«Переводы МГИМО»

Internet Governance

УПРАВЛЕНИЕ ИНТЕРНЕТОМ

ПРОБЛЕМЫ, СУБЬЕКТЫ, ПРЕГРАДЫ

Issues, Actors and Divides

Jovan Kurbalija • Eduardo Gelbstein

Йован Курбалийя • Эдуардо Гелбстайн

DiPLO
www.diplomacy.edu

GLOBAL KNOWLEDGE PARTNERSHIP GKP

ББК 32.973
К93

ISBN 99931-53-12-X

Публикация DiploFoundation и Глобального партнерства во имя знания в сотрудничестве с Центром интернет-политики Московского государственного института международных отношений (Университета) МИД России.

DiploFoundation

Мальта:
4th Floor, Regional Building
Regional Rd.
Msida, MSD 13, Malta

Швейцария:
DiploFoundation
Rue de Lausanne 56
CH-1202 Genève 21, Switzerland
E-mail: diplo@diplomacy.edu
Website: http://www.diplomacy.edu

Секретариат Глобального партнерства во имя знания:

Level 23, Tower 2, MNI Twins
11, Jalan Pinang
50450 Kuala Lumpur , Malaysia
E-mail: gkps@gkps.org.my
Website: http://www.globalknowledge.org

Центр интернет-политики Московского государственного института международных отношений (Университета) МИД России

Россия, 119454, Москва, проспект Вернадского, дом 76
E-mail: netpolitics@mgimo.ru
Веб-сайт: http://www.netpolitics.ru

Редакторы: Деян Константинович и Стивен Славик
Иллюстрации: Зоран Марчетич-Марча
Дизайн обложки: Ненад Дошен
Верстка и подготовка к публикации: Лидия Тушек
Научный редактор русского перевода: Михеев А.Н.
Перевод: Михеев А.Н., Лазуткина А.В.
Корректор: Фролов В.Н.
Верстка: Винник Н.В., Головкина М.С.

Содержание

ЧАСТЬ 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

Всего за несколько лет интернет совершил революцию в торговле, здравоохранении, образовании, в самой ткани человеческого общения. Более того, потенциал интернета отнюдь не исчерпывается теми возможностями, свидетелями которых мы стали за относительно непродолжительное время, прошедшее с момента его появления. Регулирование, развитие и защита присутствия интернета в нашей жизни *требует от нас не меньшей изобретательности, чем понадобилась его создателям.* Очевидно, что интернетом необходимо управлять, но это не означает, что к чему-то столь особенному нужно подходить с традиционных позиций.

Кофи Аннан, Глобальный форум по вопросам управления интернетом. (Нью-Йорк, 24 марта 2004 г.)

За относительно недолгое время интернет стал неотъемлемой частью современного общества. На данный момент (середина 2005 г.) интернет можно охарактеризовать следующими параметрами:

- по некоторым оценкам, около миллиарда пользователей по всему миру;
- ежегодный оборот электронной коммерции, который составляет около 150 млрд. долларов и, согласно прогнозам, стремительно возрастет в ближайшие годы;
- крайне важное влияние на общество в сфере образования, здравоохранения, функционирования органов власти и в других сферах деятельности;
- киберпреступность (например, мошенничество), азартные игры, порнография и кража личности;
- ненадлежащее и незаконное использование технологии в форме вредоносного кода (вирусов) и спама.

Интернет и статистика не очень дружны между собой. С самых первых дней существования глобальной сети точно определить число пользователей и веб-сайтов, объем передаваемых данных (трафика), финансовые показатели и большинство других параметров было сложно. К тому же цифрами часто злоупотребляют для создания шумихи вокруг темпов развития Сети. Некоторые исследователи считают причиной роста мыльного пузыря «дот-комов»[1] завышение количественных показателей при оценке потенциала интернета.

Возрастающая информированность о социальном, экономическом и политическом влиянии интернета на общество активизировала внимание к вопросам управления интернетом[2]. Обращение к правовым аспектам и социальным последствиям технологического развития неизбежно отстает от технологических инноваций. Это относится и к интернету.

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;
- защитить пользователей от последствий ненадлежащего и незаконного использования технологии;
- способствовать дальнейшему развитию интернета.

[1] «Дот-ком» (англ. dotcom, dot-com, dot.com. Англоязычный термин происходит от названия домена верхнего уровня «.com», в зоне которого находится основная часть коммерческих сайтов интернета) — неологизм для обозначения компаний, чья бизнес-модель целиком основывается на работе в рамках интернета (в первую очередь, интернет-магазинов). Наибольшее распространение «дот-комы» получили в конце 1990-х гг. на волне повышенного внимания инвесторов к возможностям, предоставляемым интернетом для ведения бизнеса, однако в 2000-2001 гг. большая часть подобных компаний потерпела крах. — *Прим. пер.*

[2] Здесь и далее в тексте используется официальный перевод термина «Internet Governance», употребляющийся в документах Рабочей группы по управлению интернетом (РГУИ). В документах Всемирного саммита по информационному обществу (ВСИО) употребляется также выражение «управление использованием Интернета». В отличие от документов ВСИО мы предлагаем, в соответствии с уже закрепившейся в русском языке тенденцией (нашедшей отражение и в докладе РГУИ), склонять термин «интернет». Мы также предлагаем писать слово «интернет» со строчной буквы, как слова «телефон», «телеграф». — *Прим. пер.*

Сейчас мы находимся на ранней стадии международных переговоров по управлению интернетом. Она характеризуется необходимостью выработки и согласования общих рамок и выбора подходящих инструментов для ведения дискуссии по многим возникающим вопросам. Какие действующие лица вероятнее всего будут оказывать влияние на развитие интернета? Какова будет их политика в отношении обеспечения подключения, коммерции, содержания (контента), финансирования, безопасности и других вопросов, являющихся центральными для появляющегося информационного общества? Это лишь некоторые из ключевых вопросов, ответы на которые необходимо искать в рамках управления интернетом.

ЭВОЛЮЦИЯ УПРАВЛЕНИЯ ИНТЕРНЕТОМ

Одним из поразительных особенностей интернета в период его создания и на ранних этапах развития была уникальная система управления. Интернет начался как правительственный проект. В конце 1960-х гг. правительство США финансировало проект Управления перспективных исследовательских проектов (DARPA)[3] по созданию надежного средства коммуникации, призванного сохранить способность к функционированию даже в случае ядерного удара, в результате чего появилась сеть DARPANet.

К 1980-м годам возможностями этой сети, которую стали называть «Интернет», уже пользовалось более широкое международное сообщество. В 1986 г. была основана Рабочая группа проектирования интернета (РГПИ)[4]. РГПИ управляла последующим развитием интернета, принимая решения на основе сотрудничества и консенсуса, с привлечением широкого круга участников. У интернета не было центрального правительства, централизованного планирования, «великой стратегии».

Подробный обзор эволюции процесса управления интернетом приводится на с. 178—179.

[3] Defense Advanced Research Projects Agency
[4] Internet Engineering Task Force, IETF

Тогда ситуация была относительно простой. Однако в 1994 г. Национальный фонд науки США решил привлечь к обеспечению функционирования интернета частный сектор, передав управление системой доменных имен (DNS)[5] компании Network Solutions Inc. (NSI). Реакция интернет-сообщества на этот шаг была негативной, и началась так называемая «война DNS».

Эта «война DNS» вовлекла в процесс регулирования интернета других участников: бизнес, международные организации и государства. Она закончилась в 1998 г. созданием новой организации — Корпорации по присвоению имен и номеров в интернете (ИКАНН)[6] .

С 1998 г. — года создания ИКАНН — дискуссия по вопросам управления интернетом характеризуется более активным вовлечением национальных правительств, в первую очередь через структуры ООН.

МЕЖДУНАРОДНЫЕ ПЕРЕГОВОРЫ ПО УПРАВЛЕНИЮ ИНТЕРНЕТОМ

Всемирный саммит по информационному обществу (ВСИО)[7], состоявшийся в Женеве в декабре 2003 г., официально включил вопросы управления интернетом в дипломатическую повестку дня. В Декларации принципов и Плане действий, принятых на ВСИО, предлагался ряд мер в области управления интернетом, включая создание Рабочей группы по управлению интернетом (РГУИ)[8] .

Статья Декларации принципов ВСИО, касающаяся управления интернетом, гласит:

> 50. Вопросы управления использованием Интернет на международном уровне следует решать согласованным образом. Мы обращаемся к Генеральному секретарю Организа-

[5] Domain Name System
[6] Internet Corporation for Assigned Names and Numbers, ICANN
[7] Working Group on Internet Governance, WGIG В официальных документах на русском языке используются также аббревиатуры ВСИС (от англ. WSIS) и ВВУИО (сокр. от Всемирная встреча на высшем уровне по вопросам информационного общества). — *Прим.пер.*
[8] Working Group on Internet Governance, WGIG

ции Объединенных Наций с просьбой учредить рабочую группу по управлению использованием Интернет в рамках открытого и всеобъемлющего процесса, обеспечивающего механизм для полномасштабного и активного участия органов государственного управления, частного сектора и гражданского общества как из развивающихся, так и из развитых стран, в том числе соответствующих межправительственных и международных организаций и форумов, в целях изучения вопроса об управлении использованием Интернет и представления к 2005 году в надлежащих случаях предложений для принятия решения в отношении организации управления использованием Интернет.

О том же говорится и в пункте плана действий ВСИО, посвященном управлению интернетом:

13. b) Мы обращаемся к Генеральному секретарю Организации Объединенных Наций с просьбой учредить рабочую группу по управлению использованием Интернет в рамках открытого и всеобъемлющего процесса, обеспечивающего механизм для полномасштабного и активного участия органов государственного управления, частного сектора и гражданского общества как из развивающихся, так и из развитых стран, в том числе соответствующих межправительственных и международных организаций и форумов, в целях изучения вопроса об управлении использованием Интернет и представления к 2005 году предложений для принятия решения в отношении организации управления использованием Интернет. В частности, группе следует:

i) выработать рабочее определение управления использованием Интернет;
ii) выявить вопросы государственной политики, которые относятся к управлению использованием Интернет;
iii) сформировать единое понимание соответствующей роли и сферы ответственности органов государственного управления, существующих межправительственных и международных организаций и других форумов, а также частного сектора

и гражданского общества как из развивающихся, так и из развитых стран;
iv) подготовить отчет о результатах проделанной работы для представления на рассмотрение в ходе второго этапа ВВУИО в Тунисе в 2005 году и принятия соответствующего решения.

ВСИО и Рабочая группа по управлению интернетом представляют собой первый этап процесса управления интернетом, результатом которого должно стать прояснение вопросов, касающихся управления интернетом, определение повестки дня, а также внедрение процедур и механизмов.

Процесс многосторонних переговоров и управление интернетом

СТАДИИ ПЕРЕГОВОРОВ	ДЕЯТЕЛЬНОСТЬ ВСИО
До переговоров	С 1998 по ВСИО в Женеве (2003 г.)
Определение повестки дня и разъяснение вопросов	Начаты в декабре 2003 г. на саммите в Женеве с решения основать РГУИ. Она представила свой доклад в июне 2005 г. Эта стадия процесса должна завершиться в Тунисе.
Поиск формулировок	После Туниса-2005.
Обсуждение деталей	
Заключение соглашения	
Реализация	

ЧТО ОЗНАЧАЕТ ТЕРМИН «УПРАВЛЕНИЕ ИНТЕРНЕТОМ»?

На Глобальном форуме по управлению интернетом, состоявшемся в ООН в Нью-Йорке 24—25 марта 2004 г., некоторые из выступавших приводили различные варианты истории о слепцах и слоне.

Мораль стихотворения применительно к проблематике управления интернетом такова: обсуждение значения термина «управление интернетом» — не просто дань лингвистическому педантизму. Различное понимание значения этого термина порождает различные ожидания и различные подходы к выработке политического курса.

Специалисты по телекоммуникациям рассматривают управление интернетом сквозь призму развития технической инфраструктуры.

Профессионалы в области компьютерных технологий в основном уделяют внимание разработке различных стандартов, языков и приложений — таких, как XML или Java. Специалисты в сфере 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 технооптимизме (больше компьютеров — больше образования) и угрозах (безопасность интернета, защита детей). Дипломатов в первую очередь беспокоят сам процесс регулирования и защита национальных интересов. Список потенциально противоречащих друг другу профессиональных точек зрения на управление интернетом можно продолжить.

Шесть мудрецов из Индостана,
Любовь к познанию питая,
Отправились к слону
(хоть были все слепыми),
Чтобы свои теории проверить.
……
Так мудрецы из Индостана
В горячих спорах
Стояли твердо на своем.
Был каждый в чем-то прав,
Но ошибались все.

Отрывок из стихотворения «Слепцы и слон» американского поэта Джона Годфри Сакса (1816-1887) в вольном переводе Валерия Земских; полный текст см. в Приложении I.

РГУИ выработала следующее рабочее определение управления интернетом: «Управление интернетом представляет собой разработку и применение правительствами, частным сектором и гражданским обществом, при выполнении ими своей соответствующей роли, общих принципов, норм, правил, процедур принятия решений и программ, регулирующих эволюцию и применение интернета».

Это рабочее определение является хорошей отправной точкой для дискуссий по теме, которые неизбежно приведут к более тщательному определению значений обоих ключевых понятий: «интернет» и «управление».

Каждый из терминов: «интернет» и «управление» (governance) — допускает спорные трактовки. Некоторые авторы утверждают, что по-

нятие «интернет» не охватывает все существующие аспекты глобального развития информационно-коммуникационных технологий (ИКТ). Обычно в качестве более полных предлагаются два других термина: «информационное общество» и «информационно-коммуникационные технологии». Они включают в себя области, выходящие за пределы непосредственно интернета, — такие, как мобильная связь.

Однако в пользу употребления термина «интернет» свидетельствует стремительный переход глобальных коммуникаций к использованию протокола TCP/IP как основного технического стандарта коммуникаций. Вездесущий интернет продолжает распространяться с огромной скоростью с точки зрения не только количества пользователей, но и предлагаемых услуг, среди которых наиболее заметен протокол передачи голоса по интернету (VoIP)[9] , способный заменить обычную телефонную связь.

Термин «управление» был предметом противоречий в недавних дискуссиях, в особенности в рамках ВСИО. Основным источником непонимания является использование термина «управление» (governance) как синонима «правительства» (government). Когда термин «управление интернетом» появился в процессе ВСИО, многие страны, особенно развивающиеся, связали его с понятием правительства. Одним из последствий такого подхода стало убеждение в том, что вопросы управления интернетом необходимо решать на межправительственном уровне, при ограниченном участии других участников, в первую очередь неправительственных.

Каковы основные причины этой терминологической путаницы? Разьве не очевидно, что «управление» не означает «правительство»? Не обязательно. Термин «надлежащее управление» (good governance) использовался Всемирным банком для продвижения реформ в государственном аппарате, нацеленных на повышение прозрачности, уменьшение коррупции и повышение эффективности деятельности чиновников. В этом контексте термин «управление» был непосредственно связан с ключевыми правительственными функциями.

[9] Voice over Internet Protocol

Другим потенциальным источником путаницы является перевод термина «управление» (governance) на другие языки. В испанском языке этот термин относится преимущественно к государственной деятельности или правительству (*gestión pública, gestión del sector público* и *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* и *mode de gouvernement).* Похожая ситуация наблюдается и в португальском языке: налицо связь с государственным сектором и правительством (*gestão pública* и *administração pública*). Такое несоответствие переводов термина «управление» может дать лингвистическое объяснение тому, почему многие делегаты ВСИО связывали вопросы управления интернетом с государственным сектором и обсуждение вращалось вокруг необходимости правительственного вмешательства.

ИНСТРУМЕНТАРИЙ УПРАВЛЕНИЯ ИНТЕРНЕТОМ

Режим управления интернетом находится на очень ранней стадии развития. Опыт других международных режимов (например, в области окружающей среды, воздушного транспорта, контроля над вооружениями) показывает, что в рамках режимов часто создаются общая система взглядов, ценностей, представлений о причинно-следственных связях, единые способы аргументации, терминология, специальная лексика, жаргон и сокращения.

Во многих случаях на эти общие рамки влияет специфическая профессиональная культура (способ мышления и поведения, общие для представителей одной профессии). Установление 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 будет включать множество вопросов, участников, механизмов, процедур и инструментов.

У вопросов, связанных с интернетом, есть по меньшей мере пять измерений: инфраструктурное, правовое, экономическое, связанное с развитием и социокультурное. Каждое из них обсуждается в последующих главах. В каждом из этих измерений участвует множество лиц — как в частном, так и в государственном секторе. Большинство из них (операторы «корневых» серверов, интернет-провайдеры, специалисты по вопросам защиты торговых марок и проблемам развития, активисты гражданского общества и т. д.) принадлежат к очень специфическим и развитым профессиональным культурам.

Различные сочетания вопросов и участников имеют свои цель, задачи, терминологию и сферы сотрудничества и влияния. Кажется, что в настоящий момент очень многие из таких сочетаний существуют в относительной изоляции от остальных. Добавьте к этому количество «рабочих» языков, отражающих глобальную природу проблемы — и задача упорядочивания всех этих элементов в цельную архитектуру управления многократно усложняется (хотя, при условии наличия доброй воли у всех сторон, остается решаемой).

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

Сложность управления интернетом показывает, что мышление линейное, основанное на поиске единственной причины и подходе «или—или», не годится для решения соответствующих вопросов. Поэтому требуются новые инструменты познания, адекватные этой сложности и предлагающие общие подходы и руководящие принципы.

Основные цели создания такого «набора инструментов» для управления интернетом таковы:

- упорядочить инструменты, используемые в настоящий момент в дискуссиях по управлению интернетом;
- создать дополнительные инструменты познания;
- способствовать включению в процесс управления интернетом новых участников, предоставив им такие инструменты и тем самым помогая им лучше понять сущность проблем, позиций и происходящих изменений.

Инструментарий управления интернетом состоит из:

- моделей и подходов;
- руководящих принципов;
- аналогий.

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 сложилось несколько подходов и моделей, представляющих собой те измерения, по которым можно обнаружить различия между позициями участников переговоров, а также между профессиональными и национальными культурами. Выявление общих подходов и моделей может уменьшить степень сложности переговоров и помочь выстроить общую «систему координат».

До сегодняшнего дня противостояние между «узким» и «широким» подходами к управлению интернетом является одним из основных вопросов, отражающих различные интересы в процессе управления интернетом. При «узком» подходе внимание обращается в первую очередь на инфраструктуру интернета (систему доменных имен, IP-адресов и «корневых» серверов) и на позицию ИКАНН 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. Проведение различия между этими двумя подходами особенно важно на ранней стадии переговоров — при определении повестки дня.

«Широкий» подход неявно поддержан в Декларации ВСИО, давшей РГУИ мандат на «определение проблем государственной политики, касающихся управления интернетом». Этот подход также преобладает в политических и научных дискуссиях по вопросам управления интернетом.

Сегодня дискуссия перешла от стадии «или—или» к стадии определения приоритетов и наиболее приемлемого баланса между «узким» (вопросы, связанные с ИКАНН) и «широким» (другие аспекты управления интернетом) подходами.

Технические и политические аспекты

Интеграция технических и политических аспектов с точки зрения процесса управления интернетом является серьезным вызовом, поскольку провести четкую границу между ними сложно. Технические решения не являются нейтральными. В конечном счете любое техническое решение способствует доминированию чьих-то интересов, усиливает позицию определенных групп и в известной степени влияет на общественную, политическую и экономическую жизнь.

Известны случаи, когда первоначальная политическая цель, определявшая техническое решение, изменялась. Например, архитек-

тура интернета, основанная на сквозной передаче данных и пакетной коммутации, разрабатывалась с политической целью создать надежную сеть, способную пережить ядерный удар. Та же архитектура впоследствии стала основой для развития творчества и свободы выражения убеждений в интернете.

Другие технические решения — такие, как электронные средства защиты авторских прав, — создаются сознательно, для замены определенных политических решений или обеспечения их выполнения (в данном случае в области защиты авторских прав).

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 новых заинтересованных сторон, в первую очередь бизнес-сектора и правительств, в 1990-х гг. единство технологии и политики было нарушено. Чтобы восстановить баланс, была проведена реформа системы управления интернетом, включая создание ИКАНН. Эта проблема остается открытой и, скорее всего, будет одной из потенциально спорных тем в рамках ВСИО/РГУИ.

Старый «реальный» подход и новый «кибер-подход»

Практически любой вопрос в рамках управления интернетом можно рассмотреть двояко. Сторонники старого «реального» подхода — по принципу «новое вино в старые меха» — доказывают, что интернет не привнес ничего нового в сферу управления. Интернет, с точки зрения регулирования, — еще одно техническое устройство, не отличающееся от предшественников: телеграфа, телефона или радио.

Например, в дискуссиях по юридическим аспектам сторонники этого подхода указывают, что существующие законы с небольшой корректировкой могут быть применены и к интернету. Поскольку интернет связан с коммуникацией между людьми, он не отличается от телефона или телеграфа и может регулироваться, как и любое другое средство коммуникации. В области экономики приверженцы этого подхода утверждают, что разницы между обычной и

«электронной» коммерцией нет. Следовательно, нет необходимости специального правового регулирования электронной коммерции. Сторонники старого «реального» подхода выступают также против мораториев на налогообложение электронной коммерции.

Приверженцы нового «кибер-подхода» (назовем его «новое вино в новые меха») доказывают, что интернет — принципиально новая технология по сравнению со всеми предшествующими. Поэтому она требует принципиально иного регулирования. Этот подход был особенно популярен в первые годы существования интернета. Были даже надежды на то, что новаторский способ управления интернетом — «согласие в целом и работающий код» (rough consensus and running code) — может стать моделью регулирования других областей человеческой деятельности. Основная посылка нового «кибер-подхода» состоит в том, что интернет отделил нашу социальную и политическую реальность от мира суверенных государств. Киберпространство отличается от реального мира, а потому требует иной формы управления.

Преобладание этого подхода было заметно в процессе создания ИКАНН, где, например, влияние правительств «реальных» государств было минимизировано. «Кибер-подход» был смягчен реформой ИКАНН в 2002 г., которая расширила полномочия правительств и приблизила ИКАНН к политической реальности.

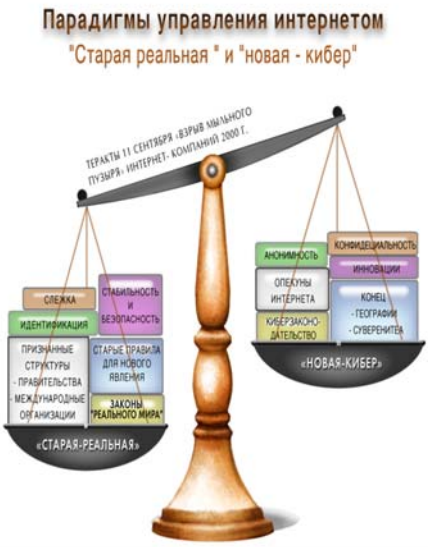
Обращаясь к области права, представители «кибер-подхода» утверждают, что существующие законы, касающиеся юрисдикции, киберпреступности и заключения контрактов, не могут применяться к интернету, а потому должны быть созданы новые законы.

Учитывая постоянное взаимодействие этих двух походов, весьма вероятно, что противостояние старого «реального» и нового «кибер-подходов» не исчезнет и будет существенно влиять на переговоры по управлению интернетом.

Децентрализованная и централизованная структура управления интернетом

В соответствии с децентрализованным подходом структура управления должна отражать саму природу интернета: сеть сетей. Столь

сложную систему невозможно поместить под единый «зонтик» управления, например, в рамках международной организации. Однако 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 централизованного подхода апеллируют, среди прочего, и к практической сложности, которая для стран с ограниченными людскими и финансовыми ресурсами заключается в необходимости 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 ИКАНН, W3C[10] и РГПИ. Такие страны (в основном развивающиеся) выступают за принцип «единого окна», предпочтительно в виде международной организации.

