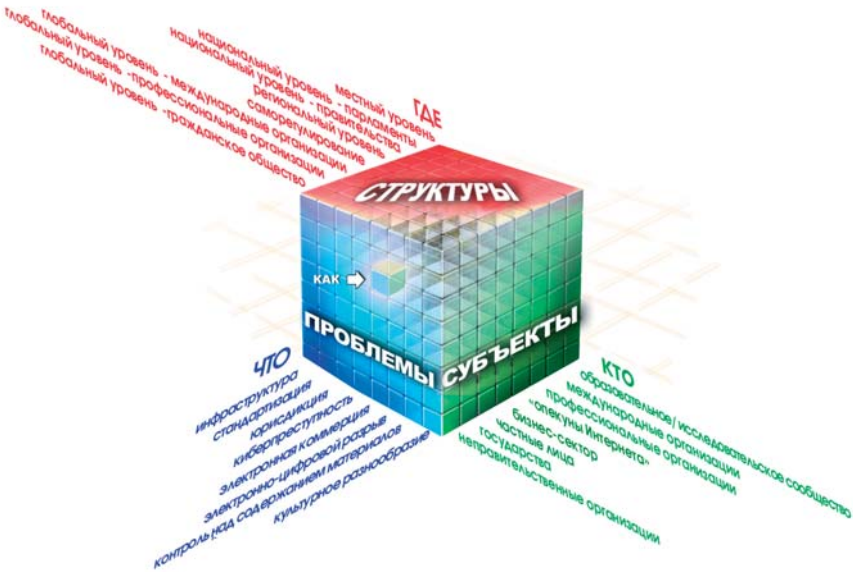
ПРИЛОЖЕНИЕ 3.
ОБЗОР ЭВОЛЮЦИИ УПРАВЛЕНИЯ ИНТЕРНЕТОМ

Период	Деиствующее лицо					
	США	«Опекуны» Интернета	Международные организации	Частный сектор	Государства	Гражданское общество
	Министерство обороны управляет системой DNS.					
1986	Национальный фонд науки (НФН) принимает управление структурами Интернета от Минобороны.					
1994				Компания NSI подписывает с НФН контракт на управление системой DNS в 1994–1998 гг.		
НАЧАЛО «ВОЙНЫ DNS» После передачи управления DNS от НФН к NSI (частной компании) интернет-сообщество (в первую очередь ISOC) в течение многих лет пытается вернуть управление DNS под контроль общественности. Через 4 года ему это удается. Ниже приводится обзор этого процесса, включавшего в себя множество дипломатических приемов: переговоры, создание коалиций, использование силы, нахождение консенсуса и т. д.						
июнь 1996		IANA/ISOC планируют взять на себя функции NSI по завершении контракта; появляются новые домены; сильная оппозиция новым доменам со стороны участников, заинтересованных в защите торговых марок, и МСЭ.				
весна 1997		Предложение о создании Международного специального комитета (МСК – International Ad Hoc Committee). Участники МСК: по два представителя от групп интересов (в сфере защиты торговых марок), ВОИС, МСЭ и НФН; и пять представителей от IETF. Подписание меморандума о взаимопонимании по родовым доменам верхнего уровня, предусматривающего: статус DNS как «публичного ресурса»; создание семи новых доменов; усиление защиты торговых марок. Создание Совета регистраторов (Council of Registers) – церемония подписания состоялась в марте 1997 г. в МСЭ, Женева; Совет регистраторов немедленно распался. Мощная оппозиция со стороны правительства США, НФН и Евросоюза.				

