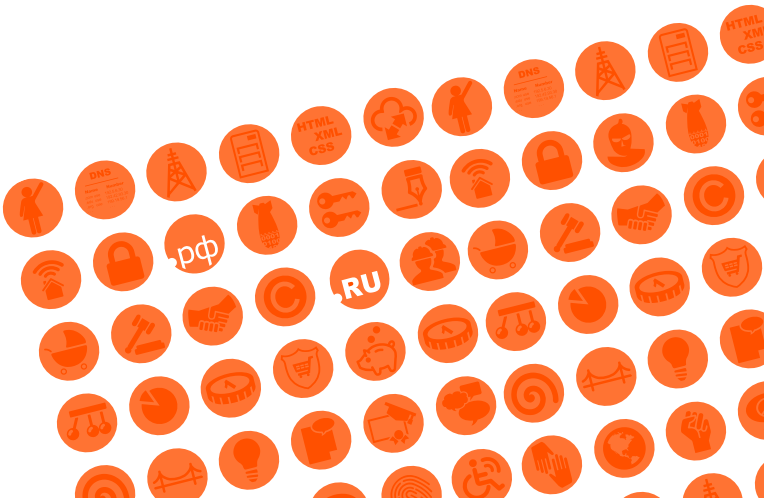
КООРДИНАЦИОННЫЙ ЦЕНТР ДОМЕНОВ .RU/.РФ

DiPLO

УПРАВЛЕНИЕ ИНТЕРНЕТОМ

Йован Курбалийя



Опубликовано DiploFoundation (2016)

Мальта: DiploFoundation
Anutruf, Ground Floor
Hriereb Street
Msida, MSD 1675, Malta

Швейцария: DiploFoundation
7bis, Avenue de la Paix
CH-1211 Geneva, Switzerland

Сербия: DiploCentar
Braničevska 12a/12
11000 Belgrade, Serbia

Эл. почта: diplo@diplomacy.edu
Сайт: www.diplomacy.edu

Иллюстрации: Др. Владимир Велясевич
Оформление, макет, допечатная подготовка: Ольга Стрелкова
Редактор: Ирина Пыжова

Перевод подготовлен по заказу Координационного центра доменов .RU/.РФ

Содержание

У этой книги достаточно долгая, по меркам Интернета, история. Первые тексты и общий подход, включая методологию «пяти корзин», были разработаны в 1997 г. при подготовке образовательного курса по политике в области информационно-коммуникационных технологий (ИКТ) для чиновников государственных ведомств стран Содружества. В 2004 г. Diplo впервые опубликовал печатную версию своих материалов по управлению Интернетом в форме книги «Управление Интернетом: проблемы, субъекты, преграды».

Эта книга, соавторами которой были Стефано Балди, Эдуардо Гелбстайн и Йован Курбалийя, стала частью «Библиотеки информационного общества», изданной Diplo. За 14 лет вышло уже семь изданий этой книги, и в каждом из изданий информация актуализируется, обновляется, добавляются новые факты, фиксируются события и тенденции. Книга переводилась на многие языки мира.

В России впервые книга увидела свет в 2010 году, ее выпуск был приурочен к проведению Первого российского форума по управлению Интернетом (RIGF 2010). Тогда было переведено третье издание книги, причем тираж дважды допечатывался — настолько она оказалась популярной. В 2018 году книга «Управление Интернетом» выходит на русском языке во второй раз — это уже седьмое издание бестселлера Diplo. Русская версия 3-го и 7-го изданий была подготовлена и выпущена Координационным центром доменов .RU/.РФ (www.cctld.ru).

Автор выражает благодарность команде кураторов из обсерватории GIP Digital Watch за их вклад в переработку ряда разделов издания 2016 г.: Радеку Беждаку, Стефани Борг Псаиле, Катарине Хене, Терезе Хорежсовой, Арвину Камбери, Аиде Махмутович, Адриане Минович, Вирджинии Пак, Роксане Раду, Владимиру Радуновичу, Барбаре Розен Якобсон и Сорине Телеану. Стефано Балди, Эдуардо Гелбстайн и Владимир Радунович очень помогли в разработке идей для иллюстраций этой книги. В тексте также приводятся ссылки на цитаты и предложения других коллег.

Предисловие автора

В 2004 году я вошел в состав Рабочей группы по вопросам управления Интернетом (Working Group on Internet Governance, WGIG), и мои друзья, полагая, что я занимаюсь вопросами, непосредственно связанными с компьютерами, постоянно обращались ко мне с просьбами помочь наладить принтер или установить новую программу. Помню, я провел экспресс-опрос своих коллег по WGIG, чтобы выяснить, как они объясняют, чем именно они занимаются, своим друзьям, детям и партнерам. Оказалось, что и они сталкивались с немалыми трудностями. Это и подтолкнуло меня к написанию книги, первого иллюстрированного пособия фонда Diplo по вопросам управления Интернетом.

Прошло более 10 лет. И сегодня тех, кто когда-то обращался ко мне по поводу принтеров, интересуют другие вопросы: как сохранить контроль над данными в Facebook или обеспечить безопасность детей в Интернете, как избежать кибервойн или обезопасить объекты критической инфраструктуры.

Конечно, вопрос управления Интернетом более актуален для тех, кто глубоко интегрирован в мир сетевых технологий, будь то посредством интернет-предпринимательства или просто используя Facebook для общения. Но управление Интернетом касается не узкого круга людей, а всех нас, хотя и в разной степени, включая 3,6 млрд. интернет-пользователей и получателей услуг в учреждениях, использующих Интернет.

Осуществляя этот проект, я ставил своей целью внести посильный вклад в борьбу за сохранение Интернета как важнейшего фактора, способствующего деятельности миллиардов людей. Надеюсь, что книга окажется познавательной и послужит стимулом для углубления знаний в этом замечательном и постоянно меняющемся предмете. Оставайтесь в курсе последних событий. Следите за новостями на сайтах http://www.diplomacy.edu/capacity/IG и http://www.diplomacy.edu/ig.

Йован Курбалийя
Директор фонда DiploFoundation
Глава Geneva Internet Platform
Ноябрь 2016

Предисловие директора Координационного центра доменов .RU/.РФ

Книга «Управление интернетом» Йована Курбалийи у себя на родине пережила уже семь изданий. На русском языке она впервые была издана в 2010 году Координационным центром доменов .RU/.РФ, и сразу же стала де-факто главным источником знаний по этой достаточно новой и непростой теме.

Восемь лет для интернета — огромный срок, за это время глобальная сеть изменилась до неузнаваемости. Появились новые игроки на рынке, новые технические стандарты, активно развивалась инфраструктура Интернета. Заметно изменилось законодательство, регулирующее Интернет во всем мире — гораздо больше внимания стало уделяться вопросам сохранности персональных данных и авторских прав на цифровые объекты, цифрового суверенитета, сетевой нейтральности. В ответ на это пышным цветом расцвели системы анонимизации и шифрования трафика, набрала популярность криптовалюта. Заметная часть всей информации в сети предназначена даже не для людей — количество подключенных автономных устройств уже в ближайшие несколько лет в разы превысит число живых пользователей.