Интернет и общественное благо

Основная часть технической инфраструктуры, через которую идут передаваемые по интернету данные (трафик), находится в собственности частных или государственных компаний, чаще всего телекоммуникационных. Это можно сравнить с транспортной компанией, перевозящей контейнеры. Однако маршруты перевозок являются открытыми и регулируются морским правом, в соответствии с которым открытое море является *res communis omnium*[11],

[10] World Wide Web Consortium — организация, создающая и развивающая стандарты для WWW (основной части интернета), такие как HTML, CSS, XML и другие. — *Прим. пер.*

[11] Общая вещь, общее достояние (лат.) — *Прим. пер.*

в то время как сетевыми «магистралями» (backbones), по которым перемещаются данные, владеют телекоммуникационные компании. Это вызывает ряд вопросов:

- Можно ли обязать частные компании управлять своей частной собственностью — интернет-магистралями — в общественных интересах?
- Может ли интернет (или его части) считаться глобальным общественным благом?
- Можно ли применить старую концепцию римского права *res communis omnium* к интернету, как это было в случае с морским правом?

Наиболее сложными аспектами в этой дилемме общественного и частного являются, с одной стороны, создание необходимой для коммерческой деятельности частного сектора среды, а с другой — обеспечение дальнейшего развития интернета как общественного ресурса, состоящего из знаний и информации, которые являются общественным достоянием. Больше по этому вопросу см. на с. 167.

География и интернет

На заре развития интернета было распространено мнение о том, что эта глобальная сеть преодолевает национальные границы и разрушает принцип суверенитета. В своей знаменитой «Декларации независимости киберпространства» Джон Перри Барлоу обратился ко всем правительствам с таким посланием: «Вы лишние среди нас. Вы не обладаете верховной властью там, где мы собрались. Вы не имеете ни морального права властвовать над нами, ни методов принуждения, которые действительно могли бы нас устрашить. Вы не знаете ни нас, ни нашего мира. Киберпространство лежит вне ваших границ»[12] .

Эта декларация — пример преобладавшего в середине 1990-х годов технооптимизма. С момента появления декларации Барлоу произошло многое, в том числе появилось сложное геолокационное программное обеспечение. Сегодня все еще сложно определить точно, кто на-

[12] Перевод Е. Горного. Опубликовано в Zhurnal.ru #1, 2 октября 1996 г. (http://www.zhurnal.ru/1/deklare.htm).

ходится «с той стороны экрана», но достаточно просто понять, через какого провайдера этот человек получил доступ в интернет. К тому же недавние законодательные акты ряда стран требуют, чтобы провайдеры идентифицировали пользователей и предоставляли по запросу властей необходимую информацию о своих клиентах.

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 проще — с опорой на существующие законы.

«Делай то, что проповедуешь»

Принцип «делай то, что проповедуешь» предполагает использование онлайн-инструментов для переговоров по вопросам виртуального мира. Процесс переговоров по управлению интернетом представляет существенную сложность с точки зрения многосторонней дипломатии и требует использования как проверенных и эффективных методов и инструментов переговоров, так и новаторских подходов. Одной из основных инноваций в этой области может быть использование онлайн-инструментов при переговорах.

Применение интернет-технологий должно способствовать участию в переговорах широкого круга заинтересованных лиц, в особенности тех, кто не имеет возможности принимать участие в традиционных дипломатических конференциях. Поэтому необходимо содействовать участию развивающихся стран в процессе управления интернетом.

РУКОВОДЯЩИЕ ПРИНЦИПЫ

Руководящие принципы представляют собой определенные ценности и интересы, утверждению которых должен способствовать складывающийся режим управления интернетом. Некоторые из этих принципов — такие, как прозрачность и открытость для участия, были одобрены на ВСИО. Другие были внедрены неявно, в дискуссиях 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.

1) созданные специально для интернета (например, ИКАНН);
2) требующие существенной адаптации для применения к связанным с интернетом вопросам (например, защита торговых марок, налогообложение электронной коммерции);
3) применимые к интернету без существенных изменений (например, защита свободы слова).

Использование существующих норм существенно повысило бы правовую стабильность и уменьшило бы сложность 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, ведущих к большей функциональности и легитимности. Общепризнано, что стабильность и функциональность интернета должны выступать одними из руководящих принципов управления им. Стабильность интернета должна быть сохранена путем использования давно известного подхода «работающего кода», предполагающего постепенное внедрение тщательно проверенных изменений в техническую инфраструктуру.

Однако некоторые озабочены тем, 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).

Управление интернетом и развитие

Ряд вопросов, поднимаемых в сегодняшних дискуссиях по управлению интернетом, имеет непосредственное отношение к проблемам развития. Среди них: плата за подсоединение (interconnection charges), распределение IP-адресов, инвестиции, защита интеллектуальной собственности, способствование развитию электронной коммерции. Процесс управления интернетом должен руководствоваться общими целями ВСИО в области развития и «Целями Тысячелетия» ООН.

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. Также необходимо учитывать активное сближение цифровых технологий, включая перевод телекоммуникационных услуг на использование интернет-протоколов.

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).

«За деревьями не видно леса»

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

РУКОВОДЯЩИЕ ПРИНЦИПЫ ИКАНН

«Белая книга» по управлению интернетом, подготовленная правительством США в 1998 г., определяет следующие руководящие принципы, относящиеся к созданию ИКАНН:

- Стабильность: функционирование интернета не должно быть нарушено собенно 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.

Делайте подразумеваемые технические решения ясными политическими принципами

В интернет-сообществе весьма распространено мнение о том, что особенности технического устройства интернета («сквозной» принцип) способствуют распространению определенных общественных ценностей, например свободы общения. 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. Такой при-

нцип, как свобода коммуникации, должен быть четко обозначен на политическом уровне, а не предполагаться неявно, на техническом уровне.

Принцип технологической нейтральности

В соответствии с данным принципом, тесно связанным с предыдущим, политика не зависит от конкретных технологических или технических устройств. Например, правовые нормы в области защиты тайны 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. Во-первых, она отделяет управление от какой-либо конкретной технологии и учитывает возможность технологических изменений в будущем. Во-вторых, технологическая нейтральность является наиболее подходящим принципом регулирования в условиях начавшегося слияния основных технологий (телекоммуникации, СМИ, интернет и т. д.).

В Европейском Союзе технологическая нейтральность обозначена в качестве одного из краеугольных камней телекоммуникационной политики. Хотя адекватность принципа технологической нейтральности задачам управления интернетом очевидна, сложности при переходе от существующих в области телекоммуникаций норм к новым неизбежны. Это уже проявляется в таких областях, как интернет-телефония (VoIP).

Риск управления обществом через программный код

Лоренс Лессиг[13] 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 програм-

[13] Известный американский специалист по юридическим аспектам информационных технологий, профессор права Стэндфордского университета. — *Прим. пер.*

мным кодом, а не законами. Некоторые законодательные функции парламентов и правительств могут *де факто* принять на себя компьютерные компании и разработчики программного обеспечения. Используя программное обеспечение и технические решения, 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*

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 мыслительным 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), «всемирную паутину» WWW (см. аналогию с теле- и радиовещанием) и базы данных (см. аналогию с библиотекой). Любая аналогия с какой-либо одной технологией может излишне упростить понимание интернета.

Во-вторых, по мере сближения различных телекоммуникационных и медиауслуг 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 являются 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, 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, содержание интернет-коммуникации 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 (МСЭ).

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.

Председатель ИКАНН Пол Туоми привел такую аналогию между почтовой системой и функциями ИКАНН: «Если представить себе интернет в виде почтовой системы, 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 ИКАНН. Ее функция — гарантировать, что письмо дойдет по адресу».

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.

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: Как и в случае с телефоном, интернет — гораздо более широкое понятие, 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 за 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 (Communications Decency Act), предусматривавший тщательный контроль за содержанием материалов интернета, чтобы предотвратить возможность 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», «кибер-библиотека», «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). В интернете же редакторов нет;
- материалы библиотеки организованы определенным образом, облегчающим их поиск. В интернете, помимо нескольких каталогов (таких, как Yahoo! и Google), индексирующих лишь небольшую часть доступной информации, такой схемы классификации нет;
- помимо библиографических описаний содержание материалов библиотеки (текст книг и статей) не доступно 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.)

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 (DMCA)[14], который устанавливал ответственность организаций,

[14] Digital Millennium Copyright Act

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 «peer-to-peer» (непосредственно между компьютерами пользователей), такого, как Grokster и StreamCast.

Интернет — магистраль

Общие черты: Эта аналогия тесно связана с американской культурой и тем значением, которое в ней придается автомагистралям и железным дорогам; она показывает, насколько американцы очарованы идеей открытий и достижения новых рубежей.

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 годов, 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.

КЛАССИФИКАЦИЯ ВОПРОСОВ УПРАВЛЕНИЯ ИНТЕРНЕТОМ

Управление интернетом — сложная новая область, требующая предварительного «нанесения на карту» и классификации. Слож-

ность управления интернетом связана с его междисциплинарной природой, охватывающей технологию, общественно-экономические вопросы, развитие, право и политику.

Составление «карты» управления интернетом имеет как научную, так и практическую важность. С научной точки зрения, появляется все больше исследований по вопросам управления интернетом, однако они в основном посвящены ИКАНН и другим проблемам, рассматриваемым в рамках «узкого» похода. По-прежнему отсутствует общая теоретическая схема, в особенности применительно к международным аспектам управления интернетом. Практическая потребность в классификации ярко проявилась в процессе ВСИО. Многим участникам, включая государства, было непросто разобраться во всех сложностях управления интернетом. Составление концептуальной схемы проблемного поля должно способствовать повышению эффективности переговоров в контексте ВСИО, а также других многосторонних переговоров по вопросам, связанным с интернетом.

Такая классификация может помочь участникам процесса управления интернетом:

- четко определить основные вопросы, требующие обсуждения;
- снизить уровень переговорного «шума», вызванного непоследовательной трактовкой основных концепций;
- избежать дублирования, когда одни и те же вопросы рассматриваются на нескольких форумах;
- поддержать необходимое равновесие между широким подходом и конкретными вопросами, избежав тем самым ситуации, когда «за деревьями не видно леса».

В конечном счете тщательная подготовка перечня связанных с интернетом вопросов должна сделать процесс переговоров по управлению интернетом более эффективным. С экономической точки зрения, это должно снизить транзакционные издержки — иными словами, сократить общее время переговоров. Это особенно важно для стран с ограниченными финансовыми и людскими ресурсами, поскольку позволит им принимать более активное участие в управлении интернетом. Неясный и запутанный процесс переговоров требует непропорционально больших затрат людских ресурсов и времени.

Разработанная DiploFoundation классификация аспектов управления интернетом разбивает все вопросы 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.

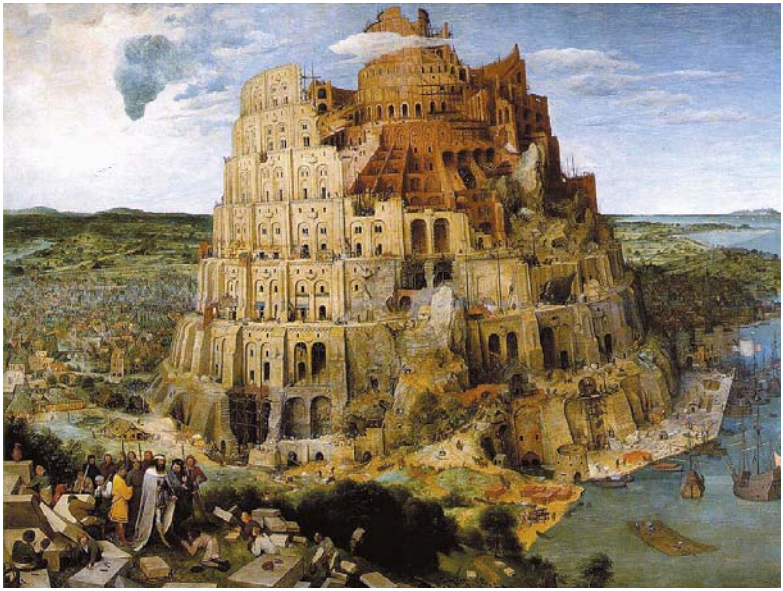
Модель «пяти корзин» метафорически представлена иллюстрацией «Строящееся здание» на странице 37.

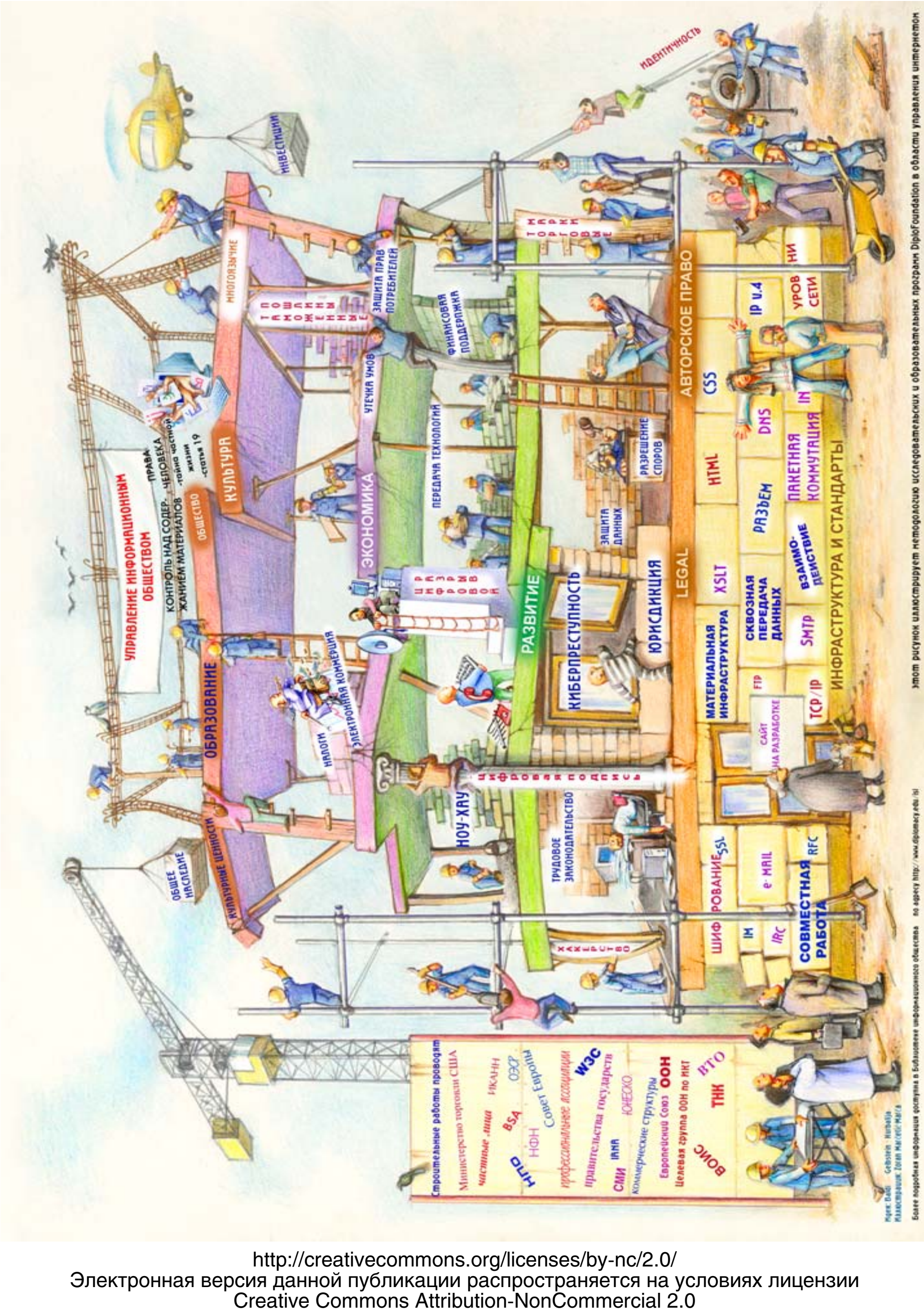
Разработанная Diplo классификация аспектов управления интернетом является концептуальной основой подхода Diplo к этой области в целом, включая образование, профессиональную подготовку, исследования и разработку инструментария. С момента ее появления эта классификация использовалась авторами курсов, на которых обучалось более 300 студентов, а также многими исследователями. Эта схема постоянно перерабатывается с учетом множества комментариев. Таким образом, современная классификация основана на многочисленных повторениях, а также на накопленных знаниях и опыте.

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

Картина Питера Брегеля-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 (Бытие 11, 5-7), Бог не позволил людям достроить башню, смешав язык строителей, «так чтобы один не понимал речи другого».

Аналогия со строительством Вавилонской башни кажется весьма уместной при рассмотрении вопросов, связанных с интернетом. Это сравнение натолкнуло авторов на образ другого строящегося здания, цель которого не достичь небес, но по крайней мере 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.





ЧАСТЬ 2

Инфраструктура и стандартизация

КОРЗИНА «ИНФРАСТРУКТУРА И СТАНДАРТИЗАЦИЯ»

Корзина «инфраструктура и стандартизация» включает в себя основополагающие, в основном, технические вопросы, связанные с функционированием интернета. На рисунке «Строящееся здание», иллюстрирующем управление интернетом, первый этаж представляет собой вопросы инфраструктуры и стандартизации (см. с. 37). Проблемы, относящиеся к этой корзине, можно разделить на две группы.

Первая, включающая в себя наиболее важные вопросы, без решения которых ни интернет, ни WWW не могли бы существовать, представлена следующими тремя уровнями, или слоями:

1. Телекоммуникационная инфраструктура, по которой передаются все информационные потоки (трафик).
2. Технические стандарты и услуги — инфраструктура, благодаря которой интернет работает (например, TCP/IP, DNS, SSL).

Одной из сильных сторон интернета является его многоуровневая архитектура. Уровень интернет-инфраструктуры не зависит от телекоммуникационной инфраструктуры (нижний слой) и стандартов приложений (верхний слой).

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, включая безопасность, шифрование данных и борьбу со спамом.

ТЕЛЕКОММУНИКАЦИОННАЯ ИНФРАСТРУКТУРА

СОВРЕМЕННОЕ СОСТОЯНИЕ

Информационные потоки интернета 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 электрическая сеть! Стремительный рост интернета вызвал существенное увеличение потенциала телекоммуникаций. По некоторым оценкам, с 1998 г. телекоммуникационный потенциал вырос в 500 раз благодаря технологическим инновациям и инвестициям в новое оборудование.

Поскольку передача интернет-трафика опирается на уровень телекоммуникаций, любые новые меры регулирования телекоммуникационных услуг неизбежно влияют и на интернет. Телекоммуникационная инфраструктура регулируется целым рядом государственных и частных организаций как на национальных, так и на международном уровнях.

Традиционно международные телекоммуникации координировал Международный союз электросвязи (МСЭ), который разработал подробные правила, регулирующие отношения между национальными операторами, распределение радиочастот и положение спутников.

Однако впоследствии в сфере телекоммуникаций возобладал либеральный подход. На международном уровне процесс либерализации был формализован в 1998 г. Соглашением по основным телекоммуникациям (BTA)[1], заключенным в рамках Всемирной торговой организации (ВТО). После заключения BTA более 100 стран начали процесс либерализации, характеризующийся приватизацией национальных телекоммуникационных монополий, внедрением конкуренции и созданием национальных регулирующих органов.

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, для обеспечения функционирования интернета.

ВТО постепенно заняла центральное место в международном режиме телекоммуникаций, традиционно регулировавшемся МСЭ. Однако роли ВТО и МСЭ существенно отличаются. МСЭ устанавливает детально разработанные технические стандарты, международные нормы, касающиеся непосредственно телекоммуникаций, и предоставляет помощь развивающимся странам. ВТО же задает рамки общих правил рынка.

Вследствие либерализации почти полная монополия МСЭ как основного института, разрабатывающего стандарты телекоммуникаций, была подорвана другими профессиональными организациями и группами — такими, как Европейский институт стандартизации электросвязи (ETSI)[2], разработавший стандарты GSM, Институт инженеров по электротехнике и электронике (IEEE)[3], разработавший стандарты WiFi, и Рабочая группа проектирования интернета (РГПИ)[4], создавшая TCP/IP и другие протоколы интернета.

[1] Basic Telecommunications Agreement
[2] European Telecommunications Standardization Institute
[3] Institute of Electrical and Electronics Engineers
[4] Internet Engineering Task Force, IETF

Либерализация национальных рынков телекоммуникаций дала крупным телекоммуникационным компаниям (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 управление интернетом.

ВОПРОСЫ

«Последняя миля» — местные линии связи

«Последней милей» (или, по-английски, «местной петлей» — local loop) называется линия связи между интернет-провайдером и индивидуальным пользователем. Проблемы с местными линиями связи являются препятствием для более широкого распространения интернета во многих (чаще — в развивающихся) странах. Причина обычно заключается в недоразвитости национальной телекоммуникационной инфраструктуры. В некоторых развивающихся странах с обширной территорией удаленные города и деревни сложно подключить с помощью традиционных наземных линий связи.

В качестве наилучшего решения проблемы «последней мили» все чаще называется 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.

Предполагается, что 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 беспроводной 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 в процессе установления и внедрения стандартов на столь быстро развивающемся рынке дает им возможность оказывать существенное влияние на него.

Технология, стандарты и политика

Дискуссия о сетевых протоколах демонстрирует, как стандарты предстают «политикой иных средств». 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 ожидания и конфликты интересов. Сам пыл, с которым заинтересованные стороны спорят по поводу тех или иных решений в отношении стандартов, служит для нас знаком того, что за чисто техническими решениями скрывается более глубокий смысл.
Источник: Janet Abbate. Inventing the Internet. MIT Press, 1999.

ТЕХНИЧЕСКИЕ СТАНДАРТЫ И УСЛУГИ (Инфраструктура интернета)

На этом уровне интернет обретает «форму». Большинство относящихся к этому уровню задач — базовые вопросы управления интернетом, обычно перечисляющиеся в рамках «узкого» подхода. Они подразделяются на две группы. Первая включает в себя ключевые вопросы, связанные с техническими стандартами и услугами (TCP/IP, DNS и «корневые» серверы), а вторая касается коммерческих аспектов интернет-инфраструктуры, включая роль провайдеров интернет-услуг и оптовых провайдеров услуг широкополосной связи, а также экономические аспекты обеспечения подключения к интернету (плата за подключение и использование коммутационных станций интернета — КСИ)[5] .

Из всех организаций наиболее часто в контексте дискуссий по управлению интернетом упоминается, пожалуй, ИКАНН. Причина этого заключается в центральной роли этой организации в управлении системой числовых адресов (IP-адресов) и доменных имен.

Противоположные взгляды на роль ИКАНН в управлении интернетом

УЗКИЙ-ТЕХНИЧЕСКИЙ	ШИРОКИЙ-ПОЛИТИЧЕСКИЙ
ИКАНН является всего лишь координирующим органом, осуществляющим техническое администрирование в сфере IP-адресов и доменных имен. С этой точки зрения, ИКАНН только координирует интернет, но не управляет им.	Деятельность ИКАНН включает в себя больше, чем просто техническую координацию. Хотя за ИКАНН необходимо сохранить осуществление таких ключевых технических функций, как управление «корневыми» серверами и распределение IP-адресов, политика должна вырабатываться легитимным международным органом, представляющим все государства. Это может быть сделано или через систему ООН, или через специально созданную международную структуру.
Кто придерживается такого мнения: ИКАНН, «Сообщество интернета»[6], правительство США, правительства других промышленно развитых стран.	*Кто придерживается такого мнения*: в основном развивающиеся страны

[5] Internet eXchange Points, IXPs

[6] «Сообщество интернета» (Internet Society, ISOC) — профессиональная некоммерческая организация, членами которой являются более 100 организаций и 20000 частных лиц из 180 стран. Деятельность ISOC направлена на содействие использованию и развитию интернета, распространение обучающих материалов и организацию конференций и форумов по связанной с интернетом тематике. ISOC также координирует деятельность РГПИ и Internet Architecture Board. — *Прим. пер.*

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

СОВРЕМЕННОЕ СОСТОЯНИЕ

TCP/IP — основной технический стандарт интернета, определяющий способ передачи данных по интернету. Этот протокол основан на трех принципах: пакетная коммутация, сквозная передача данных и устойчивость к помехам.

Для передачи данных по интернету используется метод *пакетной коммутации*. Все данные, отправляемые с компьютера, разбиваются на небольшие блоки (пакеты), которые перемещаются по интернету, а затем, достигнув компьютера назначения, собираются воедино.

Сквозная передача данных означает, что вся сложность, интеллектуальность и инновации связаны с конечными точками сети. Благодаря этому принципу в интернете возможны самые разнообразные инновации. Сеть является нейтральной и не препятствует развитию и творчеству в этих конечных точках. Это означает, что приложение, работающее через интернет, может разрабатываться в конечных точках сети без необходимости получения разрешения от сетевых операторов или любой другой стороны.