Период	США	«Опекуны» Интернета	Международные организации	Частный сектор	Государства	Гражданское общество
1997	Правительство США передает управление DNS Министерству торговли.					
июнь 1998	«Белая книга» Министерства торговли призывает основных участников предлагать собственные решения.	Предложения получены от Международного форума по «Белой книге» (International Forum on White Paper), Открытой конфедерации корневых серверов (Open Root Server Confederation) и Бостонской рабочей группы (Boston Working Group).				
		Вместо подготовки нового документа ISOC сосредоточивается на: – создании широкой коалиции, включающей международные организации (из инициативы МСК), представителей частного сектора (IBM) и ключевых стран (ЕС, Япония, Австралия); – создании новой организации.				
вторая половина 1998		Сентябрь 1998 г. – Предварительное соглашение между ISOC и NSI. Октябрь 1998 г. – ISOC выходит из соглашения и создает ICANN.				
15 ноября 1998	Министерство торговли передает полномочия ИКАНН.	ИКАНН получает две новые важные функции: – право давать аккредитацию регистраторам родовых доменов верхнего уровня; – управление на основе авторитета (политический аспект по-прежнему контролируется Министерством торговли США).				
апрель 1999		Соглашение Министерства торговли США, ICANN и NSI и внедрение «системы регистрации общего пользования» (shared registry system). NSI теряет монополию, но получает благоприятные условия на переходный период (управление четырьмя доменами).				
июнь 1998		Создание Организации поддержки протоколов (Protocol Supporting Organization), включающей в себя IETF, W3C и других «пионеров» Интернета.	В рамках ВОИС начат «процесс доменных имен Интернета».	Создана Организация поддержки адресов (Address Support Organization) – чтобы представлять ассоциацию регистраторов DNS (ARIN, RIPE, NCC). Создана Организация поддержки доменных имен (Domain Name Supporting Organization) – для защиты торговых марок и коммерческих интересов.	30 стран создают Правительственный консультативный комитет (Government Advisory Committee), чтобы получить больше влияния на управление национальными доменами. ICANN в ответ создает подкомитет по страновым доменам верхнего уровня.	

Период	США	«Опекуны» Интернета	Международные организации	Частный сектор	Государства	Гражданское общество
КОНЕЦ «ВОЙНЫ DNS» «Война» завершилась компромиссом. ISOC удалось расширить контроль общественности над управлением DNS, хотя коммерческие интересы все еще очень сильны. Таким образом, защищены интересы и частного бизнеса, и сообщества «опекунов». Однако в отношении позиций государств и интернет-сообщества в целом это далеко не так. Это два наиболее слабых аспекта системы управления ИКАНН.						
2000–2003			Интернет привлекает все большее внимание МСЭ, ВОИС, ЮНЕСКО, ОЭСР, Совета Европы и Всемирного банка.	Сильное давление частного сектора в пользу регулирования Интернета (защита авторских прав, электронная коммерция и т. д.).	Развитие законодательства и судебной практики, касающихся Интернета.	Неправительственные организации вовлекаются в решение проблем «цифрового разрыва», прав человека, гендерных проблем в Интернете.
			Многосекторные и глобальные инициативы, посвященные развитию и управлению Интернета и др.: Целевая группа по цифровым возможностям «Большой восьмерки» (G-8 Dot Force), Всемирный экономический форум, Целевая группа ООН по ИКТ, ВСИО, Глобальное партнерство во имя знания			
июнь 2002 – ноябрь 2003	В июне 2002 г. состоялась первая подготовительная встреча WSIS; управление Интернетом появилось на повестке дня во время региональной подготовительной встречи по Западной Азии в Бейруте (январь 2003 г.); Участники WSIS в Женеве включают вопросы управления Интернетом в повестку дня Тунисского этапа встречи (2005 г.) Многосекторные и глобальные инициативы, посвященные развитию управления Интернетом: группа «Большой восьмерки» Dot Force, Всемирный экономический форум, Целевая группа ООН по ИКТ.					
2004–2005	Содержание дискуссий по управлению Интернетом в этот период задавала Рабочая группа по управлению Интернетом (WGIG). WGIG включала в себя представителей различных заинтересованных сторон: правительств, бизнеса и гражданского общества. WGIG провела четыре подготовительных встречи и подготовила отчет, ставший основной последующих решений по управлению Интернетом во время встречи WSIS в Тунисе (2005 г.) Участники WSIS в Тунисе решают создать Форум по управлению использованием Интернета как результат компромисса между противниками каких-либо изменений в режиме, основанном на ICANN, и сторонниками межгосударственного режима управления Интернетом.					
2006–2009	После завершения Тунисского этапа WSIS (2005 г.) с целью продолжения политического процесса по управлению Интернетом был создан Форум по управлению использованием Интернета (IGF). На сегодняшний момент состоялись четыре встречи Форума: в 2006 г. в Афинах, в 2007 г. в Рио-де-Жанейро, в 2008 г. в Хайдарабаде и в 2009 г. в Шарм-эш-Шейхе. 30 сентября 2009 г. правительство США и ICANN подписали «Подтверждение обязательств»; этот документ положил конец контролю США над ICANN – одному из наиболее спорных моментов управления Интернетом. ICANN выходит на новый этап развития в качестве независимой организации; относительно ее будущего статуса и роли вопросов пока больше, чем ответов.					