Все эти явления еще потребуют своего описания, однако уже сейчас понятно, что сложившиеся модели управления Интернетом требуется дополнять и развивать. Новая книга Йована Курбалийи доступно рассказывает обо всем многообразии существующих подходов к управлению Интернетом, о том, каким образом в современном мире учитываются мнения различных заинтересованных сторон, и какова в этом роль основных мировых игроков. Эта книга — пожалуй, самое полное описание тех процессов, которые происходят в современном Интернете.

Мы уверены, что благодаря легкому языку и системному изложению эта книга станет хорошим подспорьем как тем, кто только знакомится с процессом управления глобальной сетью, так и тем, кто уже давно занимается развитием глобальной сети как в России, так и за ее пределами.

Андрей Воробьев
Директор Координационного центра доменов .RU/.РФ
Август 2018

Раздел 1

ВВЕДЕНИЕ

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

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

ВВЕДЕНИЕ

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

Что означает термин «Управление Интернетом»?

В рамках Всемирной встречи на высшем уровне по вопросам информационного общества (World Summit on the Information Society — WSIS)[1] было предложено следующее определение термина «управление Интернетом»:

> *Управление Интернетом представляет собой разработку и применение правительствами, частным сектором и гражданским обществом, при выполнении ими своей соответствующей роли, общих принципов, норм, правил, процедур принятия решений и программ, регулирующих эволюцию и применение Интернета»[2].*

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

Еще в 2003 г. журнал The Economist впервые напечатал слово «Интернет» с маленькой буквы. Другие издания вскоре также взяли на вооружение такой подход, включая Associated Press и The New York Times. Подобная редакционная политика явилась отражением того факта, что Интернет стал частью повседневной жизни, перестал быть чем-то уникальным и особенным, нуждающимся в написании с большой буквы. Таким образом, с точки зрения лингвистики, слово «Интернет» постигла та же участь, что и многие другие изобретения, такие как (т)елеграф, (т)елефон, (р)адио и (т)елевидение.

Вопрос о написании Интернета/интернета со строчной или прописной буквы обсуждался в ходе конференции Международного союза электросвязи (МСЭ) в Анталье в ноябре 2006 г. Вопрос приобрел политическое измерение, когда в резолюции МСЭ по вопросам управления Интернетом появилось слово «Интернет», начинающееся, в отличие от традиционного написания, со строчной буквы. Дэвид Гросс, посол США и Координатор по вопросам международных коммуникаций и информационной политики, выразил озабоченность по поводу того, что использование МСЭ строчной буквы может свидетельствовать о намерении организации рассматривать Интернет в одном ряду с другими телекоммуникационными системами, регулируемыми на международном уровне в рамках МСЭ. Некоторыми это было интерпретировано как дипломатический сигнал, отражающий стремление МСЭ играть более значимую роль в управлении Интернетом[3].

Однако это определение представляется достаточно широким и не позволяет решить проблему различных интерпретаций двух ключевых терминов: «Интернет» и «управление».

Интернет

Понятие «Интернет» не охватывает все существующие аспекты развития цифровых технологий. Обычно в качестве более полных предлагаются

два других термина: «информационное общество» и «информационно-коммуникационные технологии» (ИКТ). Эти понятия включают в себя сферы, выходящие за пределы непосредственно Интернета — такие как мобильная связь. Однако в пользу употребления термина «Интернет» свидетельствует стремительный переход глобальных коммуникаций к использованию протоколов передачи данных Интернета как основного технического стандарта. И без того вездесущий Интернет продолжает стремительно расти не только с точки зрения количества пользователей, но и с точки зрения спектра предлагаемых услуг, среди которых предоставление видеоуслуг через Интернет (OTT), включая протокол передачи голоса по Интернету (VoIP) и IP-телевидение (IPTV), которые все больше теснят обычную телефонную связь и телевидение.

Управление

В дискуссиях по проблемам управления Интернетом предметом противоречий стал термин «управление» и его различные интерпретации. В соответствии с одной из интерпретаций управление является синонимом правительства. На первых Всемирных встречах на высшем уровне по вопросам информационного общества (WSIS, World Summit of the Information Society) представители многих государств изначально вкладывали в это понятие такой смысл и полагали, что Интернет должен регулироваться государствами на межправительственной основе с ограниченным участием других, в основном негосударственных, субъектов.

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

Подобному толкованию противостояло иное, более широкое понимание термина «управление», которое предполагает регулирование деятельности различных институтов, в том числе негосударственных. Именно такой трактовки придерживались члены интернет-сообщества, поскольку она наиболее соответствует особенностям регулирования Интернета с момента его создания.

Терминологическая путаница усугублялась различными переводами термина «управление» (governance, англ.) на другие языки. В испанском языке этот термин относится преимущественно к государственной деятельности или правительству (*gestión pública, gestión del sector público, función de gobierno*). Связь с государственной деятельностью и правительством также заметна во французском языке (*gestion des affaires publiques, efficacité de l'administration, qualité de l'administration, mode de gouvernement*). Похожая ситуация наблюдается и в португальском языке: налицо связь с государственным сектором и правительством (*gestão pública, administração pública*).

Эволюция управления Интернетом

Начальный период управления Интернетом (1970-е — 1994)

Начало созданию Интернета было положено в рамках правительственного проекта. В конце 1960-х годов правительство США финансировало развитие сети Арпанет (от англ. Advanced Research Projects Agency Network) с целью обмена цифровыми ресурсами между компьютерами. К середине 1970-х, когда был создан протокол TCP/IP, сеть превратилась в то, что сегодня называется Интернет.

Одним из ключевых принципов Интернета является его распределенная природа: пакеты данных могут передаваться в сети по различным маршрутам, обходя традиционные барьеры и механизмы контроля. Этому технологическому принципу соответствовал схожий подход к регулированию Интернета на ранних этапах: Рабочая группа по проектированию Интернета (IETF), созданная в 1986 г., управляла дальнейшим развитием Интернета, принимая решения на основе сотрудничества и консенсуса, с привлечением широкого круга участников. У Интернета не было центрального правительства,

централизованного планирования, «великой стратегии».

В результате популярным стало утверждение, что Интернет формирует уникальное пространство, альтернативное политической системе современного мира. Джон Перри Барлоу, автор знаменитой *Декларации независимости киберпространства*, обращается ко всем правительствам:

> *«[Интернет] по своей природе транснационален, к нему не применим принцип государственного суверенитета, и ваш [государственный] суверенитет на нас не распространяется. Мы должны сами принимать решения»*[4].

«Война DNS» (1994—1998)

Вскоре государства и бизнес осознали значимость глобальной сети, и децентрализованный подход к управлению Интернетом подвергся изменениям. В 1994 г. Национальный фонд науки США, управлявший ключевой инфраструктурой Интернета, принял решение передать управление системой доменных имен субподрядчику — частной компании Network Solutions Inc. (NSI), зарегистрированной в США. Интернет-сообщество негативно отреагировало на этот шаг, что привело к так называемой войне DNS.

«Война DNS» вовлекла в процесс регулирования Интернета новых участников: международные организации и государства. Она закончилась в 1998 г. созданием новой организации — Корпорации по присвоению имен и адресов в Интернете (Internet Corporation for Assigned Names and Numbers, ICANN), которая стала выполнять функции координатора основных технических ресурсов Интернета, действуя на основании договора с правительством США. В последующих спорах по вопросу управления Интернетом ICANN отводилось центральное место.