Устойчивость к помехам достигается за счет динамической маршрутизации. Первоначально этот принцип был использован в предшественнике интернета ARPANET для того, чтобы создать устойчивую к повреждениям военную систему, способную пережить возможный ядерный удар. Динамическая маршрутизация использовалась для связи сетей различных типов.

Управление интернетом в том, что касается протокола TCP/IP включает в себя два важных компонента: внедрение новых стандартов и распределение IP-адресов. Стандарты для TCP/IP устанавливаются РГПИ. Поскольку протокол TCP/IP имеет принци-

пиальное значение для функционирования интернета, он строго охраняется РГПИ.

IP-адреса — это числовые адреса, которые должны иметь все компьютеры, подключенные к сети. IP-адреса уникальны; два компьютера, подключенные к интернету, не могут иметь одинаковый IP-адрес. Это делает IP-адреса потенциально дефицитным ресурсом.

Система распределения IP-адресов организована иерархически. «Наверху» находится Администрация по присвоенным именам в интернете (IANA)[7], являющаяся дочерней структурой ИКАНН. IANA распределяет блоки IP-адресов по региональным интернет-регистратурам. На сегодняшний день это Американская регистратура интернет-номеров (ARIN), Сетевой информационный центр Азиатско-Тихоокеанского региона (APNIC), Региональная регистратура IP-адресов Латинской Америки и Карибского бассейна (LACNIC) и Сетевой координационный центр «Reseaux IP Européens», отвечающий за Европу и Ближний Восток (RIPE NCC). Африканская регистратура (AFRINIC) в настоящий момент только создается.

Региональные интернет-регистратуры распределяют IP-адреса по крупнейшим интернет-провайдерам, а также национальным и местным интернет-регистратурам. Ниже по иерархической лестнице находятся более мелкие интернет-провайдеры, компании и частные лица.

ВОПРОСЫ

Достаточно ли IP-адресов?

На сегодняшний день при использовании IPv4 (интернет-протокола версии 4) общее количество IP-адресов составляет около 4 миллиардов и может быть исчерпано с появлением связанных с интернетом устройств — таких, как мобильные телефоны, карманные компьютеры, игровые приставки и бытовые электроприборы.

[7] Internet Assigned Numbers Authority

Озабоченность тем, что IP-адреса могут закончиться (что в итоге воспрепятствует дальнейшему развитию интернета), заставила техническое сообщество предпринять два важных шага.

Первый — рационализация использования существующего запаса IP-адресов. Это было достигнуто за счет использования технологии преобразования сетевых адресов (NAT)[8], дающей возможность подключать частную сеть (например, компании или университета) всего через один IP-адрес. Без использования NAT каждому компьютеру в частной сети понадобился бы свой IP-адрес.

Вторым шагом было внедрение новой версии интернет-протокола IPv6, которая предоставляет гораздо больший запас IP-адресов (430 000 000 000 000 000 000).

Такие действия являются примером быстрого и упреждающего решения проблемы. Техническое интернет-сообщество избрало подход «лучше обезопаситься, чем сожалеть» (известный в экологической дипломатии как принцип предосторожности), хотя не было ясно, как быстро закончатся IP-адреса в системе IPv4.

Однако если те, кто распределяет IP-адреса на местном уровне (например интернет-провайдеры), станут злоупотреблять своей властью и начнут присваивать адреса, например, только при условии приобретения других услуг (что, естественно, повлияет на доступность и стоимость IP-адресов), это повлечет за собой искусственный дефицит адресов.

Изменение в TCP/IP и безопасность интернета

Безопасность не входила в список важных вопросов первых разработчиков интернета, поскольку в то время интернет состоял из закрытой сети исследовательских институтов. Безопасность обеспечивалась преимущественно за счет ог-

[8] Network Address Translation

раничения физического доступа к сетям и подключенным компьютерам, которые использовались небольшой группой специалистов. Данные передавались без какой-либо специальной защиты.

Распространение интернета привело к росту числа пользователей, многократно превышающему представления первых разработчиков (порядка миллиарда пользователей по всему миру). Интернет превратился также в важный коммерческий инструмент.

Все это вывело проблему безопасности на одно из первых мест в списке вопросов по управлению интернетом. Уровень безопасности постепенно повышался за счет разнообразных решений, большей частью создававшихся «по случаю», для конкретных ситуаций. Некоторые из них — «брандмауэры», антивирусное и шифровальное программное обеспечение — оказались весьма эффективными.

Поскольку архитектура интернета создавалась без учета вопросов безопасности, встраивание в нее соответствующих инструментов потребует существенного изменения самой основы интернета, 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.

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. Такое качество определяется доступностью (время бесперебойного функционирования), пропускной способностью (объем передаваемых данных за единицу времени), вре-

менем задержки (запаздывания) и количеством ошибок. Это особенно важно для приложений, где задержка недопустима, например, при передаче репортажа в режиме реального времени. «Застывшее» или замедленное изображение, эхо при передаче звука — все это последствия недостаточной пропускной способности. Обеспечение качества услуг может потребовать изменений в интернет-протоколах, включая частичный отказ от одного из ключевых принципов интернета — сквозной передачи данных.

ВОЗМОЖНЫЕ ВАРИАНТЫ РАЗВИТИЯ СИТУАЦИИ

Можно предположить, что потребность в изменении существующей сетевой архитектуры возрастет. Однако некоторые решения, направленные на обеспечение более высокого уровня безопасности и расширение пропускной способности, могут быть найдены без фундаментальных изменений в интернет-протоколах.

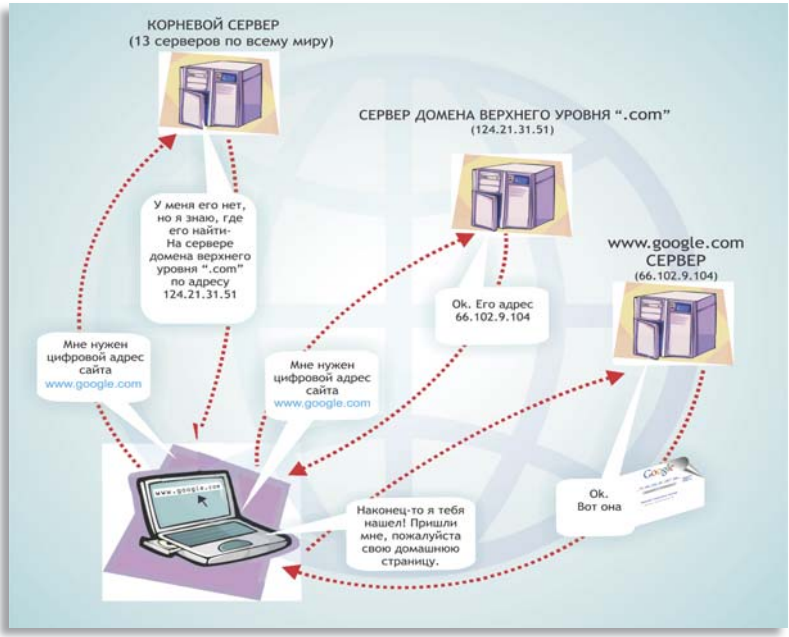
Один из способов — создание различных сетевых вариантов «поверх» существующего протокола TCP/IP. Весьма вероятно, что частные компании будут продолжать разработку таких инициатив, призванных обойти как ограничения интернета в его современном виде, так и нежелание органов стандартизации интернета изменить ключевые принципы его функционирования, в особенности принцип сквозной передачи данных.

СИСТЕМА ДОМЕННЫХ ИМЕН (DNS)

СОВРЕМЕННОЕ СОСТОЯНИЕ

DNS работает с интернет-адресами (такими, как www.google.com) и превращает их в IP-адреса. Таким образом, чтобы получить доступ к определенному сайту, компьютер должен сначала обратиться к DNS-серверу. Этот DNS-сервер затем нахо-

дит цифровой адрес конкретного сайта (в случае с Google это 196.23.121.5). 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 иерархическая организация DNS и в конечном счете возможность правительства США контролировать ее (через министерство торговли).

DNS включает в себя два типа доменов верхнего уровня. Первый тип — это так называемые «родовые» (или «общие»); второй — домены, основанные на кодах стран. Родовые домены верхнего уровня включают в себя:

- .com, .edu, .gov, .mil и .org (с 1984 г.);
- .net и .int (добавлены в 1985 г.);
- .biz, .info, .name, .pro, .museum, .aero и .coop (добавлены в 2000 г.).

Список адресов для каждого родового домена верхнего уровня (рДВУ)[9] поддерживает одна регистратура. Например, домен .com администрируется компанией VeriSign. Функцию «продавцов» берут на себя регистраторы. ИКАНН 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, предоставляемых регистратурой и регистраторами. Таким образом, ИКАНН действует как регулирующий орган по экономическим и правовым вопросам на рынке родовых доменных имен верхнего уровня.

Важной частью управления доменами является защита торговых марок и разрешение споров. На заре интернета регистрация доменных имен основывалась на принципе «первым пришел — первым обслужили», то есть любой мог зарегистрировать какое угодно название. Потенциальная ценность доменных имен породила явление, известное как киберсквоттинг[10], — регистрацию доменных имен с целью их последующей перепродажи (спекуляции). Невозможность существования двух доменов с одинаковым названием привела к спорам о праве на регистрацию. Эта проблема имела особое значение для доменных имен, использующих названия известных марок (например, Microsoft, Nike, Toyota, Rolex).

В результате реформы управления системой DNS, с принятием Единой политики рассмотрения споров о доменных именах (ЕПРС)[11] были внедрены механизмы, существенно сократившие киберсквоттинг. ЕПРС касается только доменов .com и .net и не затрагивает доменов, основанных на кодах стран. Юрисдикция ЕПРС признается автоматически, когда частное лицо, компания или организация заключает соглашение о регистрации доменного имени. ЕПРС дает некоторые преиму-

[9] generic top level domain, gTLD
[10] От англ. «squat» — самовольно селиться на чужой земле; незаконно вселяться в дом. — *Прим. пер.*
[11] Uniform Dispute Resolution Policy, UDRP

щества тем, кто претендует на уже зарегистрированные названия (обычно это обладатели традиционных торговых марок): к примеру, быстрое разрешение конфликтов с помощью арбитража и простое вступление в силу арбитражных решений путем непосредственного внесения изменений в DNS (без продолжительных судебных процедур).

Другой важной составляющей существующей структуры управления DNS является управление национальными доменами верхнего уровня (скДВУ)[12]. На сегодняшний момент национальными доменами управляет множество различных институтов, получивших аккредитацию на начальных этапах развития интернета, когда правительства не интересовались такими вопросами. В их числе научные учреждения, технические ассоциации, неправительственные организации и даже частные лица. Во многих случаях право на управление кодами стран выдавалось по тому же принципу «первым пришел — первым обслужили».

Создание новых родовых доменных имен

В середине 1990-х гг. один из основателей интернета Джон Постел предпринял неудачную попытку добавить несколько новых доменов к существующему списку (.com, .edu, .org и .int). Наибольшее сопротивление этому оказали представители бизнеса, озабоченные тем, что увеличение числа доменов усложнит проблему защиты торговых марок. В результате ограничительный подход возобладал, и в 2000 г. ИКАНН добавила лишь несколько новых доменов (.biz, .info, .name, .pro, .museum, .aero и .coop).

Другой вопрос, связанный с новыми доменами, касается связи доменных имен с содержанием соответствующих сайтов. Например, в соответствии с законом, принятым Конгрессом США, создается домен «kids.us», где могут размещаться только

[12] country code top level domain, ccTLD

материалы, предназначенные для детей. Основная сложность с этой инициативой заключается в неопределенности: неизвестно, кто будет решать, какие материалы подходят для детей? За этим следуют непростые концептуальные и практические вопросы, связанные с проблемой контроля над информационными материалами. Пока домен «kids» используется только как часть национального домена США.

Управление национальными доменами

Управление национальными доменами верхнего уровня включает в себя три важных вопроса. Первый касается часто политически противоречивого решения о том, *какие национальные коды могут регистрироваться* в случаях, когда международный статус страны или образования неясен или оспаривается (например, в случае с государствами, недавно получившими независимость, с движениями сопротивления). Джон Постел выступал за распределение национальных доменных имен в соответствии со стандартом ИСО, где все страны и другие образования обозначаются двухбуквенными комбинациями. Подход Постела оказался удачным и используется до сих пор несмотря на то, что список ИСО касается «определенных экономических областей», а не суверенных государств.

Второй вопрос — *кто должен управлять национальными кодами?* Многие страны пытались получить контроль над своими доменами, считая их национальным достоянием. Например, ЮАР использовала свое суверенное право в качестве аргумента за возвращение контроля над своим национальным доменом. В соответствии с недавно принятым законом использование национального домена в каких-либо целях, помимо тех, что определены правительством ЮАР, считается преступлением. 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. Наоборот, опыт Кам-

боджи, где управление национальным доменом было отдано правительству, часто называется примером неудачной передачи полномочий. Правительство снизило качество услуг и ввело более высокие пошлины, что усложнило регистрацию камбоджийских доменов.

Иногда национальные домены используются ненадлежащим образом — для регистрации родовых доменов верхнего уровня:

КОД СТРАНЫ	СТРАНА	ДОМЕННАЯ ОБЛАСТЬ
Tv	Тувалу	Телестанции
Mu	Маврикий	Музыка
Md	Молдова	Медицина и здоровье
Fm	Федеративные Штаты Микронезии	Радио
Tm	Туркменистан	Торговая марка

Большинство вышеназванных стран пыталось вернуть контроль над своими национальными доменами. Например, Маврикий начал интенсивную кампанию дипломатического лоббирования в этом направлении.

Третий вопрос связан с *нежеланием доменных операторов многих стран становиться частью системы ИКАНН*. До сегодняшнего дня ИКАНН не удалось собрать операторов национальных доменов под своей крышей. Некоторые операторы национальных доменов начали создавать собственные региональные организации — такие, как Совет Европейских национальных регистратур ДВУ (CENTR)[13].

Языковая проблема: многоязычные доменные имена

Одним из основных препятствий дальнейшему развитию интернета является недостаток многоязычных методов управления интернет-инфраструктурой. Доменные имена регистрируются и используются на английском языке. Даже символы

[13] Council of European National TLD Registries

из немецкого и французского алфавитов, не соответствующие стандарту ASCII, не могут использоваться в интернет-адресах (например café превращается в cafe). Еще более сложная ситуация складывается с системами письма, где не используется латиница, например, японской, арабской или китайской.

Среди многочисленных решений в области многоязычных доменов верхнего уровня наиболее актуальными являются системы «интернационализированных имен доменов» (ИИД)[14] и «интернет-адресов на родном языке» (NLIA)[15]. ИИД, техническое решение, предложенное РГПИ, постепенно занимает доминирующее положение. ИИД преобразовывает названия на других языках в англоязычные доменные имена прямо на компьютере пользователя, а затем отправляет DNS-запрос на основе англоязычного доменного имени. Одним из основных препятствий для более широкого использования ИИД является ее полная интеграция в основные интернет-браузеры, такие как Internet Explorer.

Помимо технических трудностей еще одной, возможно, более сложной проблемой будет разработка политики и процедур управления. Все более активно продвигается идея передачи управления частями системы ИИД странам или группам стран, жители которых говорят на одном языке. Так, правительство Китая несколько раз указывало, что системой ИИД на китайском языке должен управлять Китай. Разработка и реализация политики управления системой ИИД будет одним из серьезных вызовов, с которым столкнется ИКАНН, и испытанием для ее подхода, ориентированного на привлечение представителей разных стран.

[14] Internationalised Domain Name, IDN
[15] Native Language Internet Address

«КОРНЕВЫЕ» СЕРВЕРЫ

Поскольку «корневые» серверы находятся на самой вершине иерархической структуры системы доменных имен, они 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, можно рассмотреть беспокоящий многих сценарий, согласно которому интернет перестанет функционировать, если «корневые» серверы будут отключены. Во-первых, существует 13 «корневых» серверов, распределенных по всему миру (10 в США, 3 в других странах; из 10 серверов в США некоторые находятся в ведении правительственных агентств). 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.

Иными словами, копии файлов корневой зоны хранятся в 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 схема Anycast, копирующая содержимое этих серверов в более чем 80 точках 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). Тринадцать «корневых» серверов находятся под управлением разнообразных организаций: научных или общественных институтов (6 серверов), коммерческих компаний (3 сервера) и правительственных компаний (4 сервера).

Организации, управляющие корневыми серверами, получают файл корневой зоны по предложению IANA (ИКАНН) и с одобрения правительства США (министерство торговли). После получения одобрения содержимое файла вводится в основной «корневой» сервер, находящийся под управлением компании VeriSign по контракту с Министерством торговли. Таким образом, правительство США имеет возможность в одностороннем порядке вносить изменения в систему DNS.

ВОПРОСЫ

Необходима ли интернационализация политического контроля над «корневыми» серверами?

Многие страны высказывали озабоченность существующей на данный момент схемой, в которой окончательные решения о содержимом корневых серверов принимает Министерство торговли США, и предложили заключить Соглашение о «корневых» серверах, которое бы передало политический контроль над этими серверами международному сообществу или по крайней мере дало бы государствам право на свои собственные национальные домены. Маловероятно, что институты власти США (в первую очередь Конгресс) согласятся с таким предложением. Возможный компромисс может быть основан на двух элементах:

- передаче контроля над «корневыми» серверами от Министерства торговли США к ИКАНН, как и было изначально задумано;
- существенной реформе ИКАНН, ведущей к созданию своего рода международной организации, которая могла бы стать приемлемой для всех стран институциональной структурой.

Насколько вероятно создание альтернативных «корневых» серверов (например, «интернета Б»)?

Как говорилось выше, создание альтернативных «корневых» серверов не является технически сложной задачей. Основной вопрос заключается в том, сколько «последователей» будет у альтернативных серверов, или, точнее, сколько компьютеров в интернете будет обращаться к ним с запросами. Без пользователей альтернативная DNS становится бесполезной. 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.

ПРОВАЙДЕРЫ ИНТЕРНЕТ-УСЛУГ

Интернет-провайдеры подключают конечных пользователей к интернету и предоставляют услуги по размещению веб-сайтов (хостинг). Поэтому, с точки зрения многих правительств, они являются самым простым и очевидным механизмом установления контроля над интернетом и обеспечения соблюдения правовых норм пользователями. В этой брошюре под провайдерами интернет-услуг (интернет-провайдерами, или просто провайдерами) мы понимаем как компании, которые предоставляют доступ в интернет частным лицам, так и организации, предоставляющие доступ своим сотрудникам (университеты, правительственные органы и т. д.).

Во время интернет-бума 1990-х годов провайдеры были защищены от какой-либо ответственности за содержание размещаемых и просматриваемых пользователями материалов или нарушение авторского права. Было распространено мнение о том, что дополнительное давление на провайдеров воспрепятствует будущему развитию интернета. По мере возрастания коммерческой значимости интернета и актуализации

вопросов безопасности многие государства начинают использовать провайдеров как инструмент обеспечения соблюдения законов.

ВОПРОСЫ

Рынок интернет-услуг и монополия на телекоммуникации

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 устанавливаю тся завышенные цены, качество услуг остается низким и обнаруживается неспособность решить проблему разрыва в цифровых технологиях. В некоторых случаях телекоммуникационные монополии терпят существование других интернет-провайдеров, но вмешиваются непосредственно в их деятельность (например, ограничивая пропускную способность или создавая помехи для оказания услуг).

Ответственность интернет-провайдеров с точки зрения авторских прав

Для большинства правовых систем общим является принцип, по которому провайдер не может нести ответственности, если не знает о том, что предоставляемые им услуги используются для размещения материалов, нарушающих авторское право. Основное отличие заключается в том, какие юридические действия предпринимаются после того, как провайдер проинформирован, что материал, размещенный на его сервере, нарушает авторское право.

Законы США и ЕС предусматривают процедуру «предупреждение — удаление», в соответствии с которой провайдер должен удалить соответствующий материал, чтобы избежать судебного преследования. Законодательство США и ЕС более строго защищает интересы владельца авторских прав, не давая человеку, использующему материал, привести свои доводы. Японское законодательство предполагает более сба-

лансированный подход (процедура «предупреждение — предупреждение — удаление»), который предоставляет право использующему материал лицу обжаловать требование убрать его с сайта.

Роль интернет-провайдеров в политике по отношению к информационным материалам

«Не убивайте гонца!» — таков ответ провайдеров на растущее давление со стороны властей, стремящихся обеспечить соблюдение норм о содержании ресурсов интернета. Постепенно интернет-провайдеры, хоть и неохотно, вовлекаются в политику по регулированию информационных материалов. У них есть два возможных пути. 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 правительственные функции.

Во многих странах приняты законодательные нормы, которые налагают на провайдеров специальные обязанности по регулированию материалов интернета, — как тех, что размещаются на их серверах, так и тех, к которым получают доступ их клиенты. Этот может возлагать на провайдера дополнительные расходы и в итоге увеличивать стоимость доступа в интернет для пользователей.

ОПТОВЫЕ ПРОВАЙДЕРЫ УСЛУГ ШИРОКОПОЛОСНОЙ СВЯЗИ

Архитектура доступа в интернет состоит из трех ярусов. Провайдеры интернет-услуг, подключающие конечных пользователей, составляют ярус 3. Ярусы 1 и 2 состоят из оптовых

провайдеров услуг широкополосной связи. Ярус 1 (интернет-магистрали) обычно контролируется крупными компаниями — такими, как MCI, AT&T, Cable Wireless и France Telecom. В том, что касается широкополосных каналов связи, традиционные телекоммуникационные компании распространили свое присутствие на глобальных рынках и на интернет-магистрали. Провайдеры, представляющие ярус 2, обычно действуют на национальном или региональном уровнях.

ВОПРОСЫ

Нужно ли считать интернет-инфраструктуру услугой общего пользования?

Данные интернета могут передаваться по любому каналу коммуникации. Однако на практике определенные мощности, такие как магистрали яруса 1, стали особенно важны для функционирования интернета. Их центральное положение в структуре интернета дает их владельцам возможность устанавливать цены и диктовать условия на предоставление своих услуг. Два связанных с этим случая упомянуты в недавнем докладе Организации по безопасности и сотрудничеству в Европе (ОБСЕ).

Первый случай касается судебного разбирательства в отношении веб-сайта, размещенного на сервере провайдера Flashback в Швеции и содержащего сомнительные материалы, которые можно счесть пропагандирующими нацизм. Суд вынес решение, что материалы сайта не нарушают шведское законодательство о запрете нацизма. Тем не менее один убежденный антинацистский активист начал масштабную кампанию против Flashback, оказывая давление на интернет-провайдера Flashback — Air2Net и оператора главной магистрали MCI/Worldcom. В результате компания MCI/Worldcom приняла решение отключить Flashback, несмотря на отсутствие какой-либо правовой основы для этого. Попытки Flashback найти другого провайдера оказались безрезультатными, поскольку большинство из потенциальных провайдеров также были подключены через магистраль MCI/Worldcom.

Второй случай произошел в Нидерландах, где небольшой голландский интернет-провайдер Xtended Internet был отключен от своего основного провайдера, находящегося в США, в результате лоббистских усилий саентологов. Таким образом, работоспособность интернета может оказаться в зависимости от решений, принимаемых операторами центральных магистралей. Имеет ли глобальное интернет-сообщество право требовать от основных телекоммуникационных операторов гарантий надежного функционирования наиболее важной интернет инфраструктуры? Управляют ли эти компании объектами общего пользования?