ПРИЛОЖЕНИЕ 4. «КУБ УПРАВЛЕНИЯ ИНТЕРНЕТОМ»



Ось «ЧТО» связана с вопросами, рассматриваемыми в рамках управления Интернетом (инфраструктура, авторское право, тайна частной жизни и т. д.). Она является воплощением **многодисциплинарности** данного подхода.

На оси «КТО» представлены основные ДЕЙСТВУЮЩИЕ ЛИЦА (государство, международные организации, гражданское общество, частный сектор). Эта сторона представляет множество участников процесса (**многосторонний** подход).

Ось «ГДЕ» характеризует те структуры, в рамках которых могут решаться вопросы, связанные с Интернетом (саморегулирование, местный, национальный, региональный и глобальный уровни). Это иллюстрация **многоуровневого** подхода к управлению Интернетом.

Пересекаясь между собой, три оси куба образуют своеобразные перекрестки, для каждого из которых можно задать вопрос «КАК?». Каждое из таких пересечений помогает понять, как нужно регулировать тот или иной вопрос — с точки зрения и когнитивно-правовых технологий (аналогия), и инструментария («мягкое право», соглашения, декларации). Так, одно из таких пересечений помогает понять, КАК гражданское общество (КТО) на национальном уровне (ГДЕ) должно действовать в отношении вопросов, связанных с тайной частной жизни (ЧТО).

Вне куба рассматривается компонент «КОГДА».

ОБ АВТОРЕ

ЙОВАН КУРБАЛИЙЯ

Йован Курбалийя является основателем и директором фонда DiploFoundation. В прошлом профессиональный дипломат, он имеет опыт работы и исследований в области права, дипломатии и информационных технологий. В 1992 г. Й. Курбалийя создал Центр по информационным технологиям и дипломатии в Средиземноморской академии дипломатических исследований на Мальте. После более чем десяти лет успешной работы в сфере обучения, исследований и подготовки публикаций в 2003 г. Центр превратился в фонд DiploFoundation.

С 1994 г. доктор Курбалийя ведет курсы по влиянию ИКТ/Интернета на дипломатию и по управлению ИКТ/Интернетом. Он преподавал в Средиземноморской академии дипломатических исследований на Мальте, Венской дипломатической академии, Нидерландском институте международных отношений (Клингендал), Институте международных исследований и проблем развития в Женеве, Колледже персонала системы ООН и Университете Южной Калифорнии. Он разработал и в настоящее время возглавляет «Программу развития потенциала в области управления Интернетом» DiploFoundation (2005—2009). Основные исследовательские интересы доктора Курбалийи: становление международного режима Интернета, использование Интернета в дипломатии и переговорах, влияние Интернета на современные международные отношения.