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

Управление Интернетом стало частью дипломатической повестки в результате Всемирной встречи на высшем уровне по вопросам информационного общества (WSIS), которая прошла в два этапа в Женеве в 2003 г. и в Тунисе в 2005 г. Участники Женевского этапа WSIS, которому предшествовал ряд заседаний подготовительных комитетов и региональных встреч, предложили обсудить широкий круг вопросов, связанных с ИКТ. При этом в ходе первых подготовительных и региональных встреч термин «управление Интернетом» не использовался[5].

Управление Интернетом стало частью переговорного процесса в рамках WSIS в ходе Западноазиатской региональной встречи, прошедшей в феврале 2003 г., а по итогам Женевского этапа WSIS управление Интернетом стало ключевым вопросом саммита.

В результате длительных переговоров и соглашений, заключенных в последнюю минуту, участники встречи 2003 г. в Женеве приняли решение создать Рабочую группу по вопросам управления Интернетом (Working Group on Internet Governance, WGIG). WGIG подготовила отчет[6], послуживший основой для дальнейших переговоров в рамках второго этапа WSIS, прошедшего в Тунисе в ноябре 2005 г. В итоговом документе встречи —Тунисской программе для информационного общества — подробно рассматривается проблема управления Интернетом, включая принятое Рабочей группой определение этого понятия, список проблемных областей, а также решение о создании Форума по управлению Интернетом (Internet Governance Forum, IGF). Форум представляет собой многосторонний орган, созванный по решению Генерального секретаря ООН в целях обсуждения вопросов государственной политики, связанных с управлением Интернетом[7].

События 2006 г.

После завершения встречи в Тунисе предметом дискуссий по вопросам управления Интернетом в 2006 г. стали важнейшие три события. Во-первых, в этом году истек срок действия Меморандума о взаимопонимании между ICANN и Министерством торговли США, и был подписан новый документ. Надежды на то, что это событие изменит характер взаимоотношений между правительством США и ICANN, которая бы стала международной организацией нового типа, не оправдались. Новый вариант Меморандума лишь слегка ослабил связь между ICANN и правительством США, существовавшую

с момента основания организации, хотя и не исключил возможности интернационализации ICANN в будущем.

Вторым знаковым событием 2006 г. стал Форум по управлению Интернетом, прошедший в Афинах (Греция). Это был первый форум такого рода; во многих отношениях он представлял собой экспериментальный формат многосторонней дипломатии. Форум был по-настоящему многосторонним. Все действующие лица, вовлеченные в процесс регулирования Интернета — государства, компании, представители научно-технического сообщества и гражданского общества — участвовали в нем на равных условиях. Необычной была организационная структура основных мероприятий и семинаров в рамках Форума. Модераторами на всех прениях выступали журналисты, и, следовательно, Форум отличался от традиционных ооновских конференций. Однако некоторые критики заявили, что Форум — всего лишь «говорильня», не дающая реальных результатов в форме итоговых документов или планов действий.

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

События 2007 г.

В 2007 г. в ICANN шли дискуссии вокруг возможного создания домена «для взрослых» «.xxx». В результате возобновились дебаты и по многим другим вопросам управления Интернетом, включая сферу компетенции ICANN, а именно — должна ли ICANN заниматься исключительно техническим регулированием, или в ее компетенцию входят вопросы государственной политики[8]. Вмешательство со стороны США и других стран в отношении домена «.xxx» заострило вопрос об участии государств в работе ICANN.

В ходе второй встречи IGF в ноябре 2007 г. в Рио-де-Жанейро главным событием стало внесение в повестку Форума пункта о критически важных ресурсах Интернета (пространство имен и адресов).

События 2008 г.

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

В 2008 г. одним из важнейших вопросов управления Интернетом стала так называемая сетевая нейтральность[9]. Эти вопросы даже фигурировали в предвыборной кампании, причем Барак Обама выступал в поддержку принципа сетевой нейтральности.

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

Подробнее о сетевой нейтральности см. ***Раздел 2.***

События 2009 г.

В первой половине 2009 г. представители вашингтонской элиты пытались определить направления политики президента США Б. Обамы в отношении Интернета и оценить ее последствия. Назначения на ключевые

посты, связанные с регулированием Интернета, не принесли сюрпризов, подтвердив приверженность Обамы принципам открытости Интернета. В соответствии с обещаниями, данными в ходе предвыборной кампании, его команда приняла ряд мер в поддержку принципа сетевой нейтральности.

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

В ноябре 2009 г. в Шарм-эш-Шейхе (Египет) прошла четвертая встреча IGF. Главной темой мероприятия стало обсуждение будущего форума в свете намеченного на 2010 г. пересмотра мандата IGF. Мнения участников дискуссии разделились. Хотя большинство выступало за сохранение IGF, наметились глубокие расхождения в отношении будущей организации форума. Китай вместе со многими развивающимися странами выступал за интеграцию IGF в систему ООН, что повысило бы роль государств в регулировании Интернета. США, большинство развитых стран, представители делового сообщества и гражданского общества склонялись в пользу сохранения IGF в существующем виде.

События 2010 г.

В 2010 г. дискуссии по вопросу об управлении Интернетом во многом определялись стремительным развитием социальных сетей. В частности, в центре внимания оказалась проблема защиты неприкосновенности частной жизни пользователей такой социальной сети как Facebook. Главным событием 2010 г. в мире Интернета с точки зрения геополитики стала речь Государственного секретаря США Хилари Клинтон о свободе выражения мнений в Интернете, в частности, применительно к Китаю[10]. В то время между компанией Google и китайскими властями произошел конфликт в связи с ограничением доступа к поисковику Google в Китае. В итоге, компания

была вынуждена прекратить предоставлять услуги интернет-поиска китайским пользователям.

Этот год был отмечен двумя важными событиями для ICANN: (1) появлением первых доменов верхнего уровня с символами, не входящими в набор ASCII, на арабском и китайском языках (решив проблему с доступом к доменам верхнего уровня с символами, отличными от латинского алфавита, ICANN снизила риск фрагментации мировой системы доменных имен); (2) утверждением решения о создании домена .xxx («для взрослых»). Это решение оказалось судьбоносным для ICANN, поскольку впервые Корпорация приняла решение по вопросу, связанному с политикой управления Интернетом. До этого ICANN, по крайней мере формально, старалась ограничиваться в своей деятельности вопросами технического характера.

В 2010 г. в отношении IGF был запущен обзорный процесс после принятия Комиссией Организации Объединенных Наций по науке и технике в целях развития (КНТР ООН) резолюции о продолжении проведения Форума по управлению Интернетом в течение следующих пяти лет и внесении незначительных изменений в его организацию и структуру. В июле 2010 г. Экономический и социальный совет ООН (ЭКОСОС ООН) принял соответствующую резолюцию, на основании которой Генеральная Ассамблея ООН осенью того же года приняла окончательное решение о продолжении работы IGF.

События 2011 г.