Либерализация телекоммуникаций и роль интернет-провайдеров

Существуют противоположные точки зрения на то, в какой степени провайдеры интернет-услуг 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

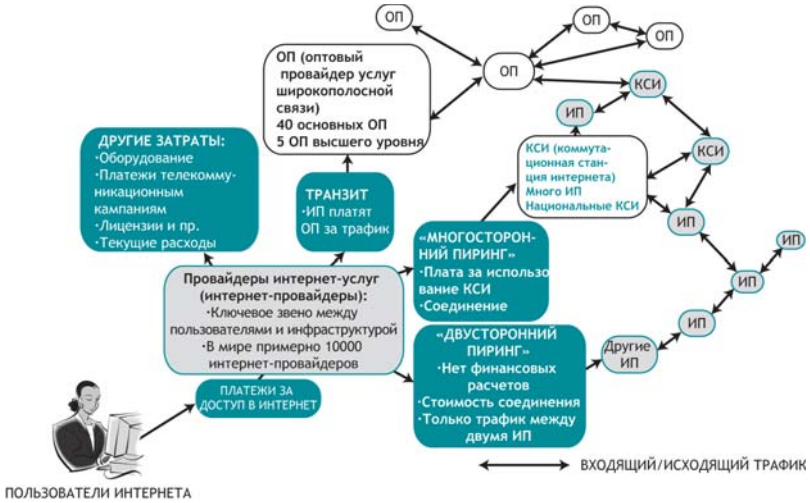
СОВРЕМЕННОЕ СОСТОЯНИЕ

Очень часто обсуждение вопросов управления интернетом завершается анализом распределения средств и источников дохода. Каковы потоки денежных средств в интернете? Кто платит за интернет?

Между различными сторонами, вовлеченными в процесс функционирования интернета, происходит множество финансовых операций:

- индивидуальные пользователи и компании платят интернет-провайдерам;
- интернет-провайдеры платят за услуги операторов связи и за канал доступа в интернет;
- 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);
- стороны, регистрирующие доменные имена, платят за услуги не только регистратору, но и IANA;
- интернет-провайдеры платят региональным интернет-регистратурам за IP-адреса;
- региональные интернет-регистратуры платят ИКАНН;
- операторы связи платят производителям кабелей и спутников, а также компаниям, предоставляющим телекоммуникационные услуги. Поскольку эти операторы часто берут средства в кредит, они выплачивают проценты банкам и консорциумам.

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



ВОПРОСЫ

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

На сегодняшний день затраты покрываются в основном развивающимися странами. 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. Парадоксально, но факт, что таким образом небольшие и бедные страны субсидируют интернет в развитых странах.

Проблема денежных расчетов особенно важна для наиболее бедных стран, в которых прибыль от международных коммуникаций является важным источником пополнения бюджета. Ситуацию еще более усложнило появление и распространение интернет-телефонии (VoIP), в результате чего большая часть телефонных переговоров стала вестись не через национальных операторов связи, а через интернет.

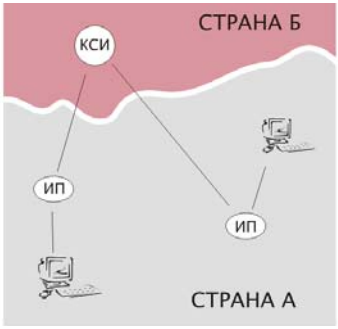
По инициативе МСЭ были начаты переговоры о возможном усовершенствовании существующей системы покрытия затрат на интернет, цель которых — более сбалансированное распределение стоимости доступа в интернет. В результате противодействия со стороны развитых стран принятая МСЭ Резолюция № D.50 практически не имела последствий.

Сокращение стоимости доступа за счет использования коммутационных станций интернета

Коммутационные станции интернета (КСИ) — это технические устройства, с помощью которых провайдеры обмениваются интернет-трафиком. КСИ обычно создаются для обмена трафиком внутри ограниченной группы пользователей (напр., внутри города, региона, страны), чтобы избежать ненужной

маршрутизации (направления потоков данных) через географически удаленные точки.

Интернет-трафик без национальной КСИ



Интернет-трафик при наличии национальной КСИ

ИП — интернет-провайдер

КСИ также могут сыграть важную роль в сокращении разрыва в цифровых технологиях. Например, если в стране нет национальной КСИ, необходимо направлять существенную долю интернет-трафика между пользователями в этой стране через другую страну. Это увеличивает объем международной передачи данных на дальние расстояния и стоимость предоставления услуг интернета.

СТАНДАРТЫ ВСЕМИРНОЙ ПАУТИНЫ (WWW)

К концу 1980-х гг. «битва» по поводу сетевых стандартов завершилась. TCP/IP постепенно стал основным сетевым протоколом, оттеснив другие: поддерживавшийся МСЭ протокол X-25 (часть архитектуры Взаимодействия открытых систем)[16] и многие проприетарные [17] стандарты — такие, как SNA, разработанный IBM. Хотя интернет и облегчил коммуникацию между разнообразны-

[16] Open Systems Interconnection

[17] Проприетарный (от англ. proprietary) — эксклюзивно принадлежащий кому-либо и закрытый для использования без специального разрешения владельца, запатентованный. В основном употребляется по отношению к программному обеспечению (ПО), стандартам. Так, проприетарное ПО запрещено копировать, распространять, изменять без согласования с владельцем патента. — *Прим. пер.*

ми 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 ЦЕРН[18] в Женеве и представляло собой новый стандарт обмена информацией по интернету, названный HTML [19] (по сути, упрощение существовавшего стандарта ИСО, называвшегося SGML). Для представления информационных материалов в интернете их сначала стало нужно отформатировать в соответствии со стандартом HTML. 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. В то время как изначально HTML позволял работать только с текстом и изображениями, 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, что большинство браузеров будут адекватно отображать любой размещенный в интернете материал.

Стандартизация приложений вступила в новую фазу с появлением языка XML[20], 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). Стандартиза-

[18] Европейский совет по ядерным исследованиям (фр. Conseil Européen pour la Recherche Nucléaire — CERN). — *Прим. пер.*
[19] HyperText Mark-up Language — язык гипертекстовой разметки
[20] eXtensible Mark-up Language — расширяемый язык разметки

ция приложений осуществляется преимущественно в рамках консорциума 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.

ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ НА ОСНОВЕ ОТКРЫТОГО ИСХОДНОГО КОДА

Данное ПО распространяется бесплатно и может быть изменено пользователями. Приложения на основе открытого исходного кода разрабатываются программистами по всему миру, работающими с одним и тем же исходным кодом. Когда идея открытого кода только появилась, ей прочили роль эффективной альтернативы дорогому проприетарному ПО. Наиболее известной инициативой в области открытого исходного кода является операционная система Linux. Распространение ПО на основе открытого кода оказалось более медленным, чем ожидалось, — в первую очередь из-за отсутствия у пользователей гарантий получения технической поддержки. Недавнее решение ряда таких ключевых игроков рынка, как IBM и Intel, об использовании Linux — основной платформы на основе открытого исходного кода — может способствовать развитию идеологии Open Source.

Более того, интерес к открытому исходному коду возрождается под новым названием и со слегка измененной концепцией — Free/Libre Open Source Software (FLOSS). Основное различие между концепциями открытого исходного кода и FLOSS заключается в том, что последняя предполагает возможность свободного доступа к коду без какой-либо регистрации.

О концепции открытого кода часто говорят как о решении проблемы наращивания возможностей развивающихся стран в сфере информационных и коммуникационных технологий. Во время саммита ВСИО попытка представителей глобального гражданс-

кого общества и ряда развивающихся стран документально закрепить открытый код и FLOSS в качестве способа преодоления разрыва в цифровых технологиях была выхолощена включением в текст общих фраз о различных моделях ПО, в том числе проприетарного, на основе открытого кода и бесплатного.

КОНВЕРГЕНЦИЯ: ИНТЕРНЕТ — ТЕЛЕКОММУНИКАЦИИ — МЕДИА

Широкое и все возрастающее использование интернет-протоколов привело к конвергенции телекоммуникаций, мультимедиа и развлекательных систем. Сегодня при помощи интернета можно делать телефонные звонки, слушать радио, смотреть телепрограммы и обмениваться музыкой. В сфере традиционных коммуникаций основным направлением конвергенции является интернет-телефония (VoIP). Растущая популярность интернет-телефонии основывается на низкой стоимости, возможности объединить линии голосового общения и передачи данных, а также использовать разнообразные компьютерные инструменты. TCP/IP также приобретает доминирующее положение в сфере мультимедиа и развлечений. В то время как с технической точки зрения процесс конвергенции 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. Еще неясно, кто станет лидером на этом все более интегрированном рынке: телекоммуникационные компании (такие, как MCI), или компании сферы ИКТ (такие, как IBM).

То же относится и к рынку мультимедиа, хотя в этой области некоторые компании уже отреагировали на новую ситуацию, либо развивая одновременно направления ИКТ и медиаразвлечений, либо вступая в партнерства. Так, компания Sony начала развивать оба направления. Целью слияния компаний America Online и Time Warner было объединение телекоммуникаций и возможностей в сфере медиаразвлечений. Таким образом, AOL/Time Warner объединила предоставление услуг интернета, телевидение, музыку и разработку ПО под одним корпоративным «зонтиком».

Необходимость правовых рамок

Правовая система наиболее медленно адаптируется к переменам, связанным с технологическим и экономическим сближением. Каждый из сегментов: телекоммуникации, медиаразвлечения и ИКТ — имеет собственные нормативные рамки.

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 теле- и радиовещание? Будут ли разрабатываться новые режимы, связанные преимущественно с интернетом? Должно ли регулирование процесса сближения 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.

Риск слияния 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 этим процессом сближения?

Некоторые участники дискуссий утверждают, что положение операторов кабельных сетей как «буфера» между пользователями и интернетом может представлять угрозу для принципа сквозной передачи данных.

Основное отличие между традиционным доступом в интернет по телефонной линии и кабельными сетями заключается в том, что вторые не подпадают 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.

БЕЗОПАСНОСТЬ ИНТЕРНЕТА

СОВРЕМЕННОЕ СОСТОЯНИЕ

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

Побочные последствия стремительного внедрения интернета почти во все сферы человеческой жизни усиливают уязвимость современного общества. Критически важные элементы инфраструктуры, включая электрические сети, транспортные системы и системы здравоохранения, являются частями глобальной сети, потенциально уязвимыми перед кибернападениями. 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 информационной безопасности более подробно обсуждаются в трех других брошюрах этой серии:

- «Правила гигиены» для данных и персональных компьютеров
- Информационная безопасность и организации
- «Хактивизм», кибертерроризм и кибервойна

Вопросы информационной безопасности можно классифицировать по трем критериям: тип действий, тип злоумышленника и тип цели. Классификация, основанная на типе действий, включает в себя: перехват данных, нарушение целостности данных, нелегальный доступ, внедрение шпионского ПО 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 безопасности интернета

Вопросам безопасности интернета посвящено множество национальных, региональных и глобальных инициатив.

На национальном уровне происходит усовершенствование законодательства и судебной практики в области безопасности интернета. 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 страну, в особенности развитую, где не выдвигалось бы каких-либо инициатив, связанных с безопасностью интернета.

На международном уровне наиболее активными организациями являются ОЭСР, опубликовавшая Директивы по информационной безопасности, и МСЭ, разработавший большое количество рамочных документов, архитектур и стандартов безопасности, включая X.509, который является основой инфраструктуры «открытого ключа» (PKI)[21], используемой, например, в защищенной версии протокола HTTP (HTTPS).

«Большая восьмерка» также выступила с несколькими инициативами в области безопасности интернета — такими, как

[21] Public key infrastructure

совершенствование механизмов сотрудничества между правоохранительными органами. «Большая восьмерка» создала также 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 с целью противостояния киберпреступности и развития 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 г.), 54/49 (1999 г.), 55/28 2000 г., 56/19 (2001 г.), 57/239 (2002 г.) и 58/199 (2003 г.) С 1998 г. все последующие резолюции имеют сходное содержание без каких-либо существенных улучшений. Они не отражают значительных перемен, произошедших в области безопасности интернета с 1998 г.

Важным международным правовым инструментом, связанным с безопасностью интернета, является Конвенция Совета Европы по киберпреступности, вступившая в силу 1 июля 2004 г.

Некоторые страны заключили также двусторонние соглашения. США имеет двусторонние соглашения о правовом сотрудничестве по вопросам уголовных преступлений с более чем 20 странами. Эти соглашения используются также в отношении киберпреступлений.

Одной из попыток исследователей и неправительственных организаций выработать международное соглашение является Стэндфордская предварительная конвенция о защите от киберпреступлений и кибертерроризма. Этот черновой документ рекомендует создать международный орган — Агентство по защите информационной инфраструктуры[22].

[22] Agency for Information Infrastructure Protection

ВОПРОСЫ

Архитектура интернета и безопасность

На безопасность интернета влияет сама природа его организации. Должны ли мы продолжать придерживаться существующего подхода, пытаясь «надстроить» безопасность на изначально существующий небезопасный фундамент, или стоит изменить что-то 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 преследовали цель улучшения производительности или внедрения новых приложений. Безопасность не была приоритетом.

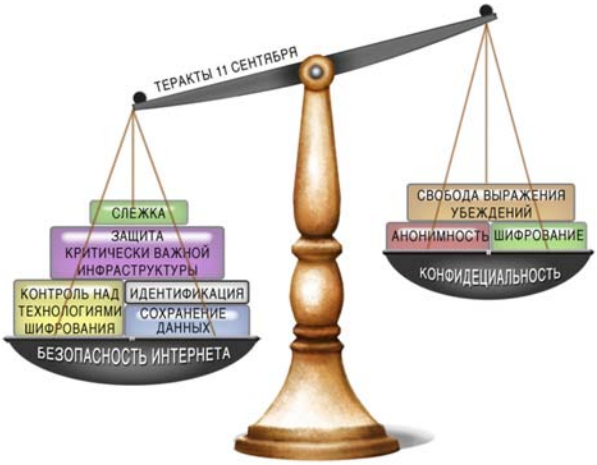
Неясно, сможет ли РГПИ изменить стандарты электронной почты, чтобы гарантировать удостоверение подлинности (аутентификацию) и в итоге сократить ненадлежащее использование интернета (например спам, киберпреступность). Учитывая противоречия, связанные с любым изменением основных стандартов интернета, вероятнее всего, связанные с безопасностью усовершенствования базового интернет-протокола будут постепенными и медленными. Представители бизнеса и другие стороны, заинтересованные в более быстрых решениях, могут начать разработку новых уровней, «умного интернета», которые будут способствовать, среди прочего, и более защищенной интернет-коммуникации.

Электронная коммерция и безопасность интернета

Безопасность часто упоминают в числе предварительных условий для ускоренного 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 онлайн-услугам и использованию электронных денег.

Приватность и безопасность интернета

Еще одним спорным моментом является баланс между безопасностью и правами человека. Требует ли обеспечение безопасности интернета частичного отказа от права на тайну частной жизни (приватность)? Как должно регулироваться использование шифровального ПО, которое может применяться и для законной защиты тайны переписки, и для защиты незаконной коммуникации террористов и преступников? Этот баланс между безопасностью интернета и правами человека постоянно изменяется.



После 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. Гражданское общество отреагировало на это привлечением внимания к защите тайны частной жизни и принципу свободы выражения убеждений.

Вопрос о балансе между информационной безопасностью и приватностью ярко обозначился в спорах о возможности распространения Конвенции Совета Европы по киберпреступности на глобальный уровень. Основным возражением

активистов, отстаивающих права человека, было то, что Конвенция стремится решить проблемы безопасности интернета 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, связанная с инструментами, использующимися для защиты передаваемых данных.

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

Международные аспекты политики в отношении криптозащиты касаются управления интернетом постольку, 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 шифровального ПО была не слишком успешной, поскольку США не могли контролировать распространение такого ПО на международном уровне. Американские компании, производящие ПО, начали мощную кампанию лоббирования, 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. Вассенаарское соглашение — это международный режим, установленный 33 развитыми странами[23] 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 технологии «клиппер чип» на международный уровень, чтобы 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 в самих США это предложение также было отозвано. Этот пример демонстрирует связь между событиями на национальной и международной аренах, и в данном случае последние имели решающее влияние на первые.

ОЭСР — еще один форум международного сотрудничества в области шифрования данных. Хотя документы ОЭСР не имеют обязательной юридической силы, ее указания по различным вопросам являются весьма влиятельными. Они появляются в результате работы экспертов и принятия решений на основе консенсуса. Большинство таких указаний в итоге включаются в национальные законы. Деятельность ОЭСР в области криптог-

[23] На сегодняшний день число стран, присоединившихся к Вассенаарскому соглашению, составляет 39. — *Прим. пер.*

рафической 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.

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 13 электронных сообщений 10 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. Недавнее исследование, проведенное по заказу ЕС, показало, 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 должно сопровождаться 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. Хотя закон предусматривает суровое наказание за распространение спама, вплоть до тюремного заключения на срок до пяти лет, некоторые его положения, как утверждают критики этого 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.

В июле 2003 г. в Европейском Союзе был принят собственный закон по борьбе со спамом, ставший частью Директивы по при-

ватности и электронным коммуникациям. Несмотря на требование ЕС к странам-участницам ввести в действие этот закон до конца 2003 г., 9 государств ЕС не соблюли этот срок. Законодательство ЕС делает акцент на саморегулировании и инициативах частного сектора, способствующих сокращению спама.

МЕЖДУНАРОДНЫЕ ИНИЦИАТИВЫ

Законы по противодействию 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 по противодействию 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.

Спам и развитие

Если пользователи в развитых странах, пусть и с трудом, но могут справиться с создаваемыми спамом трудностями, то во многих развивающихся странах спам наносит значительный урон всей интернет-инфраструктуре. В условиях низкой скорости передачи данных и недоразвитости интернет-инфраструктуры спам ставит под угрозу саму возможность доступа в интернет для многих пользователей из развивающихся стран. Этим странам не хватает технических ресурсов и знаний для борьбы со спамом. Как следствие, спам увеличивает разрыв в цифровых технологиях между развитыми и развивающимися странами.

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 (7—9 июля 2004 г.) и рассмотрев 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[24], 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, Microsoft и Yahoo!. Они создали Технический альянс по противодействию спаму (ASTA)[25], основной задачей которого является координация технических и политических инициатив в сфере борьбы со спамом.

ВОПРОСЫ

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», игнорируя 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.

[24] Network of Anti-Spam Enforcement Agencies
[25] Anti-Spam Technical Alliance

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 существующих стандартов электронной почты. РГПИ работает над внедрением изменений в протокол электронной почты, которые гарантировали бы установление подлинности электронных сообщений. Это один из примеров того, как технические вопросы (стандарты) могут влиять на политику. Возможная уступка, на которую необходимо будет пойти для обеспечения удостоверения 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 могут 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. Некоторые из участников недавнего совещания МСЭ предложили принять многосторонний меморандум о взаимопонимании или разработать некий инструмент в контексте ВСИО. 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 заинтересованы в выработке глобального ответа на проблему спама.

ЧАСТЬ 3

Правовые аспекты

КОРЗИНА «ПРАВОВЫЕ АСПЕКТЫ»

Почти каждый аспект управления интернетом содержит правовые компоненты, однако правовая база, которая соответствовала бы быстрому развитию интернета, еще только начинает формироваться. Существуют два общепринятых подхода к правовым аспектам управления интернетом:

1. «Реальное» право — подход, в рамках которого интернет рассматривается как явление, аналогичное предшествующим ему телекоммуникационным технологиям (начиная от сигнальных костров и заканчивая телефоном). Хотя интернет быстрее и масштабнее, он по-прежнему является способом дистанционного общения между отдельными людьми. Следовательно, существующие правовые нормы могут применяться и по отношению к интернету.
2. «Киберправо» — исходит из того факта, что интернет породил новые виды социальных взаимоотношений, осуществляющихся в киберпространстве. Следовательно, возникает необходимость формулировать новые «киберзаконы» для киберпространства. Доводом в поддержку этого подхода является тот факт, что невероятная скорость и объем межнационального общения, которое ведется при помощи 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 некоторых случаях — таких, например, как защита торговых марок, — существующие в реальном мире правовые нормы придется видоизменить для того, чтобы иметь возможность применить их к киберпространству. Другие же случаи, например спам, должны регулироваться аб-

солютно новыми законами. Ближайшая к спаму аналогия из реального мира — так называемая макулатурная почта (массовые рекламные рассылки), не является противозаконной.

Обсуждение правовых аспектов в данной брошюре состоит из двух частей: правовые механизмы и юридические вопросы.

ПРАВОВЫЕ МЕХАНИЗМЫ

В области управления интернетом либо уже применяются, либо могут применяться следующие правовые механизмы:

- законодательные нормы;
- социальные нормы (обычаи);
- саморегулирование;
- регулирование с помощью программного кода (см. с.27);
- судебная практика (решения суда);
- международное право.

Законодательные нормы

Любая правовая норма включает в себя диспозицию (правило) и санкцию. Диспозиция определяет должное поведение (например: не совершать преступлений, платить налоги), а санкция устанавливает наказание, грозящее в случае, если правила не соблюдаются (штрафы, тюремное заключение, 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.

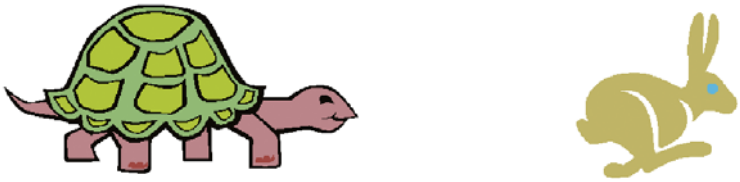
Независимо от того, признаем ли мы более адекватным «реальный» или «кибер-подход», несомненно одно: **законодательные нормы не делают противозаконное поведение невозможным, а только устанавливают наказание за него.** Тот факт, что мошенничество запрещено и в реальном, и в виртуальном мире, не означает, 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 уже весьма распространены в интернете, следовательно, законы реального мира используются неэффективно.

Социальные нормы (обычаи)

Как и нормы закона, социальные нормы предписывают 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 регулировался практически исключительно совокупностью социальных норм, получивших название «нетике́т» (netiquette). Основной мерой наказания за их нарушение было давление со стороны других членов интернет-сообщества и исключение из него. 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 регулирова-

ния все еще может использоваться, однако лишь внутри закрытых групп, обладающих хорошо развитыми внутренними связями.

Управление информационным обществом



Закон всегда отстает от технологий

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 обычно являются неорганизованной регулятивной системой, саморегулирование основывается на хорошо продуманном и организованном подходе. Нормы саморегулирования обычно закрепляются в кодексах надлежащего поведения.

Тенденция к саморегулированию особенно хорошо заметна среди провайдеров интернет-услуг. 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 в решении вопросов, вызывающих большой ин-

терес общественности (например политики контроля над содержанием материалов интернета), опора на саморегулирование 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 защите 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 инструментами — правовыми нормами.

Первым правовым инструментом, к которому прибегают судьи, является правовая 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 с. 28—33.

Международное регулирование

Согласно распространенной точке зрения, глобальный характер интернета требует глобального регулирования. Необходимость глобального подхода часто подтверждается недостаточной эффективностью национальных мер, направленных на борьбу со спамом, киберпреступностью и другими нежелательными явлениями. В качестве примера успешного универсального режима для борьбы с преступностью часто упоминается режим регулирования гражданской авиации. С момента подписания договоров о гражданской авиации ко-

личество диверсий и других незаконных действий неуклонно сокращается. Одна из причин — тот факт, что существование единого правового пространства в области гражданской авиации не позволяет преступникам находить «тихие гавани». В то же время важность глобального подхода не означает, что некоторые вопросы не могут и не должны решаться на национальном и региональном уровнях.

Для глобального регулирования требуется всеобщий консенсус, которого можно достичь (если его вообще можно достичь) только посредством долгих переговоров. Для создания режима управления интернетом можно задействовать различные международные правовые механизмы. В соответствии со Статутом Международного суда, международные правовые ресурсы подразделяются на конвенции, обычаи и общие принципы. Помимо этого существует еще так называемое «мягкое право» — международно-правовой ресурс, важность которого все больше возрастает.

Международное договорное право. В настоящее время единственным соглашением, непосредственно посвященным вопросам, связанным с интернетом, является Конвенция Совета Европы по киберпреступности. Другие конвенции и договоры лишь частично применимы к интернету. Примером может служить свод норм, касающихся прав человека. Свобода выражения убеждений защищается статьей 19 Пакта о гражданских и политических правах. Другие связанные с интернетом права (на частную жизнь и на получение информации) регулируются глобальными и региональными соглашениями в области прав человека. В сфере разрешения конфликтов одним из главных инструментов является Нью-Йоркская Конвенция о признании и приведении в исполнение иностранных арбитражных решений.

Превалирующий подход к управлению интернетом (если противопоставлять национальный и международный подходы, «мягкое» и «жесткое» право) в итоге повлияет на вид и форму всеобщей конвенции по управлению интернетом, если таковая будет создана. Некоторые специалисты полагают, что интер-

нету требуется всеобъемлющий правовой инструмент — такой, как Конвенция ООН по морскому праву. Эта аналогия не является уместной, поскольку переговоры по морскому праву потребовали систематизации существующего обычного права и интеграции четырех существующих конвенций. В случае же с интернетом обычного права не существует. Его постоянно создают, в основном методом проб и ошибок. Вместо одного полномасштабного договора, вероятно, будут использоваться несколько отдельных инструментов.