Доктор Курбалийя — автор и редактор многочисленных книг, статей и глав. Среди его работ «Руководство по Интернету для дипломатов», «Знания и дипломатия», «Влияние информационных технологий на дипломатическую практику», «Информационные технологии и дипломатическая служба развивающихся стран», «Современная дипломатия» и «Язык и дипломатия». Совместно со Стефано Балди и Эдуардо Гелбстайном он является автором «Библиотеки информационного общества», серии из восьми брошюр, рассматривающих широкий спектр различных вопросов, связанных с Интернетом.

jovank@diplomacy.edu

Координационный центр национального домена сети Интернет (сокращенное название — Координационный центр домена .RU)

Организация, созданная в 2001 году для выработки правил регистрации доменных имен в доменах .RU и .РФ, аккредитации регистраторов и исследования перспективных проектов, связанных с развитием российского национального домена. Организации-учредители: общественно-государственное объединение «Ассоциация документальной электросвязи» (АДЭ), «Союз операторов интернет» (СОИ), Региональная организация «Центр интернет-технологий» (РОЦИТ) и Российский НИИ развития общественных сетей (РосНИИРОС).

В январе 2006 г. сведения о Координационном центре домена .RU были занесены в базу данных IANA. В марте 2007 года Координационный центр домена .RU формализовал отношения российской национальной регистратуры с ICANN путем обмена официальными письмами.

На сегодняшний день в ведении Координационного центра находятся вопросы, связанные с функционированием двух национальных доменов: домена .RU и нового кириллического домена .РФ. Координационный центр официально стал администратором домена .РФ 21 января 2010 г. после успешного прохождения процедуры Fast Track и утверждения ICANN заявки на домен .РФ.

http://www.cctld.ru

DiploFoundation

Некоммерческая организация, ставящая целью помочь всем заинтересованным сторонам принимать значимое участие в дипломатии и международных отношениях. Основными направлениями нашей деятельности являются образование, профессиональная подготовка и развитие потенциала.

- *Курсы*. Мы предлагаем курсы последипломного уровня и образовательные семинары по широкому спектру тем, связанных с дипломатией. Наша аудитория — дипломаты, государственные служащие, сотрудники международных и неправительственных организаций, а также все, кто изучает международные отношения. Курсы предлагаются в формате онлайн или «смешанного» обучения (онлайн и офлайн).
- *Развитие потенциала*. С помощью наших спонсоров и партнеров мы предлагаем программы развития потенциала для участников из развивающихся стран по таким темам, как управление Интернетом, права человека, публичная дипломатия, дипломатия в сфере здравоохранения.
- *Исследования*. В рамках исследовательских проектов и конференций мы изучаем темы, связанные с дипломатией, международными отношениями и онлайн-обучением.
- *Публикации*. Наши публикации посвящены как исследованиям современных тенденций, так и новому осмыслению традиционных аспектов дипломатии
- *Разработка программного обеспечения*. Мы разработали набор программных приложений, специально созданных для дипломатов и других специалистов по международным отношениям. Нашей сильной стороной также является разработка платформ для онлайн-обучения.

Центральный офис Diplo находится на Мальте, два других офиса — в Женеве и Белграде. Diplo появился из проекта по внедрению информационно-коммуникационных технологий в дипломатическую практику,

начатого в 1993 г. в Средиземноморской академии дипломатических исследований на Мальте. В ноябре 2002 г. Diplo приобрел статус независимого некоммерческого фонда, основателями которого являются правительства Мальты и Швейцарии. Спектр нашей деятельности расширился и, помимо информационных технологий в дипломатии, сегодня включает в себя как новые, так и традиционные аспекты обучения и практики в области дипломатии и международных отношений.

Первый российский форум по управлению Интернетом (RIGF-2010)

В последнее время наметилась тенденция проведения региональных и национальных форумов IGF, во время которых их участники обсуждают технические, организационные и правовые вопросы использования Интернета в своих странах и регионах. Так, региональные IGF проводятся в Европе, в Азии, в Африке, в странах Карибского бассейна, в Латинской Америке. Национальные форумы проводит большинство европейских стран.