В 2011 г. управление Интернетом стало одной из важнейших тем в глобальной политической повестке. Этот вопрос встал в один ряд с такими проблемами, как изменение климата, миграция и продовольственная безопасность. Растущее внимание политиков к управлению Интернетом привело к тому, что на национальном уровне эти вопросы, находившиеся в ведении министерств, специализирующихся на технических вопросах (информационные технологии, телекоммуникации) были переданы политическим органам (министерство иностранных дел, канцелярия премьер-министра). Кроме того, более серьезное внимание вопросу управления Интернетом стали уделять ведущие международные СМИ (например, The Economist, IHT, Al Jazeera, BBC).

События «арабской весны» оказали существенное влияние на дискуссии

по вопросу об управлении Интернетом. Мнения относительно влияния Интернета на движения «арабской весны» разнятся. Одни не придают Интернету особой роли в этих событиях, тогда как другие считают, что Интернет сыграл ключевую роль. Однако, в любом случае очевидно, что теперь социальные сети воспринимаются как инструмент, играющий решающую роль в современной политической жизни. В итоге, в 2011 г. Интернет и вопрос управления Интернетом оказались в центре внимания политиков по всему миру.

27 января власти Египта заблокировали доступ к Интернету, пытаясь тем самым добиться прекращения протестных выступлений. Это стало первым случаем полного отключения целой страны от сети по приказу правительства. До этого случаев полного отключения Интернета не было даже во время военных конфликтов (в странах бывшей Югославии, Ираке).

В 2011 г. ускорилась работа по реализации инициативы Хилари Клинтон о свободе выражения мнений в Интернете, с которой она выступила в феврале 2010 г. Этому вопросу были посвящены две крупные конференции: Конференция по правам человека и Интернету в Вене и Конференция о свободе Интернета в Гааге.

В 2011 г. ICANN продолжала свою обзорную деятельность, в том числе были проведены следующие мероприятия:

- реформа системы управления;
- завершение подготовки к созданию новых доменных имен верхнего уровня (gTLDs);
- поиск нового генерального директора.

В том же году целый ряд организаций и стран, включая Организацию экономического сотрудничества и развития (ОЭСР), Совет Европы, Европейский союз и Бразилию, представили на рассмотрение ряд новых принципов управления Интернетом, многие из которых были созвучны друг другу. Ожидалось, что эти идеи лягут в основу преамбулы к глобальной декларации об Интернете или аналогичного документа о развитии системы управления Интернетом.

События 2012 г.

В 2012 г. произошло два крупных события, последствия которых будут ощущаться на протяжении многих лет: в ICANN произошла смена руководства, а Международный союз электросвязи (МСЭ) принял новую версию *Регламента международной электросвязи* (РМЭ).

Создание в предыдущем году новых доменных имен верхнего уровня стало важнейшим событием в истории ICANN. Несмотря на некоторые трудности с регистрацией (сбои программного обеспечения, споры по политическим вопросам), были получены заявки на регистрацию более 1900 новых доменных имен верхнего уровня. Затем последовала процедура оценки с целью определения доменов, которые будут внесены в корневую систему в 2014 г. Кроме того, новый глава корпорации ICANN Фади Шехаде изменил подход к организации многостороннего процесса. На 45-й встрече он выступил перед представителями гражданского общества, отметив ряд важных изменений в ICANN, включая разработку ответственного подхода к многосторонней деятельности, необходимость честно признавать проблемы, прислушиваться к мнению других, быть чутким руководителем, искать компромисс и т. д.

В декабре 2012 г. в Дубае собралась Всемирная конференция по международной электросвязи (ВКМЭ). На повестке мероприятия было внесение изменений в РМЭ впервые с 1988 г. Эта тема находилась в центре внимания на протяжении всего года. По вопросу о влиянии нового регламента на будущее Интернета вспыхнул острый спор. Изнуряющая двухнедельная конференция не привела к результатам: переговоры зашли в тупик. Участники так и не смогли достичь консенсуса по новой версии регламента, и обсуждение этого вопроса было отложено до следующих встреч. Камнем преткновения стала рекомендательная резолюция о повышении роли МСЭ в управлении Интернетом, которая разделила участников на два лагеря: западные страны выступали за сложившуюся на тот момент многостороннюю систему, тогда как страны, поддержавшие резолюцию, включая Китай, Россию и арабские страны, предпочитали регулирование Интернета на межгосударственной основе.

Другие значимые события произошли в области регулирования прав интеллектуальной собственности. Благодаря мобилизации и протестам удалось воспрепятствовать введению правил, которые бы ограничивали законные права пользователей на национальном (законопроект США об интернет-пиратстве — SOPA) и международном уровнях (Международное соглашение по борьбе с контрафактной продукцией).

События 2013 г.

Основным событием на международной арене в сфере цифровых технологий стали разоблачения Э. Сноудена, обнародовавшего информацию о программах слежки Агентства национальной безопасности (АНБ) США и других организаций, которые привлекли внимание мировой общественности к вопросам управления Интернетом. В центре обсуждения оказались право на неприкосновенность частной жизни и защита информации.

Вопрос о защите частной жизни поднимался многими лидерами на Генеральной ассамблее ООН, которая приняла резолюцию о защите персональных данных в Интернете. Обсуждение этого вопроса продолжилось в 2014 г. в Совете по правам человека ООН (СПЧ ООН).

В октябре 2013 г. президент Бразилии Дилма Русеф и глава ICANN Фади Шехаде выступили инициаторами проведения глобальной многосторонней конференции NETmundial по вопросу о будущем управления Интернетом. Этой теме были посвящены многочисленные научные конференции и исследовательские проекты по всему миру.

События 2014 г.

В начале 2014 г. президент США Б. Обама произнес речь о программе Агентства национальной безопасности США по слежке за населением. В своем выступлении он неоднократно упоминал «кибератаки», отметив, что обеспечение кибербезопасности стало приоритетом с точки зрения безопасности и представляет даже большую угрозу, чем терроризм.

14 марта 2014 г. Национальное управление по телекоммуникациям и информации Министерства торговли США объявило о намерении передать свою координирующую роль в Администрации адресного пространства интернета (IANA) многосторонней организации. На тот момент Национальное управление по телекоммуникациям и информации контролировало деятельность Администрации адресного пространства интернета, в частности, вело реестр глобальных IP-адресов и доменных имен, а также контролировало ряд других критически важных параметров. Национальное управление по телекоммуникациям и информации также разрешило внести изменения

в файл корневой зоны (глобальный реестр интернет-адресов). За этим объявлением последовали длительные консультации и подготовка предложений. Изначально планировалось, что процесс завершится к сентябрю 2015 г., но впоследствии срок был продлен на год. Одновременно началась разработка механизмов подотчетности в рамках ICANN.

Появилось три форума для обсуждения вопросов управления Интернетом, два из которых были связаны с ICANN:

- По инициативе ICANN была создана интернет-площадка/1net для улучшения взаимодействия между различными субъектами и обмена информацией с другими форумами, в частности, NETmundial. Конференция NETmundial — Глобальная многосторонняя конференция о будущем управлении интернетом состоялась 23–24 апреля в Сан-Паулу, Бразилия, и была организована Управляющим комитетом Бразилии по обеспечению работы интернета (CGI.br) и /1Net. По итогам мероприятия было принято Многостороннее заявление NETmundial, в котором излагались принципы управления Интернетом, а также содержалась дорожная карта по развитию экосистемы управления Интернетом.
- Комиссия высокого уровня по вопросам глобального сотрудничества и управления Интернетом (GICGM) была создана ICANN в сотрудничестве с Всемирным экономическим форумом (WEF) при поддержке фонда The Annenberg Retreat at Sunnylands.
- Глобальная комиссия по вопросам управления Интернетом была создана Канадским центром инноваций в области управления и британским научно-аналитическим центром Chatham House с целью продвижения стратегического видения управления Интернетом в будущем.