Обычное право. Развитие обычного права обычно требует большего времени, которое уходит на кристаллизацию определенных обязательных к исполнению норм. В прошлом это было возможно. Однако с развитием технологий после Второй мировой войны потребовалось резко сократить период выработки международных нормативных рамок, чтобы адекватно реагировать на глубокие экономические и политические изменения, порождаемые технологическим прогрессом в течение очень короткого промежутка времени. Интернет является тому убедительным подтверждением. Маловероятно, что обычное право будет играть доминирующую роль в создающемся режиме управления интернетом.

«Мягкое право». Термин «мягкое право» применяется по отношению к различным политическим документам — таким, как декларации, руководящие принципы и проекты законов. Лингвистическим критерием для определения «мягкого» закона является частое использование слова «следует» вместо «обязан», которое обычно ассоциируется с юридически более обязывающим подходом «жесткого» права (договорного права).

Существует много примеров соблюдения странами договоренностей, заключенных на основе «мягкого права». Некоторые из них имеют большую важность, например Хельсинкский Акт 1975 г., задавший рамки взаимоотношений между Востоком и Западом. «Мягкое право» используется государствами по многим причинам, например с целью упрочения доверия, поощрения происходящих перемен, введения новых право-

вых и правительственных механизмов. «Мягкое право» может стать потенциально применимым правовым методом в управлении интернетом.

ЮРИСДИКЦИЯ

Юрисдикция является тем аспектом управления интернетом, который требует наибольшего внимания. Количество связанных с интернетом конфликтов все время увеличивается. Неясность в отношении юрисдикции может иметь следующие непосредственные 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.
- Замедление развития электронной коммерции.
- Дробление интернета на безопасные в правовом отношении зоны.

Какова взаимосвязь между юрисдикцией и интернетом?

Юрисдикция основывается главным образом на географическом разделении мира на государства. Каждое государство имеет суверенное право осуществлять юрисдикцию на своей территории. Однако интернет делает возможным существенное трансграничное взаимодействие, которое сложно (хотя и возможно) отслеживать при помощи традиционных правительственных механизмов. Вопрос юрисдикции в интернете снова возвращает нас к одной из ключевых дилемм, связан-

ных с управлением интернетом: каким образом можно «укоренить» интернет в рамках существующей правовой и политической географии?

Юрисдикция — основные аспекты

Существуют три основных составляющих юрисдикции:

- Какой суд или другой государственный орган имеет необходимые полномочия (процессуальная юрисдикция)?
- Какие законы должны применяться (материальная юрисдикция)?
- Каким образом должны исполняться 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 следствия — право государства регулировать экономические и правовые последствия, проявляющиеся на территории этого государства в результате действий, совершенных где-либо еще.

Другим важным принципом, установленным современным международным правом, является принцип универсальной юрисдикции в отношении действий, нарушающих основополагающие принципы международного права (*jus cogens*), например, геноцида или пиратства.

СОВРЕМЕННОЕ СОСТОЯНИЕ

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» (*spillover effect*).

Двумя наиболее наглядными и часто упоминаемыми судебными делами, иллюстрирующими проблему юрисдикции, является дело компании CompuServe, рассматривавшееся в Германии в 1996 г., и дело Yahoo!, рассматривавшееся в 2001 г. во Франции.

В первом деле немецкий суд потребовал, чтобы американская компания CompuServe закрыла доступ к порнографическим материалам. Чтобы соблюсти немецкое законодательство, компании пришлось удалить такие материалы со своего центрального сервера в США. В результате их не смогли найти граждане даже тех стран (включая США), где доступ к порнографическим материалам не запрещен законом. Компании CompuServe пришлось подчиниться наиболее жестким нормам в этой области. Это дело вызвало опасения, что весь интернет должен будет подчиниться самым ограничительным нормам (принцип наименьшего общего знаменателя).

Несколько более поздних случаев, включая дело Yahoo!, снова подчеркнули значимость проблемы множественной юрисдикции. Источником дела Yahoo! было нарушение французского законодательства, запрещающего распространение материалов нацистского содержания. Французские законы запрещают гражданам получать доступ к сайту Yahoo!, на котором размещены нацистские реликвии, хотя сам сайт находится в США, где размещение подобных материалов было и до сих пор является законным.

В соответствии с положениями «реального» права, в делах, подобных делу CompuServe, нет ничего нового, поскольку в реальном мире «эффект переливания» — вполне обычное явление. Из хрестоматийных примеров — уствновление Комиссией ЕС

строгих условий для слияния компаний «Боинг» и «МакДоннелл Дуглас» — сделки, одобренной властями США. Хотя ни одна из компаний не имела производственных мощностей в Европе, им все равно пришлось учесть европейские законы о конкуренции для того, чтобы иметь возможность продавать самолеты в ЕС.

В то время как рассуждения, основывающиеся на «реальном» праве, в принципе верны, они тем не менее обладают серьезными практическими недостатками, которые ограничивают возможность применения существующих законов к интернету. Основной проблемой является масштаб связанных с интернетом судебных дел, поскольку почти каждый сайт или услуга могут попасть под юрисдикцию какой-либо страны мира. Таким образом, количественный аспект (число дел) может потребовать поиска новых решений.

ВОЗМОЖНЫЕ РЕШЕНИЯ

Возможные решения проблемы множественной юрисдикции в интернете могут быть найдены при помощи:

- модернизации международного частного права;
- гармонизации национальных законов, которая сделала бы вопрос о юрисдикции менее существенным;
- использования арбитража;
- использования технических возможностей для определения происхождения пользователей (главным образом геолокационного ПО – см. с.159).

Модернизация международного частного права

В рамках традиционного судопроизводства национальные суды решают, могут ли они рассматривать то или иное дело и какие законы при этом будут применяться. Решения по вопросам и процессуальной, и материальной юрисдикции базируются на международном частном праве («коллизия законов» в англосаксонских правовых системах). Предписания международного частного права устанавливают критерии для опре-

деления юрисдикции — такие, как связь между индивидом и национальной юрисдикцией (например национальность, место проживания) или связь между определенной сделкой и национальной юрисдикцией (например место, где был заключен договор, где состоялась сделка). Интернет затрудняет применение этих критериев по сравнению с традиционными случаями, но не делает их применение невозможным.

Традиционный подход, в силу своей сложности, медлительности и высокой стоимости, редко используется для решения конфликтов, связанных с интернетом. Он также не соответствует *modus operandi* (образу действий) интернета — быстроте, простоте и прагматичности. Основные механизмы международного частного права были созданы в то время, когда межнациональное взаимодействие было менее частым и менее интенсивным, а потому и дел с участием физических и юридических лиц, подпадающих под разную юрисдикцию, было относительно немного. С появлением интернета межнациональное взаимодействие стало обычным явлением. Общение, обмен и конфликты между юридическими и физическими лицами из разных стран происходят гораздо чаще и гораздо интенсивнее, чем раньше.

Потенциальным решением может быть модернизация международного частного права с целью создания быстрой и недорогой процедуры определения национальной юрисдикции в делах, связанных с интернетом. Среди возможных улучшений — использование упрощенных процедур для определения соответствующей юрисдикции, возможность рассмотрения дел в режиме онлайн и повышение гибкости в отношении юридических консультаций.

На региональном уровне ЕС принял Брюссельскую конвенцию, которая упрощает процесс достижения решений о юрисдикции и защищает интересы потребителей в электронной коммерции.

На глобальном уровне основным форумом для обсуждения проблем развития международного частного права является

Гаагская конференция. На сегодняшний день ведущую роль в переговорах играют США. В 1992 году США инициировали переговоры о юрисдикции с целью усиления защиты интеллектуальной собственности посредством повсеместного исполнения решений американских судов. С 1992 года рост интернета и электронной торговли изменил ход переговоров. Интернет-компаниям США стало опаснее действовать в условиях множественной юрисдикции. Судебные иски против компании CompuServe и Yahoo!, инициированные Германией и Францией, показали, как материалы, размещенные в США, могут стать причиной судебных разбирательств в других странах.

«Удобные флаги» в интернете

Другим возможным последствием недостатка гармонизации может стать миграция «данных» и информационных материалов в страны с меньшей степенью контроля над содержанием материалов интернета. По аналогии с морским правом, некоторые страны могут стать «удобными флагами» или офшорами в интернете.

Если бы Гаагская конвенция была принята с изначально предложенным текстом, для правовой системы США это стало бы серьезной проблемой. Суды США были бы вынуждены следить за исполнением решений иностранных судов по материалам, размещенным на американских сайтах, что в итоге поставило бы под угрозу свободу слова, провозглашенную в Первой поправке к Конституции США. Последствия такой ситуации были вполне неожиданными — изменение позиции США и ограничение их амбиций в сфере реформирования системы международного частного права. Отсутствие прогресса в модернизации международного частного права на глобальном уровне может усилить положение других возможных способов разрешения конфликтов, связанных с юрисдикцией.

Гармонизация национальных законов

Гармонизация национальных законов должна привести к появлению единого набора норм на мировом уровне. Если правовые нормы одинаковы во всех странах, 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 всеобщей неприемлемости детской порнографии, пиратства, рабства, терроризма и киберпреступности. Постепенно сближаются позиции различных стран и по другим вопросам — таким, как спам и безопасность в интернете. Однако в некоторых областях, включая политику контроля над содержанием материалов интернета, достижение глобального консенсуса маловероятно.

Другим вариантом решения проблемы юрисдикции является арбитраж, обсуждаемый в следующем разделе.

АРБИТРАЖ

Арбитраж (третейский суд) является альтернативным механизмом разрешения конфликтов, который может использоваться вместо судебных процедур, обычно медленных и сложных. 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. Существует много вариантов соглашений об арбитраже, в которых регулируются такие вопросы, как место и процедура проведения арбитража, выбор применимого права и т. д.

Онлайн-арбитраж используется для разрешения не только связанных с интернетом споров, но и обычных коммерческих разногласий. Онлайн-арбитраж ведется полностью в интернете, включая предоставление свидетельских показаний и вынесение решения.

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, подписанной большинством стран. В соответствии с этой конвенцией национальные суды обязаны выполнять арбитражные решения. Обеспечить выполнение арбитражных решений проще, чем решения иностранных судов.

Арбитраж широко используется 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 (ЕПРС). ЕПРС была разработана Всемирной организацией интеллектуальной собственности (ВОИС) и принята ИКАНН в качестве основной процедуры разрешения споров. ЕПРС изначально оговаривается как механизм разрешения конфликтов во всех договорах, связанных с регистрацией родовых доменов верхнего уровня (.com, .edu, .org, .net). 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, разные виды ответственности, киберпреступность).

Во-вторых, многие рассматривают существующую практику включения статьи об арбитраже в обычные соглашения как

невыгодную для более слабой стороны (обычно для пользователя или покупателя при осуществлении электронной коммерции).

В-третьих, некоторых волнует тот факт, что арбитраж выводит прецедентное право на глобальный уровень, что постепенно приведет к подавлению национальных правовых систем. В отношении коммерческого права это может оказаться более или менее приемлемым, принимая во внимание уже существующий высокий уровень унификации материально-правовых норм. Однако в области содержания материалов интернета и в отношении социокультурных аспектов национальные правовые системы важны, поскольку отражают культурные особенности своих стран.

В-четвертых, существующее законодательство, связанное с интернетом, показывает, что третейские суды, в частности основанные на ЕПРС, более лояльны к интересам делового сектора, нежели к интересам частных лиц. Приведем два похожих случая. В первом обычный французский суд вынес решение против французской компании «Данон» и в пользу ее недовольного сотрудника, зарегистрировавшего домен jeboycottedanone.com («я бойкотирую «Данон»). В то же самое время арбитраж ВОИС, основываясь на ЕПРС, принял требования компании Vivendi Universal удалить сайт vivendiuniversalsucks.com. В обоих случаях доменные имена использовались как форма протеста и критики. Обычный суд во Франции принял такой вид протеста, в то время как арбитраж ВОИС оказался не готов его принять.

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, вопросом, имеющим значительные правовые и политические последствия. Моменты, связанные с защитой прав интеллектуальной собственности, касаются

различных аспектов управления интернетом. Поскольку знания и идеи являются важной частью культурного наследия и социального взаимодействия, они имеют особую ценность для многих обществ. Право интеллектуальной собственности также находится в центре дискуссий о развитии. Связанные с интернетом аспекты проблемы касаются торговых марок, авторских прав и патентов.

ЗАЩИТА ТОРГОВЫХ МАРОК

Главной проблемой, с точки зрения защиты торговых марок, является регулирование регистрации доменных имен. На ранних стадиях развития интернета доменное имя предоставлялось тому, кто первым подал заявку. Это привело к практике так называемого «кибersквоттинга», то есть регистрации названий компаний в качестве доменных имен и их последующей перепродаже по более высокой цене. По мере распространения интернета и возрастания его экономического потенциала это стало большой проблемой, поскольку зачастую затрагивало репутацию компаний. Разрешение ситуации правовыми методами через традиционные судебные системы не представлялось целесообразным, поскольку на рассмотрение таких дел уходило слишком много времени.

Подобная ситуация заставила бизнес-сектор поставить вопрос о защите торговых марок в центр реформы управления интернетом, что привело к созданию в 1998 году Корпорации по присвоению имен и номеров в интернете (ИКАНН). В «Белой книге» правительство США уполномочило ИКАНН разработать и применять механизм защиты торговых марок в области доменных имен. Вскоре после своего создания ИКАНН представила Единую политику рассмотрения споров о доменных именах (ЕПРС), разработанную Всемирной организацией интеллектуальной собственности.

Использование ЕПРС в качестве механизма решения конфликтов стало обязательным условием всех соглашений, связанных с регистрацией доменных имен в родовых доменах верхнего уровня .com, .org, и .net. Владельцы торговых марок пропагандируют распространение принципа ЕПРС на национальные домены.

Вопросы защиты торговых марок также рассматриваются в следующих частях книги:
– Система доменных имен (с. 50)
– Единая политика рассмотрения споров о доменных именах (с. 100).

АВТОРСКОЕ ПРАВО

Развитие интернет-технологий, от возможности «вырезать и вставить» отрывок текста до более сложных действий, таких, как распространение музыкальных и видеофайлов через интернет, бросило вызов традиционной концепции авторского права. Материалы стало возможно копировать и распространять по всему миру с помощью интернета без значительных расходов.

Эти возможности ставят под угрозу хрупкое равновесие между интересами авторов материалов и заинтересованностью общества в развитии творческой деятельности, общественных знаний и всеобщего благосостояния. Предотвращение неограниченного копирования материалов и в то же время сохранение доступа к этим материалам является одной из головоломок управления интернетом. На сегодняшний день обладатели авторских прав, чьи интересы представляют крупные записывающие и мультимедийные компании, защищают свои права активнее, чем

Авторское право защищает только выражение идей в форме книг, компакт-дисков, компьютерных файлов. Сама идея авторским правом не защищается.

рядовые пользователи. Общественные интересы пока не формулируются достаточно четко и не защищаются в нужной степени.

Переломным моментом, повлекшим бурную реакцию со стороны обладателей авторских прав, стал обмен музыкальными файлами в рамках пиринговых сетей[1]. По некоторым оценкам, обмен музыкальными файлами с помощью программы Napster нанес звукозаписывающей индустрии ущерб в 4,3 млрд. долл. Реакция звукозаписывающей индустрии выявила многие подводные камни, ошибочные аналогии и недоработки существующей правовой системы. Данный эпизод также стал характеристикой существующего состояния защиты авторских прав в интернете и наличия многих нерешенных вопросов.

СОВРЕМЕННОЕ СОСТОЯНИЕ

Более строгая защита 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 более строгая защита интеллектуальной собственности была внедрена 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.

[1] Пиринговые сети (от англ. peer-to-peer — равный с равным; часто используется аббревиатура P2P) — компьютерные сети, в которых каждый пользователь сети (peer) может обмениваться данными с другими включенными в сеть компьютерами напрямую, без центрального сервера. Пиринговые сети наиболее часто используются для обмена большими файлами, в первую очередь музыкой, фильмами и компьютерными программами, в большинстве случаев с нарушением существующих законов об охране авторских прав. — *Прим. пер.*

Возрастающее количество судебных дел

Только в 2003 г. провайдерам интернет-услуг было направлено приблизительно 1000 судебных повесток с требованием прекратить деятельность по обмену файлами, осуществлявшуюся их клиентами, и было возбуждено более 500 уголовных дел против индивидуальных пользователей.

Дело против компаний Grokster и StreamCast, производящих ПО 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 разработки технологий, позволяющих пользователям обмениваться файлами в нарушение закона. Изначально суды США решили не признавать компании — производители ПО (такие, 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

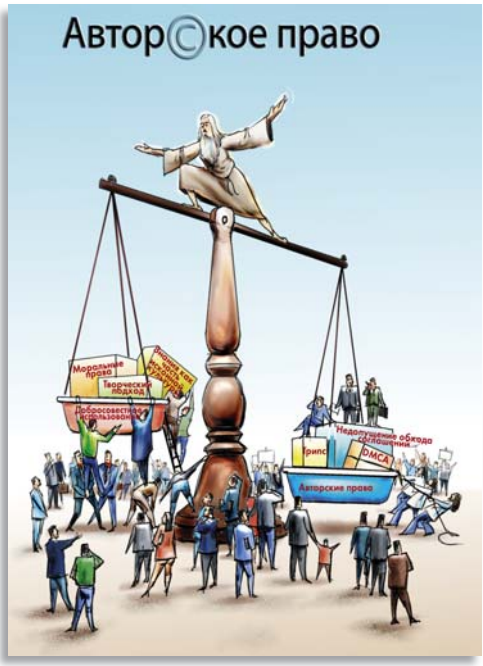
Инструменты, используемые нарушителями закона, могут также использоваться и его защитниками. Государственные власти и бизнес-структуры традиционно осуществляли свои функции с опорой на правовые механизмы. Однако активно набирает обороты использование «альтернативного» программного обеспечения для борьбы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

Статья в *International Herald Tribune* перечисляет следующие варианты использования ПО звукозаписывающими и развлекательными компаниями для защиты своих прав:

- трояны[2], перенаправляющие пользователей на веб-сайты, где они могут законным образом купить песню, которую пытались загрузить незаконно;

[2] Троян (троянский конь) — тип вредоносного компьютерного кода. Троян маскируется под полезную программу, одновременно выполняя определенную, неизвестную пользователю функцию. Весьма часто трояны используются для того, чтобы шпионить за поведением пользователя. — *Прим. пер.*

- ПО, блокирующее компьютер на некоторое время и выводящее на экран предупреждение о скачивании пиратских музыкальных файлов;
- «молчаливое» ПО, 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 в число мер, принятых для борьбы с нарушением авторских прав, не были включены вышеназванные меры. Означает ли это, что компании, самостоятельно предпринимающие такие меры, будут нарушать закон?

Технологии «управления цифровыми правами»

В качестве долговременного и более структурного подхода к решению проблемы бизнес-сектор внедряет различные технологии управления доступом к материалам, защищенным авторским правом. Компания Microsoft создала ПО для управления цифровыми правами (Digital Rights Management) 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. Последний,кроме того, придал противозаконный статус действиям, направленным на попытку 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» концепций «фиксации», распространения, передачи и публикации. Этот подход поддержан в основных международных соглашениях в области защиты авторских прав, включая Соглашение по торговым аспектам прав интеллектуальной собственности (ТРИПС) 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 все возрастающие возможности ограничения доступа к цифровым материалам, возникает вопрос о том, 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

Изначальной целью защиты авторского права было поощрение творчества и изобретений. Именно по этой причине в

это 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 жителям 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 попадет под защиту иностранных развлекательных и медиакомпаний.

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

В области защиты авторских прав существуют два основных международных режима. Всемирная организация интеллектуальной собственности (ВОИС) координирует режим

защиты интеллектуальной собственности в традиционном понимании, который основан на Бернской и Парижской конвенциях. Другой, зарождающийся, режим координируется Всемирной торговой организацией (ВТО) и основывается на Соглашении по торговым аспектам прав интеллектуальной собственности (ТРИПС). Координация вопросов интеллектуальной собственности на международном уровне была передана от ВОИС к ВТО с целью усиления защиты интеллектуальной собственности, 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 поиска равновесия между потребностями развития и защитой международных (в основном американских) прав интеллектуальной собственности. До сих пор в фокусе ВТО и ТРИПС были различные толкования прав интеллектуальной собственности в отношении фармацевтических товаров. Весьма вероятно, что в будущем темой дискуссий станет интеллектуальная собственность и интернет.

Ответственность провайдеров интернет-услуг за нарушение авторского права

Еще одним шагом в направлении ужесточения международных правоприменительных механизмов в сфере интеллектуальной собственности стало возложение на провайдеров интернет-услуг 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.

ПАТЕНТЫ

В традиционном понимании патент защищает новый процесс или продукт, главным образом в технической или производственной сфере. Лишь недавно стали выдавать патенты на ПО. По мере роста количества зарегистрированных патентов появляется все больше связанных с огромными деньгами судебных дел с участием американских компаний — производителей ПО.

С точки зрения управления интернетом, основным вопросом стала патентная защита бизнес-процессов в интернете, примером чему может служить используемая компанией Amazon процедура одинарного щелчка мышью («1-Click»). Основной критикой этого решения стало то, что Amazon запатентовала только идею (использование одинарного щелчка), а не конкретный бизнес-процесс (процедуру покупки).

Успешная регистрация патента на «1-Click» породила целую волну патентных заявок, включая некоторые смехотворные предложения — например, попытку получить патент на загрузку файлов из интернета. Другим непростым случаем стало требование компании British Telecom о выплате ей лицензионных вознаграждений по патенту на гипертекстовые ссылки, зарегистрированному в 1980 г. Если British Telecom добьется своего, пользователи интернета будут вынуждены платить за каждую созданную или использованную ссылку. В противном случае это дело уйдет в историю и встанет в один ряд с попытками запатентовать колесо.

Важно подчеркнуть, что практика выдачи патентов на ПО и связанные с интернетом процедуры не поддерживается Европейским Союзом и большинством стран мира.

КИБЕРПРЕСТУПНОСТЬ

Технологии создаются для того, чтобы приносить пользу, но ими очень часто пользуются неправильно или злоупотребляют. Говоря в целом, киберпреступность связана с нарушениями в области информационных и коммуникационных технологий. В то время как термин «преступление» достаточно хорошо определен (например, кража, детская порнография), существует много различных толкований компонента «кибер-».

Разрыв между «реальным» и «виртуальным» правом существует и в этой плоскости. Сторонники «реального» права подчеркивают, что киберпреступность — это известные и в «офлайновом» мире преступления, только совершенные при помощи компьютера. Преступления остаются теми же, отличаются только средства. В соответствии с «кибер-подходом», 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.

В 2003 году ОЭСР разработала основные принципы, призванные помочь правительствам в борьбе с интернет-мошенничеством. Евросоюз начал процесс подготовки и принятия Рамочных решений по киберпреступности[3], направленных на укрепление практических мер и взаимодействия в области борьбы с киберпреступностью.

[3] Framework Decision on Cybercrime

ВОПРОСЫ

Определение понятия «киберпреступность»

Определение понятия «киберпреступность» является одним из ключевых вопросов, имеющих практическое правовое значение. Существует много серьезных разногласий по поводу того, что такое киберпреступность, и такие расхождения в трактовке могут непосредственно сказаться на эффективности международного режима в области киберпреступности.

В частности, если определения киберпреступности в основном сосредоточиваются на методе совершения преступления (например, неавторизованный доступ к закрытым компьютерным системам), то существует возможность перепутать виртуальную преступность с так называемым «хактивизмом» (кампаниями гражданского неповиновения в киберпространстве).

Киберпреступность и права человека

Конвенция по 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.

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 данных 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 по киберпреступности касаются этой области.

ЭЛЕКТРОННЫЕ ЦИФРОВЫЕ ПОДПИСИ

Говоря в общем, электронные цифровые подписи — это инструмент, позволяющий идентифицировать человека в интернете, а 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 в целом является компонентом электронной коммерции. Она должна облегчать заключение электронных сделок за счет использования электронных контрактов. Например, является ли соглашение действительным, если оно заключено посредством электронной почты или на веб-сайте? Во многих странах закон требует, чтобы контракты были выполнены в письменном виде или подписаны. Что это означает применительно к интернету?