Российский форум по управлению Интернетом стал первым мероприятием подобного рода в Восточной Европе. Сегодня мы можем говорить о том, что наше общество «дозрело» до обсуждения вопросов управления Интернетом: в первую очередь потому, что Интернет в России, как и в большинстве других стран, уже стал двигателем большого количества экономических процессов и экономика страны во многом зависит от стабильной работы сети, формирующей современную информационно-коммуникационную среду.

Основной целью Первого российского форума по управлению Интернетом является повышение осведомленности представителей российских государственных организаций, бизнеса, научного мира и интернет-сообщества о текущих и перспективных процессах развития глобальной сети, представление многообразия использования Интернета в интересах общественного развития и повышение уровня участия России в глобальном IGF. Российский форум призван объединить все профессиональные точки зрения и организовать дискуссию для поиска консенсуса между государственными органами, профессиональным телекоммуникационным сообществом, бизнесом и гражданским обществом по вопросам дальнейшего развития Интернета в России.

Выбор времени и места проведения Форума не случаен: Форум проходит во время выставки «Связь-Экспокомм-2010», на которой будут присутствовать лидеры телекоммуникационного бизнеса и интернет-индустрии, что послужит расширению аудитории участников Форума.

Организаторы Форума — Координационный центр национального домена сети Интернет и Министерство связи и массовых коммуникаций Российской Федерации — надеются, что Первый российский форум по управлению Интернетом даст возможность всем его участникам не просто высказать свое мнение, но и услышать друг друга. Именно в равноправных дискуссиях и вырабатываются те решения, которые в дальнейшем повлияют на развитие не только российского, но и мирового Интернета и сделают процесс интернет-управления открытым для участия всех и каждого.

Подробная информация о Российском форуме по управлению Интернетом — на сайте Форума http://russia2010.intgov.net

Домен .РФ – первый кириллический домен в мировом интернет-пространстве

2010 год стал для России годом старта нового национального домена — домена .РФ. 21 января 2010 года ICANN сообщила о том, что заявка России на делегирование IDN-домена .РФ по процедуре Fast Track удовлетворена. На сегодняшний день это единственная заявка на кириллице. В мае 2010 года ожидается техническое делегирование нового домена .РФ, когда IANA разместит сведения о домене .РФ на корневых серверах мировой системы доменных имен (DNS).

Наряду с тремя арабскими государствами Российская Федерация станет одной из первых стран, которые начнут использование нелатинских доменов в интернет-пространстве. Именно в России будут внедряться те технические новшества, благодаря которым домены с использованием национальных (нелатинских) алфавитов будут доступны всему мировому интернет-сообществу.

Идею появления домена на кириллице с самого начала поддержал Президент Российской Федерации Дмитрий Медведев. Он сказал: «Мы должны сделать все от нас зависящее, чтобы добиться присвоения доменных имен на кириллице. Это символическая значимость русского языка, и у нас неплохие шансы добиться соответствующего решения».

Выбор аббревиатуры будущего домена — .РФ — обусловлен обязательным наличием хотя бы одной буквы алфавита, являющейся отличной от привычной всем кодировки ASCII. Для России это уникальный кириллический символ «Ф». Кроме того, это обозначение имеет важное смысловое значение для жителей Российской Федерации (РФ).

Русский язык является пятым в мире по распространенности, при этом 160 миллионов человек считают его родным. Чтобы запомнить название сайта на кириллице, русскоговорящему человеку требуется менее 0,8 секунд — в отличие от названия сайта, написанного латиницей, где русскоговорящий пользователь тратит на запоминание интернет-адреса в среднем около 3 секунд.

Проведенные Координационным центром национального домена сети Интернет опросы показали, что поддерживают внедрение нового национального домена .РФ более 60 % российский интернет-пользователей,

а зарегистрировать собственное доменное имя в домене .РФ собирается каждый пятый. При этом .РФ не становится конкурентом традиционному латинскому домену .RU, он лишь позволяет сделать Интернет более доступным, удобным, эффективным и «повседневным» для всех и каждого, в том числе и для тех, кто в своей повседневной жизни никогда не пользуется латинским алфавитом.