3 мая Суд Европейского союза узаконил «право на забвение», обязав компанию Google на основании обращения физического лица удалять ссылки на «устаревшие», «чрезмерные» и «неактуальные» персональные данные по результатам поиска с упоминанием имени.

События 2015 г.

На протяжении года вопросы передачи полномочий IANA и подотчетности ICANN оставались в центре внимания в связи с продлением срока пода-

чи предложений до сентября 2016 г. В число основных тем года также входила кибербезопасность в связи со взломами систем безопасности и реакции на них со стороны политиков. Постановив в 2013 г., что существующие нормы международного права применимы к использованию ИКТ государствами, Группа правительственных экспертов (ГПЭ) ООН по международной информационной безопасности согласовала ряд норм, включая отказ от атак на объекты критической инфраструктуры и создание Компьютерной группы реагирования на чрезвычайные ситуации, а также помощи другим странам в расследовании кибератак и киберпреступлений.

В июле в рамке разработки целей устойчивого развития (ЦУР) в ООН был создан новый Механизм содействия развитию технологий[11], в который вошли межведомственная целевая группа ООН по науке, технике и инновациям, многосторонний форум и платформа по обработке данных. По итогам дискуссии в СПЧ ООН было согласовано создание специального механизма по защите права на неприкосновенность частной жизни. 3 июля был назначен первый Специальный докладчик по вопросу о праве на неприкосновенность частной жизни.

Летом 2015 г. началась подготовка Совещания высокого уровня WSIS+10 (ВВУИО+10). В декабре в рамках Генеральной ассамблеи ООН состоялось заседание высокого уровня по анализу исполнения решений WSIS. В итоговом документе говорилось о продлении полномочий IGF на 10 лет, и были изложены основные направления развития на этот срок с учетом полномочий и обязанностей заинтересованных сторон согласно Тунисской программе для информационного общества 2005 г.

Сообщество ICANN продолжило работать над предложениями по передаче координирующей роли в исполнении функций IANA и подотчетности ICANN.

События 2016 г.

В самом начале 2016 г. в свет вышли два доклада, посвященные одному основополагающему вопросу: Как максимально использовать возможности Интернета, минимизировав при этом сопутствующие риски? В *«Докладе Всемирного банка о мировом развитии 2016: Цифровые дивиденды»*[12] говорилось, что Интернет не приносит общественных благ сам по себе. Для этого требуется соответствующий политический курс, меры по развитию образования и другие действия. Другой доклад выпустил Всемирный экономический форум с призывом остерегаться фрагментации Интернета с указанием рисков для Интернета (фрагментация на техническом, государственном и коммерческом уровнях)[13].

В течение нескольких месяцев на протяжении 2016 г. с первых полос газет не сходило противостояние между компанией Apple и ФБР после того, как суд обязал Apple помочь ФБР взломать iPhone одного из террористов, причастного к убийству 15 декабря 2015 г. 14 человек в г. Сан-Бернардино (штат Калифорния). Извечная проблема необходимости обеспечения безопасности и соблюдения прав человека снова оказалась в центре внимания интернет-сообщества. Хотя в конечном счете ФБР отказалось от судебного преследования Apple (по утверждению американских властей, взломать телефон удалось при помощи стороннего специалиста), вопросы шифрования, неприкосновенности частной жизни и безопасности оставались в центре внимания на протяжении всего года.

В июне 2016 г. Глобальная комиссия по вопросам управления Интернетом опубликовала доклад «Единый Интернет» (*One Internet*), который содержит ряд рекомендаций для политиков, частного сектора, технологической отрасли и других заинтересованных сторон по вопросу о защите Интернета. В частности, в нем говорится о необходимости обеспечить открытость и безопасность Интернета и защиту прав человека в цифровом мире; определить обязанности частного сектора, создать условия для устойчивой и стабильной работы ключевой инфраструктуры и повышения эффективности управления Интернетом на многосторонней основе[14].

В первом полугодии 2016 г. ICANN представила властям США предложение по передаче координирующей роли IANA и подотчетности ICANN. Проанализировав оба предложения, Национальное управление по телекоммуникациям и информации в августе 2016 г. отметило их соответствие критериям, заявленным в марте 2014 г. Это позволило ICANN перейти к исполнению положений этих документов, в частности, создать общедоступные технические идентификаторы (Public Technical Identifiers — PTI) в составе ICANN для исполнения функций IANA и расширить полномочия сообщества ICANN за счет включения в нормативные документы ICANN ряда положений для обеспечения подотчетности сотрудников и руководства ICANN. 1 октя-

бря истек срок действия соглашения между правительством США и ICANN по вопросу об исполнении функций IANA, что ознаменовало переход координирующей роли IANA к глобальному интернет-сообществу.

«Электронный» («е-»), «виртуальный», «цифровой», «сетевой» и приставка «кибер»

Слова «электронный» («е-»), «виртуальный», «цифровой», «сетевой» и приставка «кибер» используются для описания различных аспектов работы ИКТ и Интернета. Они взаимозаменяемы. Каждое такое слово или приставка связаны с Интернетом.

Прилагательное «электронный», как правило, используется применительно к торговле, приставка «кибер» в контексте преступности и вопросов безопасности, прилагательное «цифровой» получило распространение в контексте дискуссий о «цифровом разрыве», а слово «виртуальный» ассоциируется с валютами, такими как биткойн. Таким образом, налицо формирование особенностей в использовании этих слов. В то время как в обиходе мы часто используем эти слова и приставки произвольно, при обсуждении вопросов политики в области Интернета выбор слов приобретает все большее значение.

Вкратце изучим этимологию этих терминов и то, как они используются применительно к теме регулирования Интернета.

По своей этимологии «кибер» восходит к древнегреческому слову «управлять». Это слово и приставка вошли в современный лексикон благодаря книге Норберта Винера «Кибернетика» об управлении с помощью информации[15]. В 1984 г. Уильям Гибсон впервые использовал термин «киберпространство» в научно-фантастическом романе «Нейромант»[16]. Популярность приставки «кибер» росла по мере развития Интернета. В конце 1990-х гг. почти все, что было связанно с Интернетом, имело приставку «кибер»: «киберсообщество», «киберправо», «киберсекс», «киберпреступность», «киберкультура» и так далее. Любому связанному с Интернетом предмету или аспекту предшествовала приставка «кибер». В начале 2000-х гг. приставка «кибер» утратила свою былую популярность, оставшись только в терминах, связанных с вопросами безопасности.

Совет Европы использовал приставку «кибер» в названии Конвенции о киберпреступности, принятой в 2001 г. До сих пор это единственный международный договор в области интернет-безопасности. Существует Стратегия США по киберпространству, Глобальная программа кибербезопасности МСЭ, Политика НАТО в области кибербезопасности, Центр кибероборонны в Эстонии...