Столкнувшись с подобными дилеммами и необходимостью создать среду, способствующую ведению электронной коммерции, многие правительства начали принимать законы об электронной цифровой подписи. Основной сложностью остается тот факт, что правительства не регулируют существующую проблему

(противодействие киберпреступности или защита авторского права), а создают новую среду, не имея в этой области практического опыта. Это привело к появлению разнообразных решений и к общей неясности документов, касающихся электронной цифровой подписи.

В регулировании цифровых подписей сложились три главных подхода. Первый — «минималистский» подход, 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. Минимализм проявляется в части, касающейся признания подписей, существующих в электронном виде. Элементы максималистского подхода проявляются в том, что «передовые» (advanced) цифровые подписи имеют больший вес с точки зрения права (например, их правомерность легче доказать в суде).

Нормы ЕС о цифровых подписях стали одним из решений на многостороннем уровне. Хотя эти предписания были приняты всеми государствами — членами ЕС, разница в правовом статусе цифровых подписей сохраняется. Только восемь государств включили в свое законодательство предписания Директивы ЕС о том, что цифровые подписи должны иметь ту же юридическую силу, что и обычные.

На глобальном уровне Комиссия ООН по праву международной торговли (ЮНСИТРАЛ) приняла в 2001 г. Типовой закон по электронным подписям[4]. Этот закон придает электронным подписям тот же статус, что и обыкновенным, при условии, что соблюдаются определенные технические требования.

Международная торговая палата подготовила документ под названием «Общие методы осуществления международных торговых операций, заверенных в цифровой форме» (GUIDEC)[5], который содержит обзор имеющегося положительного опыта, норм и вопросов сертификации.

В непосредственной связи с цифровой подписью находятся инициативы, связанные с инфраструктурой «открытого ключа» (PKI)[6] . Созданием стандартов этой инфраструктуры занимаются две организации — МСЭ и РГПИ.

ВОПРОСЫ

Необходимость создания подробных стандартов, касающихся реализации решений

Хотя многие развитые страны приняли законодательные акты, в общем регламентирующие цифровые подписи, в этих документах зачастую отсутствует подробное описание стандартов и методов реализации решений. Принимая во внимание новизну проблем, 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 (РГПИ).

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

[4] Model Law on Electronic Signatures
[5] General Usage in International Digitally Ensured Commerce
[6] Public Key Infrastructure

Необходимый уровень гармонизации может быть достигнут при помощи региональных и глобальных организаций.

ТРУДОВОЕ ЗАКОНОДАТЕЛЬСТВО

Часто говорят о том, что интернет меняет «то, как мы работаем». Хотя это явление требует более подробного рассмотрения, следующие аспекты имеют непосредственную важность для управления интернетом.

- 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 защиты работников.
- С постоянным развитием телекоммуникаций и с распространенем широкополосного доступа к интернету все большее распространение получает работа на расстоянии (так называемая «телеработа»).
- Все более важной тенденцией становится передача части связанной с информационными технологиями работы в секторе обслуживания (call-центры, отделы обработки данных) на подряд в другие страны (аутсорсинг). 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 рабочих 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, и 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 перепиской 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 ВСИО, которая в § 47 призывает к уважению соответствую-

щих международных норм на рынке труда, связанного с информационно-коммуникационными технологиями.

ТАЙНА ЧАСТНОЙ ЖИЗНИ И ЗАЩИТА ДАННЫХ

Защита тайны частной жизни и защита данных — тесно взаимосвязанные аспекты управления интернетом. Защита информации является правовым механизмом, обеспечивающим защиту частной жизни.

Что такое «частная жизнь» *(privacy)*? Определение понятия «частная жизнь» зависит от точки зрения конкретного человека. Некоторые люди не возражают против частичного обнародования конфиденциальной информации о себе, в то время как другие стремятся оградить свою частную жизнь. Понятие «частная жизнь» также зависит от различия культур. Проблема соблюдения конфиденциальности, приватности, столь важная для западных обществ, может иметь меньшую значимость в других культурах.

Ввиду подобных разногласий необходимо дать более точное определение термина «частная жизнь», прежде чем его можно будет использовать в правовых концепциях. Определения существуют самые разные. Одно из традиционных описывает частную жизнь как «право остаться наедине с собой». Современные определения этого понятия делают акцент на тайне коммуникации (отсутствие слежки за перепиской) и защите частной информации (нераскрытие информации о частных лицах). Традиционно проблема защиты тайны частной жизни относилась в основном к взаимоотношениям между частными лицами и государством. Однако сейчас круг вопросов существенно расширился и включает в себя также деловой сектор, как показано на рисунке, приведенном на следующей странице.

Защита частной жизни: частные лица и государство

Информация всегда была для органов власти крайне важным «сырьем», основой контроля над территорией и населением. Информационные технологии значительно расширили возможности государств в области сбора и анализа информации. Это касается как информации, собираемой и обрабатываемой непосредственно властными структурами (налоги, социальная безопасность, здоровье, частная собственность, судимости), так и информации, с которой имеют дело компании, предоставляющие основные услуги населению (электричество, вода, телекоммуникации).

Вся подобная информация собирается с молчаливого, но вынужденного согласия граждан, поскольку они могут избежать подобной ситуации лишь эмигрировав в другую страну, где им все равно предстоит встретиться с подобными проблемами.

Передовые технологии обработки данных используются для накопления и интеграции данных из многих отдельных систем (например, информация налоговых органов, домовые книги, регистрация транспортных средств), а также для поиска в массивах данных закономерностей, несоответствий, необычных отклонений и т. д. Подобные сведения могут сильно повлиять на общество, но тем не менее в большинстве случаев

сбор таких данных не выходит за рамки Универсальной декларации прав человека.

Терроризм, шпионаж и другая деятельность, направленная против государства, обусловили необходимость ведения пристального наблюдения за подозрительными лицами (вне зависимости от их национальной принадлежности). Борцы за гражданские права предупреждают о постепенном размывании понятия частной жизни после введения еще более строгих мер в области национальной безопасности.

Несколько лет назад бурную реакцию общественности вызвало предложение оборудовать персональные компьютеры уникальным идентификационным устройством под названием «Clipper chip», которое — случайно или нет — могло также служить правительствам «лазейкой» для слежки за пользователями. Тогда победа была одержана защитниками гражданских прав, но сейчас маятник качнулся назад, в сторону усиления национальной безопасности.

Принятый в США после 11 сентября 2001 г. Патриотический акт (Patriot Act) и аналогичные законы в других странах задали рамки для более пристального контроля над электронной коммуникацией, включая право на законный перехват сообщений. Концепция законного перехвата с целью сбора улик также включена в Конвенцию по киберпреступности (статьи 20 и 21).

С развитием технологий возникает все больше инструментов слежения, которые смогут и дальше усиливать роль государства и ограничивать частную жизнь граждан.

Защита частной жизни: частные лица и организации

Второй стороной треугольника, иллюстрирующего различные компоненты защиты частной жизни, является взаимоотношение между частными лицами и бизнес-сектором. В информационной экономике сведения о клиентах, включая их предпочтения и особенности совершения покупок, становятся

важным товаром. Продажа данных о покупателях становится очень привлекательным бизнесом в интернете.

Существует и другой вид «слежки» коммерческих структур за частными лицами, применяющийся также и при осуществлении электронной коммерции. Миллионы частных лиц добровольно раскрывают коммерческим структурам значительный объем личной информации: номер кредитной карты, адрес и другую информацию, которая при злоупотреблении ею может привести к таким очень серьезным последствиям, как мошенничество или кража идентичности.

Успех и стабильность электронной коммерции как между организациями, так и между организациями и частными лицами, будет зависеть от доверия к политике обеспечения защиты частной жизни, проводимой бизнесом, и от мер безопасности, предпринимаемых для защиты конфиденциальной информации о клиентах от кражи и злоупотреблений.

Коммерческие структуры также используют технологии обработки информации для изучения предпочтений своих клиентов. Супермаркеты используют дисконтные карты, чтобы отслеживать покупательные привычки своих клиентов: например, в какой день недели и в какое время суток они предпочитают совершать покупки, сколько тратят, какие товары покупают и т. д. Результаты подобных анализов впоследствии используются для проведения персонализированного маркетинга товаров среди хорошо знакомых потребителей. Если законодательство о защите информации отсутствует, информация о частных лицах, собранная коммерческой фирмой, может быть продана и использована для других целей.

Защита частной жизни: государство и организации

О третьей стороне треугольника известно меньше всего, хотя это, может быть, самый значимый аспект, связанный с тайной частной жизни. Обе стороны — и государство, и организации — собирают значительный объем информации об отдельных лицах. Известно, что в рамках антитеррористических

мероприятий происходит обмен частью подобной информации. Однако в некоторых ситуациях, как, например, в предусмотренной Европейской директивой по защите данных, государство защищает информацию о гражданах, находящуюся в распоряжении коммерческих структур.

Защита частной жизни: граждане

Последним аспектом защиты частной жизни, не вошедшим в треугольник, становится потенциальная угроза приватности, исходящая от отдельных граждан. Современный технический прогресс предоставил частным лицам мощные инструменты для слежки. Даже простые мобильные телефоны с камерами могут стать средствами слежения. Более совершенные миниатюрные камеры и микрофоны можно купить по доступной цене. Технология, по выражению одного из авторов журнала *Economist*, «демократизировала слежку». Зарегистрировано много случаев нарушения неприкосновенности частной жизни — от простого подглядывания за соседями до более изощренного использования камер с целью записи номеров банковских карт и электронного шпионажа.

Основная проблема заключается в том, что большая часть законодательных норм касается защиты тайны частной жизни от государства. Столкнувшись с новыми явлениями, некоторые страны стали предпринимать соответствующие шаги. Конгресс США принял Акт о предотвращении видеовуайеризма[7], запрещающий фотографировать обнаженных людей без их согласия. Похожие законы, ограничивающие возможности слежки одних частных лиц за другими, были также приняты в Германии и в некоторых других странах.

Международное регулирование защиты частной жизни и конфидециальных сведениий

Основным международным документом, регулирующим защиту частной жизни и конфидециальных сведений, стали

[7] Video Voyeurism Prevention Act

подготовленные ОЭСР в 1980 г. Основные принципы защиты частной жизни и трансграничных потоков личных данных[8]. Эти принципы и последующая работа ОЭСР привели к созданию многих международных и региональных норм в этой области. Предложенные ОЭСР принципы были приняты во многих странах и регионах (различия кроются в способе их применения).

Один из подходов, использующийся в США, основан на саморегулировании. Политика обеспечения конфиденциальности определяется компаниями. Компании и частные лица могут сами решать, какой следует быть этой политике. Главным аргументом против этого подхода может стать то, что потребители оказываются в невыгодном положении.

В соответствии со вторым подходом, который предлагается Европейским Союзом, защита частной жизни должна обеспечиваться органами государственной власти. Такой подход к защите частной жизни, изложенный в Европейской директиве по защите данных 1995 г. (95/46/EC), регулирует защиту граждан при обработке личной информации и обмене такой информацией. Помимо директивы, являющейся основным механизмом, европейский подход к защите частной жизни и информации также формировался другими региональными инструментами, например Конвенцией Совета Европы по защите частных лиц при автоматической обработке личной информации 1981 г.[9]

Между двумя этими подходами — американским и европейским — возникли противоречия. Основная проблема — использование личных данных коммерческими структурами. Каким образом ЕС может обеспечить соблюдение своих норм, скажем, компанией по производству ПО, расположенной в США? Каким образом ЕС может гарантировать, что инфор-

[8] Guidelines on Protection of Privacy and Transborder Flows of Personal Data
[9] Council of Europe's Convention on the Protection of Individuals with regard to Automatic Processing of Personal Data

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? ЕС угрожал блокировать передачу данных в любую страну, которая не может обеспечить уровень защиты информации, соответствующий директиве. Такая позиция неизбежно вела к конфликту с американским подходом.

Эти глубокие различия затруднили процесс достижения 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 Аарон предложил формулу «безопасной гавани» (*safe harbor*). Это предложение представило проблему в новом свете и позволило выйти из дипломатического тупика.

В соответствии с предложенной формулой законодательство ЕС могло применяться к американским компаниям в своего рода правовой «безопасной гавани». Американские компании, работающие с информацией о гражданах ЕС, могут добровольно взять на себя обязательство соблюдать европейские требования по защите конфиденциальной информации, а также учитывать действие тех правоприменительных механизмов, по которым между ЕС и США было достигнуто соглашение.

Противоречащие друг другу взгляды США и ЕС на проблему защиты частной жизни в электронную эпоху показали, что взаимозависимость, порожденная электронной коммерцией, может бросить вызов некоторым основным принципам, заложенным в общественной и культурной истории двух регионов. Глобализация приведет к повторению подобной ситуации и в других странах. Соглашение о «бе-

зопасной гавани» следует рассматривать как ценный прецедент и полезный инструмент для подготовки аналогичных соглашений между ЕС и другими странами, включая Канаду и Австралию.

ЧАСТЬ 4

Экономические аспекты

КОРЗИНА «ЭКОНОМИЧЕСКИЕ АСПЕКТЫ»

Важность экономического аспекта управления интернетом может проиллюстрировать название документа, положившего начало реформе управления интернетом и учредившего ИКАНН, — «Основы глобальной электронной коммерции» (1997 г.). В этом документе указано, что «частный сектор должен возглавить» процесс управления интернетом, и основная функция такого управления заключается в обеспечении «предсказуемой, минималистской, непротиворечивой и простой правовой среды для электронной коммерции». Эти принципы являются фундаментом режима управления интернетом, в центре которого находится ИКАНН.

Различные политические и регулятивные механизмы, имеющие большую важность для электронной коммерции, рассматриваются также и в других «корзинах».

Корзина «Инфраструктура и стандартизация»

- Внедрение *широкополосного доступа* и обеспечение *качества услуг* являются важнейшим условием быстрого развития электронной коммерции в сфере мультимедиа (например распространения аудио- и видеопродукции).
- Обеспечение *безопасности интернета* должно повысить надежность и устойчивость среды электронной торговли. Это является необходимым условием и для укрепления доверия потребителей к этой сфере.
- *Шифрование информации* крайне важно для защиты коммуникации, особенно при осуществлении финансовых транзакций.

Корзина «Правовые аспекты»

- Решение вопросов *юрисдикции* важно для обеспечения надежности электронной коммерции с правовой точки зрения, в особенности для защиты интересов потребителей.

- В связи с увеличением объема сделок, связанных с нематериальными товарами, особую важность для электронной коммерции приобретает защита *прав интеллектуальной собственности.*
- Использование *электронной цифровой подписи* (ЭЦП) упрощает совершение сделок и решает проблему идентификации.
- По мере того как в процессе электронной коммерции собирается все больше информации о покупателях, вопросы *защиты данных* приобретают актуальность в контексте защиты тайны частной жизни.

ЭЛЕКТРОННАЯ КОММЕРЦИЯ

Четкое определение понятия «электронная коммерция» имеет множество практических и юридических последствий. 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 в онлайне, 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.

Существуют различные виды электронной коммерции:

- 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. В 2001 г. объем сделок в рамках этого вида электронной торговли в США достиг 995 млрд. долл., что составляет 93,3% 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; в первую очередь электронные аукционы (такие, как eBay).

Многие страны разрабатывают правовую среду для регулирования электронной коммерции. Уже приняты законы, касающиеся ЭЦП, разрешения споров, киберпреступности, защиты прав пользователей и налогообложения. На международном уровне также появляется все больше 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 торговли вопросы, в том числе либерализацию телекоммуникаций, защиту прав интеллектуальной собственности и некоторые аспекты развития информационно-коммуникационных технологий (ИКТ). Следующие 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[1], в рамках которой продолжается дискуссия по связанным с этим видом коммерции вопросам.

[1] WTO Work Programme for Electronic Commerce

Хотя вопросы электронной коммерции до сих пор оставались на периферии деятельности ВТО, в данной области было предложено много инициатив и определен ряд ключевых вопросов.

1. *Является ли электронная коммерция торговлей товарами (регулируемой в рамках ГАТТ[2]) или торговлей услугами (регулируемой в рамках ГАТС[3])?*

   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 один и тот же музыкальный альбом может иметь различный торговый статус (и подлежать обложению разными налогами и таможенными пошлинами) в зависимости от способа его доставки потребителю. Проблема классификации очень важна, поскольку к торговле товарами и услугами применяются разные правовые нормы.

2. *Какой должна быть связь между ТРИПС и защитой прав интеллектуальной собственности в интернете?*

   Поскольку ТРИПС предоставляет гораздо более мощные механизмы обеспечения соблюдения норм в области прав интеллектуальной собственности, развитые страны пытались распространить сферу применения ТРИПС на электронную коммерцию и интернет в целом, опираясь при этом на два подхода. Во-первых, апеллируя к принципу «технологической нейтральности», они указывали, что ТРИПС, 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 ТРИПС. ТРИПС предусматривает более мощные правоприменительные механизмы,

[2] Генеральное соглашение по тарифам и торговле (General Agreement on Tariffs and Trade)
[3] Генеральное соглашение по торговле услугами (General Agreement on Trade in Services)

чем конвенции ВОИС. Оба вопроса остаются открытыми, их важность для переговоров в рамках ВТО в будущем возрастет.

На сегодняшней стадии переговоров по торговле в повестке дня ВТО электронной коммерции вряд ли будет уделено существенное 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.

ДРУГИЕ МЕЖДУНАРОДНЫЕ ИНИЦИАТИВЫ В ОБЛАСТИ ЭЛЕКТРОННОЙ ТОРГОВЛИ

Одной из наиболее успешных и активно поддерживаемых международных инициатив в области электронной коммерции является Типовой закон об электронной торговле, подготовленный Комиссией ООН по праву международной торговли (ЮНСИТРАЛ). Центральным моментом проекта являются механизмы 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[4] стандарта ebXML, который в скором времени может стать основным стандартом для обмена электронной торговой документацией и вытеснить используемый сейчас стандарт EDI[5].

Деятельность ОЭСР затрагивает множество вопросов, связанных с электронной торговлей, в том числе защиту прав пользователей и использование ЭЦП. ОЭСР способствует развитию электронной коммерции и исследованию связанных с ней вопросов путем публикации рекомендаций и директив. Другие международные организации — такие, как Конференция ООН

[4] United Nations Centre for Trade Facilitation and Electronic Business — UN/CEFAT
[5] Electronic Data Interchange — электронный обмен данными (англ.)

по торговле и развитию (ЮНКТАД) и Целевая группа ООН по информационно-коммуникационным технологиям[6], — также проводят различные мероприятия, направленные на развитие потенциала и исследования в области электронной торговли.

В бизнес-секторе самыми активными организациями являются Международная торговая палата[7], которая выпускает большое количество рекомендаций и аналитических докладов по вопросам электронной коммерции, а также Глобальный бизнес-диалог[8] , который содействует развитию электронной торговли как на национальном, так и на международном уровнях.

РЕГИОНАЛЬНЫЕ ИНИЦИАТИВЫ

ЕС разработал 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, и ограничение распространения наносящих вред материалов). ЕС принял Директиву по электронной коммерции, а также ряд других документов по использованию ЭЦП, защите данных и электронным финансовым транзакциям.

В Азиатско-Тихоокеанском регионе центром взаимодействия в сфере электронной торговли является Азиатско-Тихоокеанское экономическое сотрудничество (АТЭС). Руководящая группа по электронной коммерции[9], созданная в рамках АТЭС, исследует различные вопросы, связанные с электронной коммерцией, в том числе вопросы защиты прав потребителей, защиты данных, спама и киберпреступности. Последней и на

[6] UN ICT Task Force
[7] International Chamber of Commerce
[8] Global Business Dialogue
[9] E-Commerce Steering Group

иболее значимой законодательной инициативой является Индивидуальный план действий АТЭС по развитию безбумажной торговли[10], 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. Электронная коммерция является относительно новой сферой деятельности, поэтому потребители еще не доверяют ей 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 является необходимость защиты прав потребителей на международном уровне, что не является приоритетом для традиционной торговли. Если раньше потребители редко нуждались в международной защите, то с развитием электронной коммерции все больше сделок выходит за пределы национальных границ. В связи с этим возрастает актуальность вопроса о юрисдикции, к которому существует два основных подхода.

Первый подход более выгоден для продавцов (преимущественно компаний, осуществляющих электронную торговлю) и основывается на принципе «страны происхождения», или

[10] APEC Paperless Trading Individual Action Plan

«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 со множеством разнообразных правовых систем. Одним из предлагаемых механизмов разрешения этой дилеммы является гармонизация законодательства различных стран в сфере защиты прав потребителей, что делает менее актуальным сам вопрос о юрисдикции.

В области защиты прав потребителей, как в других связанных с электронной коммерцией вопросах, ведущую роль на международной арене играет ОЭСР. В рамках этой организации были приняты Директива по защите прав потребителей в контексте электронной коммерции[11] (2000 г.) и Директива по защите потребителей от мошеннических и обманных действий на трансграничном уровне[12] (2003 г.). Основные принципы, разработанные ОЭСР, были заимствованы некоторыми бизнес-ассоциациями, включая Международную торговую палату и Совет агентств по улучшению деловой практики[13]

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 каких-либо действенных международных правовых инструментов создано не было. Один из наиболее значимых документов — Конвенция ООН о договорах международной

[11] Guidelines for Consumer Protection in the Context of E-commerce
[12] Guidelines for Protecting Consumers from Fraudulent and Deceptive Commercial Practices Across Borders
[13] Council of Better Business Bureaus

купли-продажи товаров[14] (1980 г.) — не затрагивает вопросов заключения потребительских договоров и защиты прав потребителей.

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

НАЛОГООБЛОЖЕНИЕ

Возникший в управлении интернетом спор о том, должны ли вопросы киберпространства рассматриваться как отличные от явлений реального мира, ярко проявляется в вопросе о налогообложении. США с самого начала пытались объявить интернет зоной, свободной от налогов.

В 1998 году Конгресс США принял Акт о свободе от налогов[15]. 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. Многие штаты США солидарны с этим, выступая за налогообложение коммерческой деятельности в интернете.

Еще одной проблемой из области налогообложения интернет-коммерции, по которой позиции США и ЕС расходятся, является вопрос о том, 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 вы-

[14] UN Convention on Contracts for the International Sale of Goods
[15] Tax Freedom Act

двинут критерий «страны назначения», что соответствует интересам ЕС, где с точки зрения электронной коммерции больше покупателей, чем продавцов.

ТАМОЖЕННОЕ РЕГУЛИРОВАНИЕ

Электронная коммерция напрямую касается и вопросов таможенного регулирования. Международные транзакции с товарами в цифровом формате невозможно контролировать так же, как сделки с материальными товарами. Определить, содержит ли передаваемый через интернет пакет информации товар, с которого должна быть уплачена таможенная пошлина, практически невозможно. В связи с этим возникает множество вопросов о применимости существующей системы таможенного регулирования к электронной коммерции и о внедрении новых процедур.

На политическом уровне основной инициативой является мораторий ВТО на обложение интернет-транзакций таможенными пошлинами, в последний раз официально продленный на саммите в Дохе в 2001 г. На провальном саммите ВТО в Канкуне в 2003 г. этот вопрос не обсуждался, что вызвало споры о том, действителен ли по-прежнему этот глобальный мораторий. Однако, с практической точки зрения, это не имеет большого значения, поскольку обложение таможенными пошлинами товаров и услуг, доставляемых через интернет, чрезвычайно сложно вследствие технических сложностей, связанных с контролем над содержанием интернет-трафика.

ЭЛЕКТРОННЫЕ ПЛАТЕЖИ: ИНТЕРНЕТ-БАНКИНГ И ЭЛЕКТРОННЫЕ ДЕНЬГИ

Понятие «электронные платежи» может быть определено как заключение финансовых сделок в пределах киберпространства с ис-

пользованием различных инструментов онлайн-платежей. Существование системы электронных платежей является предпосылкой успешного развития электронной торговли. Сфера электронных платежей требует разграничения понятий «электронные деньги» и «интернет-банкинг».

Предоставление банковских услуг 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. С точки зрения управления, интернет-банкинг не порождает каких-либо специфических вопросов, помимо уже освещенных (таких, как защита прав потребителей на международном уровне).