Писатель в жанре киберпанк и автор колонки в журнале Wired Брюс Стерлинг объяснил это следующим образом:

> *Кажется, я знаю, почему военные используют приставку «кибер». Дело в том, что, используя метафору киберпространства как одного из театров военных действий, легче выбивать гранты у Пентагона. Если понимать «киберпространство» как совокупность «сетей, проводов, трубок и кабелей», то все это уже 50 лет находится в ведении Агентства национальной безопасности США, и военным туда путь заказан[17].*

Использование прилагательного «электронный» («е-») закрепилось в области электронной торговли на ранней стадии коммерциализации Интернета. В английской версии Лиссабонской стратегии 2000 г. «е-» стало наиболее часто встречающейся приставкой. То же самое относится к декларациям WSIS, подписанным в Женеве в 2003 г. и в Тунисе в 2005 г. Решения WSIS затрагивают такие области, как электронное правительство, электронная коммерция, электронное дистанционное обучение, электронное здравоохранение, электронная занятость, электронное сельское хозяйство и электронная наука. Однако сейчас прилагательное «электронный» и приставка «е-» (в англоязычных терминах) используются гораздо реже. Даже ЕС постепенно отказывается от его употребления.

В настоящее время в рамках ЕС ведется работа по реализации Стратегии единого цифрового рынка[18]. Термин «цифровой» относится к использованию нолей и единиц как основы всего мира Интернета. В конечном счете, все программы начинаются с нолей и единиц. Раньше это прилагательное употреблялось преимущественно в контексте дискуссий о «цифровом разрыве». Однако в последние несколько лет прилагательное «цифровой» стало завоевывать лингвистическое пространство Интернета. Все говорит о том, что именно это прилагательное станет основным в том, что касается Интернета. Председатель Европейской комиссии Жан-Клод

Юнкер десять раз произнес слово «цифровой» в своей первой речи в Европейском парламенте после вступления в должность, в которой он изложил свою программу на пятилетний период. Помимо ЕС, в Великобритании используется термин «цифровая дипломатия». Растет число дипломатических представительств, в которых есть сотрудник, отвечающий за цифровые технологии.

Прилагательное «виртуальный» отражает нематериальную сущность Интернета. Этот термин отражает как нематериальность сети, так и тот факт, что Интернет не существует в реальном мире. Аналогичным образом, виртуальную реальность можно понимать как нематериальную реальность (что нельзя потрогать), а также как несуществующую реальность (ложная реальность). Ученые и первопроходцы в области интернет-технологий использовали слово «виртуальный», чтобы подчеркнуть новаторский характер Интернета и становление «прекрасного нового мира». В силу противоречивости этого термина, в политическом дискурсе и международных документах прилагательное «виртуальный» практически не встречается.

На данный момент в «войне прилагательных» наступило перемирие. Каждое из них занимает свою нишу и не стремится к тотальному господству, как это было, например, в конце 1990-х гг. с приставкой «кибер», которая сейчас сохраняет ведущие позиции только по вопросам безопасности. В деловом мире продолжает преобладать прилагательное «электронный». Слово «цифровой» теперь не ограничивается вопросами развития и используется гораздо более широко в сфере государственного управления, тогда как от прилагательного «виртуальный» практически отказались.

Аналитический инструментарий управления Интернетом

Есть два вида истины — тривиальная, которую отрицать нелепо, и глубокая, для которой обратное утверждение — тоже глубокая истина.

Нильс Бор, физик-атомщик (1885—1962)

Аналитический инструментарий управления Интернетом — набор инструментов, предназначенных для выработки политического курса и понимания политической аргументации. Суть этого инструментария заключается в том, чтобы помочь понять причинно-следственные связи, модели мышления, ценности, терминологию и жаргон. Он служит основой для понимания конкретных вопросов и предпринимаемых действий.

Во многих случаях на становление системы взглядов влияет специфическая профессиональная культура (способы мышления и поведения, общие для представителей одной профессии, например, для дипломатов, ученых, программистов). Установление неких «общих рамок» обычно помогает улучшить коммуникацию и понимание. Однако порой они используются для защиты «территории» и препятствия влиянию извне. По словам американского лингвиста Джефри Майрела, «всякий профессиональный язык — это язык сферы влияния»[19].

Режим управления Интернетом сложен, поскольку включает множество вопросов, участников, механизмов, процедур и инструментов. На рис. 1, выполненном по мотивам работ голландского художника М.К. Эшера, показан разброс мнений, который существует по вопросам управления Интернетом.

Аналитический инструментарий управления Интернетом является воплощением самой сути этой области как «грязной» политической проблемы. Проблемы управления Интернетом, как правило, имеют множество катализаторов, поэтому выявить для каждой из них единственную причину чаще всего непросто. Во многих случаях одна проблема — это симптом другой, что иногда создает «порочный круг» политических решений. Некоторые методы познания, такие как линейное мышление, поиск единственной причины, подход «или-или», лишь отчасти применимы к проблемам управления Интернетом. Эта сфера слишком сложна, чтобы быть представленной в последовательной, непротиворечивой и логичной форме. Чтобы понять Интернет, необходимо проявить гибкость, открытость и быть готовым к непредвиденному[20].

Как и сам процесс управления Интернетом, этот инструментарий находится в постоянном изменении. Подходы, модели и аналогии появляются и исчезают в зависимости от их уместности и важности для процесса пе-

реговоров в данный момент. Они становятся частью дискурса по тому или другому аспекту дискуссий по вопросу об управлении Интернетом.

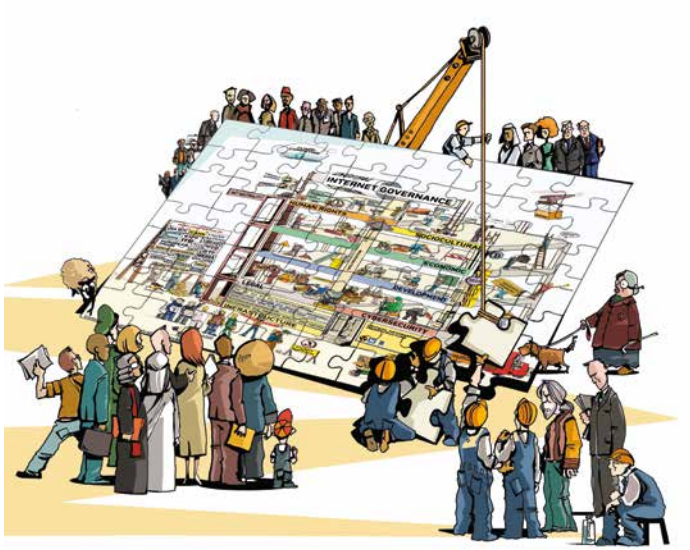


Рисунок 1. Управление Интернетом в виде составной картинки

Политические подходы

В первой части Аналитического инструментария управления Интернетом описывается ряд политических подходов, определяющих позиции основных субъектов управления Интернетом. Выявление этих политических подходов также позволяет определить переговорные позиции и форму политической дискуссии по этому вопросу.

«Широкий» или «узкий» подход

При «узком» подходе внимание сосредоточено в первую очередь на инфраструктуре Интернета (системе доменных имен, IP-адресов и «корневых» серверов) и на позиции ICANN как ключевого субъекта в этой области.

В соответствии с широким подходом переговоры по управлению Интернетом должны выходить за пределы вопросов инфраструктуры и обращаться к другим проблемам: правовым, экономическим, социокультурным, связанным с развитием. Широкий подход взят за основу в отчете Рабочей группы по вопросам управления Интернетом (WGIG) и «Тунисской программе для информационного общества». Он также используется как основополагающий принцип архитектуры Форума по управлению Интернетом.

В то же время наблюдается тенденция рассматривать кибербезопасность и электронную торговлю отдельно от темы управления Интернетом. Например, в обзорном документе Совещания высокого уровня WSIS+10 2015 г.[21] управлению Интернетом и проблеме кибербезопасности были посвящены отдельные главы. При этом определение рамок политической дискуссии по цифровым технологиям нельзя считать вопросом исключительно научным. Если рассматривать эти вопросы по отдельности (например, безопасность, права человека, электронную торговлю), это может сказаться на эффективности решения проблем, связанных с управлением Интернетом, которые, по сути, являются междисциплинарными. С проблемой отказа от «бункерного мышления» и необходимости решения вопросов управления Интернетом на основе междисциплинарного подхода сталкиваются многие субъекты, от правительств до международных организаций и частного сектора.

Согласованность политических и технических решений

В управлении Интернетом интеграция технических и политических вопросов является непростой задачей, поскольку провести четкую границу между ними сложно. Технические решения не нейтральны. В конечном счете, любое техническое решение способствует продвижению чьих-то интересов, усиливает позицию определенных групп и в известной степени влияет на общественную, политическую и экономическую жизнь. На раннем этапе развития Интернета и технические, и политические аспекты его функционирования долгое время регулировались лишь одной социальной группой — техническим сообществом периода становления Интернета.

С распространением Интернета и появлением новых субъектов в процессе управления Интернетом, в первую очередь представителей бизнеса и прави-

тельств, члены интернет-сообщества уже не могли удерживать «в одних руках» управление как технологическими, так и политическими вопросами. Последующие реформы, в том числе создание ICANN, ставили своей целью восстановление равновесия между техническими и политическими аспектами. Проблема нахождения такого равновесия еще не решена и остается одной из наиболее спорных при обсуждении вопросов управления Интернетом в будущем.

Старый «реальный» подход или новый «киберподход»

Практически любой вопрос в рамках управления Интернетом можно рассмотреть с двух разных сторон (рис. 2). Сторонники старого «реального» подхода доказывают, что Интернет не привнес ничего нового в сферу управления. По их мнению, Интернет, с точки зрения регулирования — еще одно техническое устройство, не отличающееся от предшественников: телеграфа, телефона или радио. Например, в дискуссиях по правовым вопросам сторонники этого подхода указывают, что существующие законы с небольшой корректировкой можно применить и к Интернету. В области экономики приверженцы этого подхода утверждают, что разницы между обычной и «электронной» коммерцией нет. Следовательно, нет необходимости специального правового регулирования электронной коммерции.

Рисунок 2. Парадигма управления Интернетом

Приверженцы нового «киберподхода» доказывают, что Интернет — принципиально новая система коммуникации по сравнению со всеми предшествующими.

Основной посыл «киберподхода» состоит в том, что Интернету удалось отделить современную социальную и политическую реальность от физического мира (географически разделенных) суверенных государств. Киберпространство отличается от реального мира, а потому требует иной формы управления. Подход, согласно которому киберпространство представляет новое, отличное от других пространство, закреплен в решении НАТО по итогам Саммита 2016 г. в Варшаве, которое провозглашает кибербезопасность четвертой оперативной областью наравне с землей, водой и воздухом[22].

В области права представители «киберподхода» утверждают, что существующие законы, касающиеся юрисдикции, киберпреступности и заключения контрактов, не могут применяться к Интернету, а потому должны быть созданы новые законы. Старый «реальный» подход находит все больше сторонников в сфере регулирования и политики. ГПЭ ООН заявила о том, что существующие нормы международного права применимы к использованию государствами ИКТ. Кроме того, принцип соблюдения принятых в реальном мире прав человека в интернет-пространстве закреплен в многочисленных конвенциях ООН по правам человека.

Децентрализованная или централизованная структура управления Интернетом

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

Сторонники же централизованного подхода выступают за управление Интернетом по принципу «одного окна», причем желательно в рамках меж-

дународной организации. Они апеллируют, среди прочего, к практической сложности, которую представляет для стран с ограниченными людскими и финансовыми ресурсами необходимость участвовать в обсуждении вопросов управления Интернетом в условиях сильной децентрализации и наличия множества институтов. Таким странам трудно участвовать во встречах в основных дипломатических центрах (Женева, Нью-Йорк), а тем более — следить за деятельностью других институтов, таких как ICANN, Консорциум «Всемирная паутина» (W3C) и IETF.

Защита общественных интересов в Интернете

Одной из наиболее сильных сторон Интернета является его общественный характер, что обеспечило быстрый рост сети, а также поощряло креативность и открытость. Защита общественной природы Интернета останется одной из важнейших проблем управления Интернетом. Эта проблема осложняется тем, что основная часть технической инфраструктуры Интернета — от межконтинентальных магистральных кабелей до локальных подсетей — находится в частной собственности. Можно ли обязать частные компании управлять своей собственностью в общественных интересах, какие части Интернета могут рассматриваться как глобальное общественное благо — вот некоторые из сложных вопросов, которые необходимо разрешить. Например, в поддержку идеи рассматривать основную инфраструктуру Интернета в качестве глобального общественного блага выступили голландский исследователь Денни Бредерс[23] и посол Мальты Алекс Сцеберас Тригона[24]. В последнее время вопрос об общественной природе Интернета вновь приобрел актуальность в связи с дебатами о сетевой нейтральности.

Подробнее о глобальном общественном благе см. ***Раздел 7.***

География и Интернет

На заре развития Интернета было распространено мнение, что эта глобальная сеть преодолевает государственные границы и разрушает принцип

суверенитета. Коммуникации в Интернете легко пересекают национальные границы, а принцип анонимности пользователей заложен в самой структуре Интернета, что дало повод многим полагать, цитируя знаменитую «Декларацию независимости киберпространства», что «правительства не имеют ни морального права управлять нами [пользователями], ни методов принуждения, которые действительно могли бы нас устрашить».

Однако последние тенденции в развитии технологии, в том числе и создание более сложного геолокационного программного обеспечения, все чаще ставят под вопрос утверждение о «конце географии» в эпоху Интернета. На самом деле географическое местонахождение пользователя снова стало играть важную роль. На современном этапе географический фактор имеет гораздо большее значение для интернет-пользователей, чем до появления Интернета. Чем сильнее Интернет привязан к географическому фактору, тем менее уникальной становится система управления им. Например, при возможности определять географическое местоположение пользователей и транзакций сложная проблема юрисдикции в Интернете может быть решена с опорой на существующие законы.