Вместе с тем электронные деньги представляют собой значительное нововведение. Правление Федеральной резервной 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 микропроцессором;
- 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 в отношении электронных денег.

На сегодняшний день использование электронных денег находится на ранней стадии своего развития. Электронные деньги не по-

лучили широкого распространения главным образом из-за недостаточного уровня безопасности и конфиденциальности. Развитие электронных денег возможно в двух направлениях:

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

2) революционное — 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 по сути отсутствие контроля над ними со стороны центрального банка страны. Подобный подход даст возможность частным организациям выпускать деньги для использования в электронной коммерции. По словам одного известного банкира, «наследники Билла Гейтса оставят без работы наследников Алана Гринспена». Подобный вариант развития окажет значительное влияние на будущее развития государств и международных отношений. Как заметил вышеупомянутый банкир, «в прошлом общества могли обходиться без банков. Возможно, смогут и в будущем». Другие возможности использования электронных денег остаются дискуссионными.

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. Более экономически эффективные онлайновые банковские услуги бросят серьезный вызов традиционным банкам «из стекла и бетона».

2. Согласно опросам, *отсутствие средств платежа* (например электронных карт) является третьей по значимости причиной того, что потенциальные покупатели не участвуют в электрон-

транзакций и конфиденциальности данных. На сегодняшний день осуществление электронной коммерции практически невозможно без применения электронных карт. Это является существенным препятствием для тех стран, где рынок кредитных карт не развит. Правительствам этих стран придется внести необходимые поправки в законодательство, чтобы ускорить внедрение карточных платежных систем.

3. 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 Гонконга, первым принявшего комплексное законодательство в области электронной коммерции, в ЕС в 2000 г. была принята Директива об электронных деньгах.

   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 Сакстона, «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.

4. По мнению некоторых аналитиков, перспективы действительно масштабного развития электронной коммерции во многом связаны с введением эффективной и надежной услуги 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. W3C, ведущая организация в области стандартов интернета, уже разрабатывает необходимые стандарты для систем микроплатежей.

5. Учитывая саму природу интернета, весьма вероятно, что электронные деньги станут глобальными, — а это даст повод рассматривать вопрос на международном уровне. Одним из возможных действующих лиц в сфере предоставления банковских услуг онлайн является Группа по электронным банковским услугам Базельского комитета[16]. Она уже начала заниматься проблемами аутентификации, стандартов проверки благонадежности, прозрачности, конфиденциальности, отмывания денег и трансграничного надзора над банковской деятельностью — ключевыми вопросами с точки зрения внедрения электронных денег.

6. Разработано много видов электронных платежей, особенно в рамках развитых экономических систем. Осуществлять электронные платежи можно только в стабильной, безопасной и функциональной правовой среде. В то же время в большинстве развивающихся стран основу экономики составляют наличные расчеты. Если осуществление платежей с использованием карт и возможно, то оно должно быть подтверждено личной подписью. Это серьезное несоответствие также влияет на развитие электронной коммерции и увеличивает разрыв в цифровых технологиях между богатым Севером и бедным Югом. В отличие от таких мер, как покупка оборудования, введение электронных платежей потребует множества постепенно внедряемых институциональных, технических и законодательных решений. Одним из основных элементов, который важен как для электронной коммерции, так и для электронных платежей, но который нельзя создать в короткие сроки, является доверие потребителей.

7. Недавнее обращение генерального прокурора штата Нью-Йорк к системе Paypal и банку Citibank с требованием не осуществлять платежи интернет-казино напрямую связывает электронные платежи и обеспечение правопорядка. То, чего правоохранительные органы не могут достигнуть с помощью правовых механизмов, они могут попытаться добиться за счет контроля над электронными платежами.

[16] Basel Committee E-Banking Group

ЧАСТЬ 5

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. Благодаря ему произошло значительное перераспределение богатства и власти как на уровне отдельных индивидов, так и в масштабе всего мира. То воздействие, которое оказали информационные технологии на распределение власти и на развитие, породило много вопросов, например:

- Каким образом изменения, ускоренные развитием информационно-коммуникационных технологий, повлияют на уже существующий разрыв между Севером и Югом? Увеличат ли ИКТ этот разрыв или же 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 места связанных с развитием вопросов в контексте управления интернетом.

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

- наличие телекоммуникационной инфраструктуры является предпосылкой для преодоления разрыва в цифровых технологиях;
- текущая экономическая модель доступа к интернету возлагает несоразмерно тяжелое бремя на те 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 в силу ограниченных возможностей развивающихся стран получать доступ к знаниям и информации в интернете.

В различных документах неоднократно подчеркивалась важность связанных с развитием аспектов деятельности ВСИО, начиная с Резолюции Генеральной Ассамблеи ООН по ВСИО, подчеркивающей, что саммит должен «способствовать развитию, в особенности с точки зрения доступа к технологиям и их передачи». Женевская декларация и План действий ВСИО ставят развитие во главу угла и связывают его с Декларацией Тысячелетия, которая постулирует необходимость «доступа всех стран к информации, знаниям и коммуникационным технологиям в целях развития». Будучи связанным с «Целями Тысячелетия», ВСИО играет важную роль в деле развития.

В настоящей главе мы уделим внимание только основным вопросам, связанным с развитием: разрыву в цифровых технологиях и обеспечению универсального доступа. Именно они часто обсуждаются в контексте развития. Затем мы проведем анализ основных факторов, влияющих на интернет и развитие: инфраструктуры, финансовой поддержки, политических вопросов, а также социокультурных аспектов.

Каким образом ИКТ влияют на развитие общества?

Основные вопросы, связанные с информационными технологиями и развитием, резюмировались в статье журнала *Economist* «Проваливаясь сквозь Сеть?»(сентябрь 2000 г.). Статья приводит доказательства как за, так и против утверждения 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 фирмы-гиганты вытесняют из электронной коммерции маленькие фирмы развивающихся стран. • Утеря продавцом главенствующей позиции и возрастание роли покупателя (в интернете «другой поставщик всегда рядом — только мышкой щелкнуть») вредит более бедным странам, в первую очередь производителям сырьевых товаров в развивающихся странах. • Более высокий интерес, проявляемый к «высокотехнологичным» акциям 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. Другие технологии (железные дороги и электричество) распространялись в развивающихся странах десятилетиями, тогда как ИКТ распространяются очень стремительно. • Возможность «перепрыгнуть» устаревшие технологии, пропустить такие переходные стадии, как медные провода и аналоговая телефония, что 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, имеет доступ к ИКТ, и теми, кто такого доступа 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 являются независимыми явлениями. Они отражают существующее общественно-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».

Увеличивается ли цифровой разрыв?

ИКТ развиваются намного быстрее, чем другие области (например, сельское хозяйство или медицина), и в силу того, что развитые страны (в отличие от развивающихся) обладают необходимым инструментарием, позволяющим успешно пользоваться достижениями ИКТ, создается впечатление, что «цифровой разрыв» увеличивается постоянно и с довольно внушительной скоростью. Такая точка зрения излагается во многих уважаемых источниках, например в Докладе о развитии человечества 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 ИКТ на общество — на людей, живущих в развивающихся странах. Примером могут послужить успехи Индии и Китая в области цифровых технологий.

УНИВЕРСАЛЬНЫЙ ДОСТУП

Помимо «цифрового разрыва», другой часто упоминаемой концепцией в дискуссиях о развитии является универсальный доступ, то есть доступ для всех. Хотя этот аспект должен быть краеугольным камнем любой политики, проводимой в отношении информационных технологий, существуют различные мнения и различное понимание сущности и масштаба политики универсального доступа. Частое упоминание универсального доступа 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 универсального доступа на международном уровне остается во многом вопросом политическим, который зависит в конечном счете от готовности развитых стран осуществлять инвестиции для достижения этой цели.

В отличие от универсального доступа на международном уровне, в некоторых странах универсальных доступ является хорошо развитой экономической и правовой концепцией. 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 стоит дорого. Субсидии предоставляются регионами с низкими расценками на связь — главным образом большими городами. ЕС также предпринял ряд конкретным мер, направленных на обеспечение универсального доступа.

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 такой подход не оправдал себя во многих странах (главным образом в бывших социалистических странах), где стало очевидно, что развитие общества является гораздо более сложным процессом. Технология является необходимой, но не единственной предпосылкой для развития. Другие элементы включают в себя нормативные рамки, финансовую поддержку, наличие людских ресурсов, а также другие 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 является необходимым условием для знакомства отдельных лиц и организаций с интернетом и в итоге — для преодоления «цифрового разрыва». Существуют различные способы установления связи и улучшения качества подключения.

Быстрый рост беспроводной связи предоставляет многим развивающимся странам новые возможности. Патрик Гельсингер, сотрудник компании Intel, считает целесообразным для развивающихся стран отказаться от телекоммуникаций, основанных на использовании медных проводов, и применять беспроводные способы связи для создания линий связи на участке «провайдер—пользователь», а также оптоволоконные сети для общенациональных информационных магистралей. Беспроводная коммуникация может помочь решить проблему развития традиционной инфраструктуры наземных коммуникаций (избавить от необходимости прокладки кабелей через огромные расстояния многих азиатских и африканских стран). Таким образом можно преодолеть проблему «последней мили» (местной линии связи) — одну из основных преград на пути ускорения развития интернета. Инфраструктурный аспект цифрового разрыва находится в центре внимания Международного союза электросвязи (МСЭ).

ФИНАНСОВАЯ ПОДДЕРЖКА

Развивающиеся страны получают финансовую поддержку через различные каналы, включая двусторонние и многосторонние агентства содействия развитию (такие, как Программа развития ООН или Всемирный банк), а также через региональные инициативы по развитию и региональные банки. По мере либерализации рынка телекоммуникаций соответствующая инфраструктура все больше развивается 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 все еще не готовы к инвестициям, ожидается, что в недалеком будущем они будут вкладывать деньги в развивающиеся страны, поскольку рынок развитых стран перенасыщен мощностями, созданными в конце 1990-х гг.

Важность финансового аспекта была однозначно признана во время Женевского этапа Всемирного саммита по информационному обществу. Некоторые из участников выступали за создание Фонда цифровой солидарности при ООН, в задачи которого входила бы помощь малообеспеченным странам в создании телекоммуникационной инфраструктуры. Предполагалось, что фонд будет опираться на добровольные пожертвования. Также рассматривалась система взносов, например по 1 доллару при покупке персонального компьютера, ПО или сетевого оборудования. Однако предложение основать Фонд цифровой солидарности не получило широкой поддержки от развитых стран, с точки зрения которых прямые инвестиции являются предпочтительнее централизованного фонда развития. Для исследования возможностей создания более гибких и более подходящих схем финансирования было решено основать Рабочую группу по финансированию ИКТ для развития, которая доложит о своей работе на очередном этапе Всемирного саммита по информационному обществу в 2005 году в Тунисе.

СОЦИОКУЛЬТУРНЫЕ АСПЕКТЫ

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

Для развивающихся стран одной из самых больших проблем является «утечка умов», под которой подразумевают отток высококвалифицированной рабочей силы из развивающихся страны в развитые. Из-за этого развивающиеся страны проигрывают одновременно по нескольким показателям.

Основной — потеря квалифицированной рабочей силы. Развивающиеся страны также теряют средства, вложенные в обучение уехавших специалистов. Вполне вероятно, что «утечка умов» будет продолжаться, в особенности с учетом различных иммиграционных программ и облегченных схем устройства на работу, внедренных в США, Германии и других странах с

целью привлечения квалифицированных специалистов в области ИКТ.

Одним из условий, которое может остановить или даже повернуть вспять «утечку умов», является передача некоторых задач в области ИКТ развивающимся странам. Удачный пример — создание центра по разработке ПО в Бангалоре (Индия).

На международном уровне ООН основала Сеть цифровых диаспор[6] для ускорения темпов развития в Африке посредством мобилизации технологических, деловых и профессиональных знаний и ресурсов африканских диаспор в области ИКТ.

Инициативы ЮНЕСКО особенно важны при рассмотрении социального аспекта «цифрового разрыва». ЮНЕСКО приняла Конвенцию о защите культурного разнообразия и стала инициатором нескольких проектов, направленных на поддержку языкового и культурного разнообразия в интернете.

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 нормативных рамок. В-третьих, существование национальных телекоммуникационных монополий является одной из причин более высокой стоимости доступа к интернету.

Создание соответствующей среды является сложной задачей, предполагающей постепенную демонополизацию рынка телекоммуникаций, разработку связанного с интернетом законодательства (по вопросам авторского права, права на частную

[6] Digital Diaspora Network

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 главенствующих 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. В соответствии с этой точкой зрения, проиграли в этой игре правительства развивающихся государств, а победили 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 понизились цены. В конце концов это приведет к появлению эффективного и доступного сектора телекоммуникаций, что является необходимым условием для развития общества.

ЧАСТЬ 6

Социокультурные аспекты

КОРЗИНА «СОЦИОКУЛЬТУРНЫЕ АСПЕКТЫ»

Сети, объединяющие компьютеры, существовали и до появления интернета. Отличительной особенностью интернета является его способность облегчить различные формы взаимодействия между людьми, а также способствовать осуществлению человеком своей творческой деятельности. Наиболее важным прорывом стало использование интернета для новых форм коммуникации (таких, как электронная почта, WWW, мультимедиа). В связи с этим некоторые специалисты полагают, что интернет является больше социальным, нежели технологическим явлением. Он дополняет привычные формы общения, а также создает новые (например кибер-сообщества). Все это привело к появлению социокультурного аспекта управления интернетом. Данная «корзина» включает в себя некоторые из наиболее спорных вопросов управления интернетом: политика в отношении содержания материалов и многоязычие. Эти вопросы, как никакие другие, отражают наиболее яркие национальные, религиозные и культурные различия в современном мире.

ПОЛИТИКА В ОТНОШЕНИИ СОДЕРЖАНИЯ МАТЕРИАЛОВ ИНТЕРНЕТА

Одним из основных вопросов в рамках социокультурного аспекта управления интернетом является политика в отношении содержания информационных материалов (content policy), которая часто рассматривается с точки зрения соблюдения прав человека (свобода выражения убеждений и право на общение), 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, в необходимости контролировать распространение которых ни у кого нет 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 *(jus cogens)*. Хотя необходимость удаления подобных материалов из интернета не вызывает сомнений, остаются расхождения в интерпретации. Например, какие именно действия можно расценивать как поддержку терроризма?

Вторая группа представлена материалами, которые могут оказаться оскорбительными для определенных стран, регионов или этнических групп в силу их религиозных или культурных особенностей. Глобальная и более интенсивная коммуникация является вызовом культурным и религиозным ценностям. Большинство судебных прецедентов, связанных с интернетом, касается материалов именно этой группы. В деле Yahoo! французский суд потребовал, чтобы американская компания Yahoo.com (США) закрыла для французских граждан доступ к частям своего портала, на которых продавались нацистская символика и реликвии. В Германии также существует развитая судебная практика в отношении сайтов, содержащих материалы нацистской направленности. 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.

Третью группу составляют материалы, спорные с политической или идеологической точек зрения. По сути, здесь имеет место цензура интернета. Неправительственная организация Transparency International сообщает о фактах подобной деятельности в Китае, Бирме и Саудовской Аравии.

КАКИМ ОБРАЗОМ ОСУЩЕСТВЛЯЕТСЯ ПОЛИТИКА В ОТНОШЕНИИ МАТЕРИАЛОВ ИНТЕРНЕТА?

«Основное меню» политики в отношении материалов интернета включает в себя следующие правовые и технические возможности, используемые в разных сочетаниях.

Правительственная фильтрация материалов

Распространенным способом правительственной фильтрации является «интернет-индекс» веб-сайтов, доступ к которым запрещен. Если веб-сайт включен в такой индекс, доступ к нему не предоставляется. С технической точки зрения, фильтрация осуществляется при помощи блокировки IP-адресов на уровне маршрутизаторов, прокси-серверов и переназначения при обращении к DNS. Фильтрация материалов применяется во многих странах. Широко практикуют фильтрацию Китай, Саудовская Аравия и Сингапур. Другие страны также все чаще используют ее. Например, в Австралии есть система фильтрации для отдельных страниц внутри страны. Законодательство земли Северный Рейн — Вестфалия (ФРГ) требует, чтобы интернет-провайдеры фильтровали доступ пользователей, главным образом к неонацистским сайтам (однако не только к ним).

Частные системы рейтингов и фильтрации

Столкнувшись с риском распада интернета в связи с развитием различных государственных барьеров (систем фильтрации), W3C и другие подобные институты предложили внедрять *системы рейтингов и фильтрации,* контролируемые конечными пользователями. С технической точки зрения, фильтрующие механизмы встраиваются в интернет-браузеры. Доступность определенных материалов обозначается специальным значком, соответствующим определенному веб-сайту. Использование подобной фильтрации особенно приветствовалось в качестве метода ограничения доступа к веб-сайтам «для взрослых».

Геолокационное программное обеспечение

Другим техническим решением, связанным с материалами интернета, является геолокационное ПО, которое фильтрует доступ пользователей к определенным материалам в зависимости от их географического местонахождения. Дело Yahoo! стало значимым с этой точки зрения, поскольку занимавшаяся им группа экспертов, включая Винтона Серфа[1], заявила, что в 90% случаев Yahoo! сможет определить, находится ли пользователь, пытающийся зайти в раздел сайта с нацистскими материалами, во Франции. Подобная техническая оценка помогла суду принять окончательное решение. Компании, занимающиеся геолокационным ПО, заявляют, что они могут определить страну без ошибки, а город — примерно в 85% случаев, в особенности если это большой город. Геолокационное ПО может помочь владельцам сайтов фильтровать доступ к материалам в зависимости от местонахождения пользователя и таким образом избегать судебных исков в других странах.

Контроль над материалами с помощью поисковых систем

Между наличием материала в интернете и его доступностью есть существенная разница. Сам факт того, что некоторая веб-страница или материал находится в интернете, не означает, что к ним получит доступ много пользователей. Например, если определенный сайт невозможно найти при помощи поисковой системы Google, его значимость существенно уменьшается. Поисковая система является мостиком между материалом и пользователем. Много пишут о том, что одним из первых примеров контроля над материалами с помощью поисковых систем стали действия китайских властей в отношении поисковой системы Google. Если пользователи вводили запрещенные слова в поисковую систему, их компьютер на несколько минут терял связь с интернетом. 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».

[1] Один из создателей протокола TCP/IP, часто называемый «отцом интернета». — *Прим. пер.*

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. По сути, это самоцензура со стороны Google, которая осуществляется во избежание возможных судебных исков.

Необходимость создания соответствующей правовой базы

Правовой вакуум в области политики в отношении материалов интернета, характерный для раннего периода развития интернета, давал правительствам почти полную свободу действий в сфере контроля над материалами. Поскольку политика в отношении материалов интернета является важным вопросом для каждого общества, есть необходимость выработки правовых инструментов. Государственное регулирование политики 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, регулирующее 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 пытаются ввести подобные правила и в киберпространство. Ключевым правовым инструментом, регулирующим вопросы содержания материалов интернета, является Дополнительный протокол к Конвенции по киберпреступности Совета Европы. Протокол описывает, какие виды нетерпимых высказываний должны был запрещены в интернете (расистские материалы, материалы, проповедующие геноцид, ксенофобию и преступления против человечности).

Особенно активно в этой области работает ОБСЕ. В июне 2003 г. заседание ОБСЕ, посвященное свободе СМИ и интернета, приняло так называемые Амстердамские рекомендации о свободе СМИ и интернета. Эти рекомендации направлены на защиту свободы слова и направлены на ограничение цензуры в интернете. В июне 2004 г. ОБСЕ организовала конференцию, посвященную взаимосвязи между пропагандой расизма, ксенофобии и антисемитизма в интернете и преступлениями на почве нетерпимости. На ней обсуждались возможности злоупотребления интернетом и свободой слова. Эти мероприятия ОБСЕ привлекли внимание академических и политических кругов к двум названным аспектам контроля над материалами.

Евросоюз выдвинул несколько инициатив в контексте контроля над материалами интернета, приняв Рекомендации Европейской Комиссии против распространения расизма через интернет. Практическим шагом в этом направлении явилось принятие Европейским Союзом Плана действий для обеспечения 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;
- создание ПО и сервисов;
- популяризация знаний о безопасном использовании интернета.

ВОПРОСЫ

Контроль над материалами и свобода выражения

В сфере контроля над материалами обратной стороной медали является ограничение свободы выражения. 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. Нахождение правильного баланса между контро

лем над материалами и свободой слова является непростой задачей. Большая часть недавних споров в области управления интернетом, включая рассмотрение судебных дел и принятие законодательных актов Конгрессом США, была посвящена как раз поиску такого баланса.

Конгресс США склоняется к установлению более строго контроля над материалами интернета, в то время как Верховный суд стремится защитить Первую поправку к Конституции США. В качестве самого яркого примера можно упомянуть принятый в 1996 г. Конгрессом США Акт о пристойности коммуникаций[2], который был признан Верховным судом неконституционным и противоречащим Первой поправке.

Свобода выражения во многом определяет позицию США в международной полемике по вопросам управления интернетом. Так, хотя США и подписали Конвенцию о киберпреступности, они не могут подписать Дополнительный протокол к ней, посвященный нетерпимым высказываниям и контролю над материалами. Свобода выражения также рассматривалась в контексте дела Yahoo!. Это предел, последняя черта, которую США не перейдут в ходе международных переговоров.

«Незаконно в офлайне — незаконно в онлайне»

Дискуссия о содержании материалов интернета подходит к обсуждению разницы между реальным миром и «кибермиром». Законы, регламентирующие содержание распространяемых материалов, могут быть применены и в интернете. Этот факт часто подчеркивается в европейском контексте. 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 «кибер-подхода» к управлению интернетом, заключается в том, что количество (интенсивность коммуникации, количество сообщений) влияет на качество. То есть проблема нетерпимых высказываний состоит не в том, что от-

[2] Communications Decency Act

сутствуют соответствующие нормативные акты, а в том, что масштабы интернета придают этой правовой проблеме новые черты. Все большее число людей имеет доступ к противозаконным материалам, и поэтому обеспечить соблюдение существующих норм сложно. Следовательно, связанное с интернетом отличие заключается в первую очередь не в законах, а в том, как обеспечить их соблюдение.

Эффективность контроля над материалами интернета

При обсуждении политики в отношении материалов интернета одним из ключевых аргументов является то, что, благодаря своей децентрализованной природе интернет может обходить цензуру. Интернет включает в себя многие механизмы и технологии, позволяющие осуществлять эффективный контроль, однако с технической точки зрения механизмы контроля можно обойти. В тех странах, где контроль над материалами интернета ведется на государственном уровне, технически продвинутые пользователи сумели найти обходные пути. Тем не менее контроль над материалами не направлен на эту небольшую группу пользователей — целью его являются более широкие слои населения. У Л.Лессига есть лаконичное утверждение по этому поводу: «Регулирование не должно быть абсолютно эффективным для того, чтобы быть достаточно эффективным».

Кто несет ответственность за политику в отношении материалов?

Основными действующими лицами в области политики в отношении материалов интернета являются правительства. Они определяют, что подлежит контролю и каким образом контроль должен осуществляться. Некоторые группы пользователей, например родители, стремятся внедрить более эффективную политику контроля над материалами, чтобы обезопасить своих детей. Чтобы помочь родителям отфильтровывать не подходящие для детей веб-страницы, созданы различные системы рейтингов. Политика в отношении материалов также осуществляется час-

тными компаниями и университетами для ограничения доступа к некоторым страницам. В других случаях содержание контролируется через пакеты ПО. Например, среди членов движения саентологов распространен пакет ПО Scienositter, который ограничивает доступ к сайтам, критикующим саентологию.

Одной из инновационных инициатив стало созданное в Великобритании Общество по надзору за интернетом[3], целью которого является борьба с жестоким обращением с детьми в интернете. Общество является многосторонней инициативой, в которой участвуют государство, провайдеры интернет-услуг и представители пользователей.

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, языковое разнообразие, и права меньшинств. В течение первого этапа саммита ВСИО многие группы гражданского общества предложили ввести концепцию права на общение, которое выходило бы за рамки существующих прав, связанных с интернетом. В данном разделе мы кратко рассмотрим те существующие права человека, которые не были описаны в других частях книги.

Свобода выражения убеждений и право искать, получать и распространять информацию

Это одно из основополагающих прав человека, которое обычно рассматривают в рамках обсуждения политики в отно-

[3] Internet Watch Foundation

шении материалов интернета и цензуры. В Декларации прав человека ООН свободе выражения убеждений 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 ст. 19 должны рассматриваться в контексте достижения должного баланса между двумя этими потребностями. Такой подход делает возможным неоднозначное толкование норм и их различное воплощение.

Право на частную жизнь

Данное право обсуждается в рамках правовой «корзины» (с. 87).

Право на интеллектуальную собственность

Это право дает человеку возможность защищать свои моральные и материальные интересы, являющиеся результатом научной, литературной и художественной деятельности. На другой чаше весов находится право каждого человека свободно принимать участие в культурной жизни и пользоваться научными достижениями. Поиск равновесия между двумя этими правами является одним из основных вопросов управления интернетом.

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. Такая ситуация побудила многие страны принять согласованные меры с целью поддержания многоязычия и защиты

культурного разнообразия. Задача поддержания многоязычия связана не только с сохранением культуры, но и с перспективами дальнейшего развития интернета. Чтобы интернетом могли пользоваться более широкие слои населения, а не только элита, материалы должны быть доступны на различных языках.

ВОПРОСЫ

Прежде всего развитие многоязычия требует наличия технических стандартов, позволяющих использовать иные, чем латиница, алфавиты. Одной из первых инициатив, связанных с многоязычным использованием компьютеров, стал стандарт Юникод[4]. Консорциум Юникод — это некоммерческая организация, разрабатывающая стандарты с целью облегчения использования букв различных алфавитов. Недавно ИКАНН и РГПИ предприняли важные меры, направленные на продвижение международных доменных имен на китайском, арабском и других языках, использующих иные, чем латинский алфавит, системы письма.

Неоднократно предпринимались попытки улучшить машинный перевод. Поскольку в Евросоюзе существует правило, по которому необходимо переводить официальные документы на языки всех государств-членов, ЕС оказывал поддержку различным проектам, направленным на усовершенствование машинного перевода. Несмотря на несомненные успехи, в этой области остается много ограничений.

Развитие многоязычия требует создания соответствующих рамок регулирования. Важным участником режимов управления является ЮНЕСКО. По ее инициативе были начаты многие проекты по развитию многоязычия, приняты важные документы, в частности Всеобщая декларация по культурному разнообразию. Другой структурой, способствующей развитию многоязычия, является ЕС, провозгласивший многоязычие одним из своих главных политических и рабочих принципов.

[4] Unicode Consortium

ГЛОБАЛЬНЫЕ ОБЩЕСТВЕННЫЕ БЛАГА

Концепция глобальных общественных благ связана со многими аспектами управления интернетом. В непосредственной взаимосвязи находятся такие аспекты, 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 гармоничное сочетание 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.

Среди основных особенностей интернета — создание новых знаний и информации в результате взаимодействия пользователей по всему миру. Значительный объем знаний был получен через обмен электронными сообщениями, форумы и блоги (онлайн-дневники). Во многих случаях подобные знания не защищаются какими-либо международными правовыми механизмами. Если эти знания оставить в правовом вакууме, они могут превратиться в товар, предмет продажи. Этот общий фонд знаний, важная основа для творческой деятельности, может быть исчерпан. Чем больше интернет становится источником прибыли, тем сложнее становится осуществлять свободный обмен информацией. Это может привести к сокращению творческого взаимодействия. Концепция глобального общественного блага может предоставить решения, способные сохранить этот кладезь знаний для будущих поколений.

Что же касается стандартов, то предпринимаются многочисленные попытки для того, чтобы заменить общественные стандарты частными и проприетарными. Так было с компаниями Microsoft (посредством браузеров и ASP) и Sun Microsystems (через Java). Стандарты интернета (главным образом TCP/IP) считаются открытыми и общественными. Режим управления интернетом должен обеспечить защиту основных стандартов интернета как глобальных общественных благ.

Защита интернета как глобального общественного блага

Некоторые решения, основанные на идее интернета как глобального общественного блага, 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 неисключаемость. 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.

На глобальном уровне Программа развития ООН ввела концепцию глобального общественного блага. В международном праве возможным решением является концепция *res communis omnium* (пространства как общего наследия человечества, которое регулируется и пополняется всеми странами).

Важно определить, какая из этих концепций может применяться к интернету и с какими последствиями. Многие согласны с тем, что модель будущего развития интернета будет зависеть от нахождения правильного равновесия между частными и общественными интересами.

ОБРАЗОВАНИЕ

Интернет открыл новые возможности для образования. Появились 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 для обучения 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. долл. США.

Электронное образование также стимулирует интенсивное развитие международных образовательных программ, когда студенты и преподаватели находятся в разных странах. Этот факт делает необходимым международное регулирование образовательного сектора.

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.

ВТО и образование

Одним из противоречивых аспектов переговоров в рамках ВТО является интерпретация статей 1(3) (b) и (c) Генераль-

ного соглашения по торговле услугами (ГАТС), которое предусматривает исключения из режима свободной торговли для услуг, предоставляемых государством. В соответствии с одной точкой зрения, поддерживаемой в основном США и Великобританией, эти исключения должны восприниматься в узком смысле, и де факто в области высшего образования должна осуществляться свободная торговля. Эта точка зрения продиктована главным образом заинтересованностью образовательного сектора США и Великобритании в появлении глобального рынка образования, и вызывает много возражений у других стран.

Главный аргумент против приведенной позиции состоит в том, что университеты предоставляют общественные блага и выполняют в каждой стране важные социальную и культурную функции, выходящие за рамки простой передачи знаний и информации. В соответствии с этой точкой зрения свободный мировой рынок образования может подвергнуть опасности университеты маленьких и развивающихся стран и привести к доминированию образовательных учреждений США и Великобритании, заметно сократив культурное разнообразие и лишив многие общества университетов, играющих роль катализаторов развития национальной культуры. Другим аргументом против свободной торговли в области образования является ее потенциальная несовместимость с осуществлением права на образование.

Дискуссии, которые еще возникнут в рамках ВТО и других международных организаций, вероятно, будут вестись на тему сущности образования: является ли оно товаром или общественным благом? Если рассматривать образование как товар, то правила ВТО, касающиеся свободной торговли, будут применимы 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. Исход этой дискуссии окажет значительное влияние на развитие онлайн-образования.

Обеспечение качества

Доступность инструментов, необходимых для предоставления услуг в области электронного образования, и легкость доступа на этот рынок ставят целый ряд вопросов, связанных с контролем качества. Сосредоточенность на предоставлении материалов онлайн может привести к пренебрежению качеством учебных материалов и дидактических методов. 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.

Дискуссии о транснациональном обучении вообще и электронном обучении в частности начались и на международном уровне. Одной из первых комплексных попыток обеспечения качества межгосударственных образовательных программ стала инициатива «Кодекс добросовестной практики в предоставлении транснационального образования»[5].

Признание академических степеней и создание общей системы зачетных единиц

Вопрос о признании степеней с расширением возможностей онлайн-обучения получил особую значимость. Основной задачей здесь выступает обеспечение признания дипломов и степеней за пределами региона, в первую очередь на глобальном уровне.

Всеобщая тенденция к повышению мобильности студентов, получающих высшее образование, позволяет им учиться в нескольких университетах. Евросоюз достиг определенных успехов на этой стезе, в частности при помощи программы

[5] Code of Good Practice in the Provision of Transnational Education

«Сократ» (Socrates). Мобильность студентов делает необходимой систему зачета образовательных единиц (кредитов), полученных ими в других вузах. На региональном уровне началось создание соответствующих нормативных рамок. ЕС начал разработку такой нормативной базы в контексте Европейской системы взаимозачета кредитов[6]. Азиатско-Тихоокеанский регион следует примеру Европы, создавая свою собственную региональную модель для обмена студентами и систему зачетных единиц (UCTS).

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.

Первый стандарт обучения — AICC[7]— был создан Ассоциацией авиационной промышленности для обеспечения совместимости электронных обучающих пакетов. Следующим значительным достижением стало создание IMS[8]— системы, которая ввела ряд стандартов для онлайн-обучения, включая спецификации метаданных, которыми могли бы пользоваться электронные образовательные курсы (описание содержания, название курса, авторы, стоимость обучения, система обучения и т. д.). IMS основана на стандарте XML. Кроме того, стандартизация ведется Комитетом по стандартам обучающих технологий[9] при Институте инженеров по электротехнике и электронике (IEEE).

Министерство обороны США также ведет активные разработки в области дистанционного образования, последний цикл которых начался в 1997 г. Столкнувшись с ограничен-

[6] European Credit Transfer System, ECTS
[7] Aviation Industry CBT Committee Комитет по компьютерному обучению в авиационной промышленности
[8] Instructional Management System Система управления обучением
[9] Learning Technology Standards Committee, LTSC

ностью существующих стандартов, министерство запустило проект «Передовое распределенное обучение»[10], в результате чего был создан новый стандарт SCORM[11]. SCORM является наиболее разработанным и получившим широкое признание стандартом для электронных курсов. Одной из причин его успеха является тот факт, что он стал стандартом курсов, проводящихся для Министерства обороны США (затраты на которые составляют 700 млн. долл. в год), а также для других правительственных ведомств США. SCORM приобретает все большую международную известность и популярность.

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

[10] Advanced Distributed Learning
[11] Shareable Content Object Reference Model —Модель описания разделяемых объектов контента (англ.)

ЧАСТЬ 7

Приложения

ПРИЛОЖЕНИЕ 1

СЛЕПЦЫ И СЛОН

Шесть мудрецов из Индостана,
Любовь к познанию питая,
Отправились к слону
(хоть были все слепыми),
Чтобы свои теории проверить.

Один лицом уткнулся
В шершавый бок слона
И, падая, воскликнул:
«О, Господи, меня ты вразумил,
Воистину, слон – прочная стена!»

Второй, нащупав бивень, закричал:
«Мне совершенно ясно!
Чудесный слон в моей руке –
Не что иное
Как гладкое и острое копье!»

А третий, подойдя к слону,
За хобот ухватился,
Отбросил в сторону:
И молвил: «Несомненно,
Слон и змея – одно и тоже»

Четвертый, подбежал к слону,
Колено, руками обхватив,
Сказал: «Ну что тут спорить,
Таким прямым и ровным
Быть может только дерево.»

Тут пятый, он сумел до уха
Допрыгуть, закричал:
«Любой слепец вам скажет –
Нет никаких сомнений:
На веер слон похож.»

Шестой неспешно
Добрался до хвоста
И вымолвил:
«Веревка, да и только.
Не может слон
Быть чем-нибудь еще.»

Так мудрецы из Индостана
В горячих спорах
Стояли твердо на своем.
Был каждый в чем-то прав,
Но ошибались все.

Мораль

Так часто в спорах люди,
истину свою
Пытаясь доказать,
не слушают друг друга.
И притча о слоне –
Лишь небольшой пример
Всеобщего непониманья.

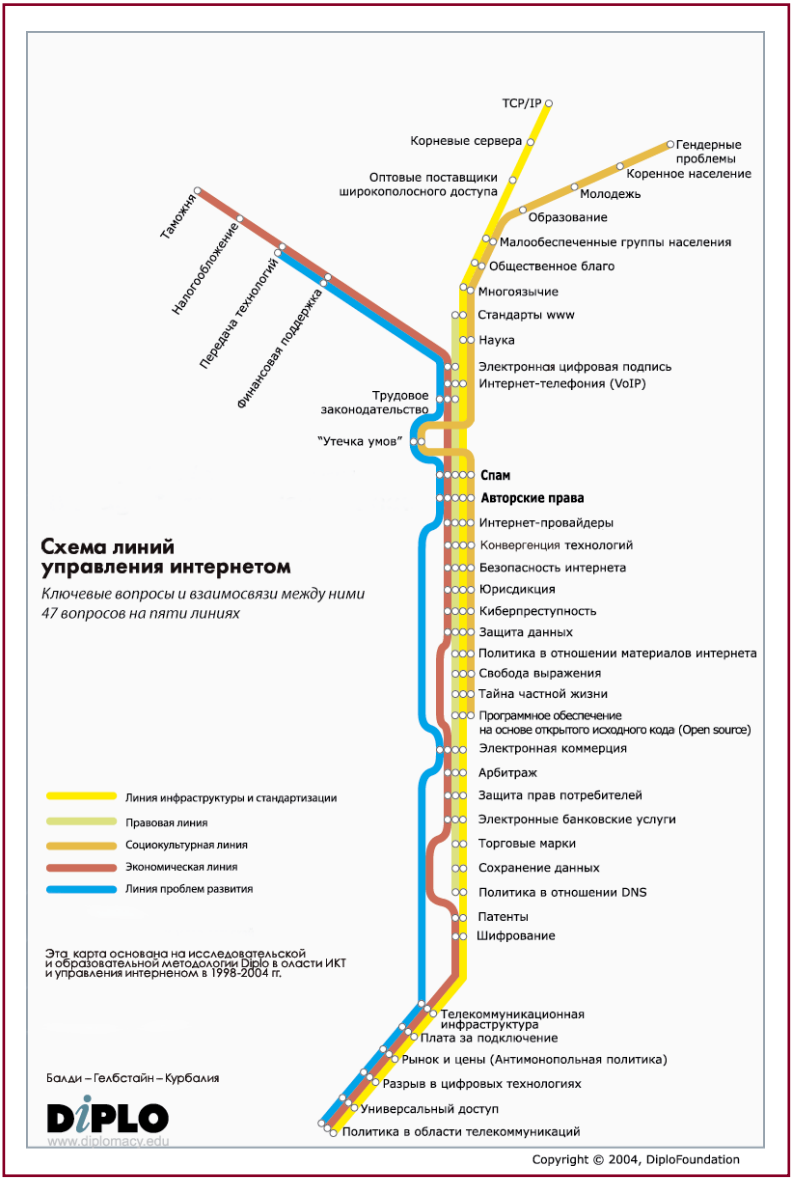
Джон Годфри Сакс (1816–1887)
Вольный перевод Валерия Земских

ПРИЛОЖЕНИЕ II. ОБЗОР ЭВОЛЮЦИИ УПРАВЛЕНИЯ ИНТЕРНЕТОМ

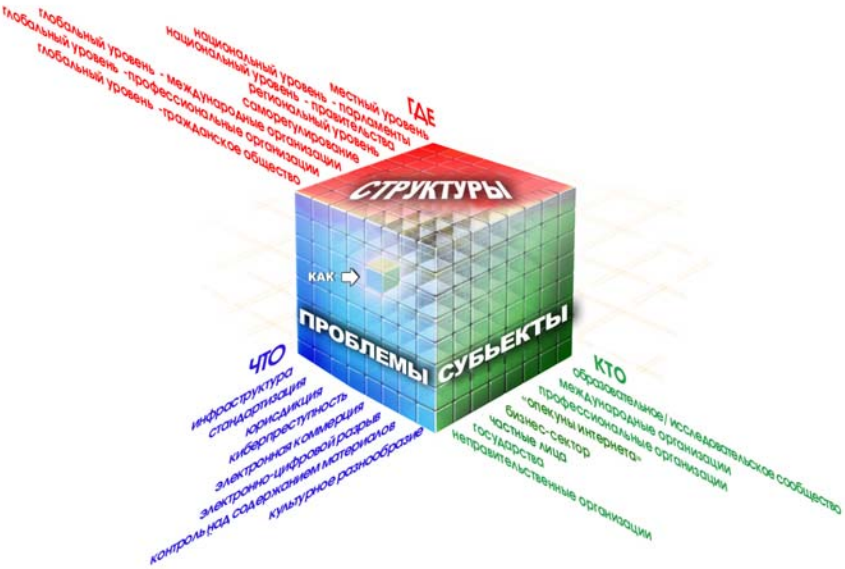
Действующее лицо / Период	США	«Опекуны» интернета	Международные организации	Частный сектор	Государства	Гражданское общество
	Министерство обороны управляет системой DNS.					
1986 г.	Национальный фонд науки (НФН) принимает управление структурами интернета от Минобороны.					
1994 г.				Компания NSI подписывает 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 г		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 г		Предложение о создании Международного специального комитета (МСК — International Ad Hoc Committee). Участники МСК: по 2 представителя от групп интересов (в сфере защиты торговых марок), ВОИС, МСЭ и НФН; и 5 представителей от РГПИ. Подписание меморандума о взаимопонимании по родовым доменам верхнего уровня (рДВУ), 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				
1997	Правительство США передает управление DNS Министерству торговли.					

июнь 1998 г.	«Белая книга» Министерство 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 г.		Сентябрь 1998 г. — Предварительное соглашение между ISOC и NSI. Октябрь 1998 г. — ISOC выходит из соглашения и создает ИКАНН.				
15 ноября 1998 г.	Министерство торговли передает полномочия ИКАНН.	ИКАНН получает две новые важные функции: - право давать аккредитацию регистраторам рДВУ; - управление на основе авторитета (политический аспект по-прежнему контролируется Министерством торговли США).				
апрель 1999 г.		Соглашение Министерства торговли США, ИКАНН и NSI о внедрение «системы регистрации общего пользования» (shared registry system). NSI теряет монополию, но получает благоприятные условия на переходный период (управление четырьмя доменами).				
июнь 1998 г.		Создание Организации поддержки протоколов (Protocol Supporting Organization), включающей в себя РПТИ, W3C и других «пионеров» интернета.	В рамках ВОИС начат «процесс доменных имен интернета».	Создана Организация поддержки доменных имен (Domain Name Supporting Organization) — для защиты торговых марок и коммерческих интересов. Создана Организация поддержки адресов (Address Support Organization) — чтобы представлять ассоциацию регистраторов DNS (ARIN, RIPE, NCC).	30 стран создают Правительственный консультативный комитет (Government Advisory Committee), чтобы получить больше влияния на управление национальными доменами. ИКАНН в ответ создает подкомитет по скДВУ.	
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 «олекунов». Однако в отношении позиций государств и интернет-сообщества в целом это далеко не так. Это два наиболее слабых аспекта системы управления ИКАНН.						
2000—2003 гг.			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.	Непровительственные 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			

ПРИЛОЖЕНИЕ III



ПРИЛОЖЕНИЕ IV
«КУБ УПРАВЛЕНИЯ ИНТЕРНЕТОМ»
(разработан DiploFoundation)



Ось «ЧТО» связана с вопросом, рассматриваемым 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 (например, 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 АВТОРАХ

Йован Курбалийя

Йован Курбалийя является директором-основателем фонда DiploFoundation. Он бывший профессиональный дипломат, имеющий опыт работы и исследований в области права, дипломатии и информационных технологий. С конца 1980-х гг. занимается исследованиями в области права и информационных технологий. В 1992 г. руководил созданием первого Отдела ИТ и дипломатии в Средиземноморской академии дипломатических исследований на Мальте. После десяти лет успешной работы в сфере преподавания, исследований и публикаций, в 2003 г. Отдел превратился в фонд DiploFoundation.

Йован Курбалийя руководит обучающими онлайн-курсами по информационным технологиям и дипломатии, читает лекции в исследовательских и образовательных учреждениях США, Австрии, Великобритании, Нидерландов и Мальты. Он также был членом Рабочей группы по управлению интернетом ООН.

Основные области его исследований: дипломатия и создание международного режима интернета, использование гипертекста в дипломатии, ведение переговоров в режиме онлайн и дипломатическое право.

jovank@diplomacy.edu

Эд Гелбстайн

Эдуардо Гелбстайн — старший научный сотрудник Института обучения и исследований при ООН (ЮНИТАР), сотрудник группы проектирования информационных технологий при ООН. Также он принимает участие в подготовке Всемирного саммита по информационному обществу. Эд Гелбстайн — бывший директор Международного вычислительного центра ООН.

Помимо работы в ООН Эд Гелбстайн выступает на конференциях и читает лекции в университетах, опираясь на свой сорокалетний опыт управления информационными технологиями.

Он работал в Аргентине, Нидерландах, Великобритании, Австралии и, в рамках сотрудничества с ООН в 1993 г., — в Женеве и в Нью-Йорке. Закончил университет Буэнос-Айреса по специальности «инженер по электронике» в 1963 г., а также получил степень магистра в Нидерландах и степень доктора в Великобритании.

gelbstein@diplomacy.edu

БИБЛИОТЕКА ИНФОРМАЦИОННОГО ОБЩЕСТВА

Сегодня нет недостатка в книгах по различным вопросам, связанным с управлением информацией и информационными технологиями. Настоящая брошюра призвана пополнить эту обширную коллекцию, и перед ней ставится несколько целей:

- дать читателям-неспециалистам представление о некоторых важных и относительно устойчивых общих принципах;
- представить материал в контексте, связанном с деятельностью в области международных отношений;
- заинтересовать читателей, побудить их прочесть другие книги, подробнее изучить затронутые вопросы, поэкспериментировать и таким образом расширить их знания.

Эти брошюры созданы по результатам курсов, проведенных авторами в последние несколько лет для различных аудиторий, и взаимодействия со студентами. Авторы с благодарностью примут отзывы читателей, которые помогут улучшить следующие издания этих брошюр.

ДРУГИЕ ИЗДАНИЯ СЕРИИ «БИБЛИОТЕКА ИНФОРМАЦИОННОГО ОБЩЕСТВА»

Internet Basics – FAQs, Facts and FFPs (Frequently Found Problems)
Finding Information in Cyberspace – From irritation to inspiration
Good Hygiene for Data and Personal Computers – Why and how to protect Data and personal computers
Appropriate Use – Guidelines and best practices for e-mail and other Internet services
Information Security and Organisations – A non-technical guide to players, offences and effective defences
Hacktivism, Cyber-terrorism and Cyberwar – The activities of the uncivil society in cyberspace
Online Learning for Professionals in Full Time Work – A guide to what works and what does not
Yellow Pages for the Information Society Library – A directory of recommended URLs

СЕРИЯ «ЗНАНИЯ ДЛЯ РАЗВИТИЯ»

Эта публикация является частью серии «Знания для развития» Глобального партнерства во имя знания (Global Knowledge Partnership), цель которой — расширение границ доступа к информации и знаниям по различным вопросам в области использования потенциала информационно-коммуникационных технологий для развития (ИКТР).

ДРУГИЕ ИЗДАНИЯ СЕРИИ «ЗНАНИЯ ДЛЯ РАЗВИТИЯ»:

Media and the Information Society
Multi-Stakeholder Partnerships
ICT for Development Success Stories
ICT for Poverty Reduction in Asia

DiploFoundation и Глобальное партнерство во имя знания (Global Knowledge Partnership) в сотрудничестве с Центром интернет-политики Московского государственного института международных отношений (Университета) МИД России

www.diplomacy.edu

DiploFoundation — некоммерческая организация, деятельность которой направлена на то, чтобы помочь странам, в особенности тем, чьи ресурсы ограничены, принимать значимое участие в международных отношениях. Diplo выступает за активное участие в регулировании международных отношений различных заинтересованных сторон, включая международные организации, гражданское общество и других действующих лиц. Деятельность Diplo включает в себя образовательные и исследовательские программы, а также разработку информационных и коммуникационных технологий для дипломатической деятельности.

www.globalknowledge.org

Глобальное партнерство во имя знания (Global Knowledge Partnership) — всемирная сеть организаций, стремящихся использовать потенциал информационных и коммуникационных технлогий (ИКТ) в интересах равенства и устойчивого развития. Цель GKP — мир равных возможностей, где все люди могут получать доступ к знаниям и информации и использовать их для улучшения своей жизни. Партнерство позволяет обмениваться информацией, опытом и ресурсами с целью сокращения бедности и предоставления людям новых возможностей.

Центр интернет-политики МГИМО (У) — структурное подразделение Московского государственного института международных отношений (Университета) МИД России. Миссией Центра является обеспечение лидирующего положения МГИМО (У) среди российских вузов в области использования современных информационных технологий в гуманитарном образовании и общественных науках. Основными направлениями деятельности Центра являются:

- разработка и реализация интернет-проектов, связанных с деятельностью МГИМО (У) (создание и поддержание вебсайтов, организация информационных кампаний в интернете, информационная поддержка проводимых при участии МГИМО (У) мероприятий);
- проведение исследований в области влияния современных информационных технологий на политику, общество, образование;
- подготовка учебных курсов и публикаций, посвященных различным аспектам интернета, а также участие в реализации программ дистанционного образования МГИМО (У).

На сегодняшний день одним из основных проектов Центра является разработка и создание всероссийского научно-коммуникационного портала по международным отношениям и мировой политике **www.worldpolitics.ru**.