Цифровые технологии и политическая неопределенность

Цифровые технологии развиваются очень быстро. Новые сервисы появляются почти каждый день, что создает дополнительные трудности при обсуждении вопросов управления Интернетом. Например, когда в Тунисе велись переговоры в рамках WSIS в ноябре 2005 г.[25], Twitter еще не было. Однако использование Twitter является важным фактором при обсуждении ключевых вопросов управления Интернетом, включая защиту персональных данных и свободу выражения мнений.

Еще одним примером влияния технологий на управление Интернетом является борьба со спамом. В 2005 г. это был один из основных вопросов в области управления Интернетом. Но технология фильтрования сейчас вышла на такой уровень, что проблема спама утратила свою актуальность.

Таким образом, некоторые из существующих в настоящее время проблем с управлением Интернетом могут быть решены по мере технологического прогресса.

Достижение политического равновесия

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

- противоречие между свободой самовыражения и защитой общественного порядка. Широко известное противоречие между статьей 19 (свобода самовыражения) и статьей 29 (защита общественного порядка) Всеобщей декларации прав человека нашло свое отражение и в Интернете. Данное противоречие обсуждается в контексте регулирования содержания материалов и цензуры в Интернете;
- противоречие между кибербезопасностью и неприкосновенностью частной жизни. Как и в реальной жизни, обеспечение безопасности в киберпространстве ставит под угрозу некоторые права человека, в том числе право на неприкосновенность частной жизни. Баланс между кибербезопасностью и неприкосновенностью частной жизни постоянно колеблется в ту или иную сторону в зависимости от политической ситуации в мире. Из-за многочисленных террористических актов вопросы безопасности приобрели больший вес в глобальной повестке дня, и баланс сместился в сторону кибербезопасности;

Подробнее о кибербезопасности см. ***Раздел 3.***

- противоречие между защитой авторских прав и добросовестным использованием материалов; еще одна правовая дилемма реального мира, также затрагивающая Интернет.

Подробнее об интеллектуальной собственности см. ***Раздел 4.***

Многие считают такие противопоставления ложными. Например, есть основания утверждать, что меры по усилению кибербезопасности не означают обязательное ограничение права на неприкосновенность частной жизни. Некоторые подходы позволяют повышать уровень безопасности и одновременно добиваться еще большего соблюдения права на неприкосновенность частной жизни. Хотя у таких взглядов есть рьяные сторонники, реальность в сфере регулирования Интернета такова, что необходимо постоянно искать точки равновесия и добиваться компромисса между различными вариантами.

«Не изобретайте колесо»

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

- созданные специально для Интернета (например, регламенты ICANN по присвоению имен и номеров в Интернете, правила нейтральности в Интернете, регламенты в отношении Интернета вещей);
- существующие нормы и регламенты, требующие корректировки в свете присущих Интернету особенностей. Масштабы корректировки могут быть разными: от достаточно ограниченных, как в случае с нормами по защите прав человека, до существенных изменений, например, в сфере кибервалют или налогообложения интернет-торговли.

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

«Не сломано — не чините!»

Управление Интернетом должно сохранить существующую функциональность и надежность Интернета и вместе с тем оставаться достаточно гибким для внесения изменений в интересах расширения технических возможностей и повышения легитимности. Общепризнано, что стабильность и функциональность Интернета должны быть ключевыми принципами управления им.

Стабильность Интернета должна быть сохранена путем использования давно известного подхода «работающего кода», предполагающего постепенное внедрение тщательно проверенных изменений в техническую инфраструктуру. Однако существует риск, что использование лозунга «Не сломано — не чините!» будет означать безоговорочный отказ от каких-либо перемен в существующей системе управления Интернетом, включая перемены, не обязательно связанные с технической инфраструктурой. В качестве одного

из возможных решений предлагается использовать этот принцип как критерий оценки конкретных шагов в области управления Интернетом (например, внедрения новых протоколов и перемен в механизмах принятия решений).

Важность комплексного подхода и определения приоритетов

Комплексный подход призван способствовать решению не только технических аспектов функционирования и эволюции Интернета, но и правовых, социальных, экономических факторов, вопросов развития, безопасности и прав человека. Необходимо также учитывать процесс сближения цифровых технологий. В частности, интернет-компании выходят на рынок телекоммуникационных услуг (например, Google и Facebook прокладывают подводные кабели), а телекоммуникационные компании оказывает услуги по предоставлению контента.

Рисунок 3. Управление Интернетом в виде леса

Придерживаясь комплексного подхода к переговорам по управлению Интернетом, заинтересованные стороны должны определить вопросы, представляющие для них наибольший интерес, то есть выбрать ветви дерева, которое их интересует, не теряя из виду лес других проблем в сфере управления Интернетом (рис. 3).

Ни развивающиеся, ни развитые страны не являются однородной группой. Среди развивающихся стран имеются существенные различия в приоритетах, уровне развития и готовности к использованию информационных технологий (например, между развитыми с точки зрения ИКТ странами, такими как Индия, Китай, Бразилия, и наименее развитыми странами Африки южнее Сахары). Комплексный подход и определение приоритетов в управлении Интернетом должны помочь заинтересованным сторонам — как из развитых, так и из развивающихся стран — сосредоточиться на определенном круге вопросов. Это повысит содержательность переговоров и может снизить их политизированность. Произойдет группировка заинтересованных сторон по интересам, а не вдоль традиционных исключительно политизированных «разделительных линий» (например, развитые — развивающиеся страны, правительства — гражданское общество).

Принцип технологической нейтральности

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

Технологическая нейтральность предоставляет множество преимуществ с точки зрения управления. Она обеспечивает долгосрочную применимость регулирующих принципов вне зависимости от будущих направлений технологического развития и вероятной конвергенции ключевых технологий (телекоммуникаций, СМИ, Интернета). Технологическая нейтральность отличается от сетевой нейтральности: принцип технологической нейтральности подразумевает независимость тех или иных мер от регулируемой технологии, тогда как в случае с сетевой нейтральностью речь идет преимущественно о нейтральности интернет-трафика.

Превращайте подразумеваемые технические решения в ясные политические принципы

В интернет-сообществе весьма распространено мнение, что особенности технического устройства Интернета способствуют распространению определенных общественных ценностей, например, свободы общения. Например, принцип сетевой нейтральности, в соответствии с которым данные передаются в сети между двумя конечными точками без какой-либо дискриминации, часто провозглашается гарантом свободы слова в Интернете. Из этого можно сделать ошибочный вывод, что технологические решения сами по себе достаточны для защиты и продвижения общественных ценностей. Развитие Интернета в последнее время, например, использование «брандмауэров» для ограничения потока информации, доказывает, что технологию можно использовать с разными целями, в том числе взаимно противоречащими друг другу. Всегда, когда это возможно, политические принципы, такие как свобода коммуникации, должны быть четко обозначены на политическом уровне, а не предполагаться неявно, на техническом уровне. Технические решения призваны способствовать реализации политических принципов, но не должны быть единственным способом их продвижения.

Помните о рисках управления обществом с помощью программного кода

Лоренс Лессиг обращает внимание на один из ключевых аспектов взаимоотношений между технологией и политикой: по мере возрастания зависимости от Интернета современное общество начинает регулироваться программным кодом, а не законами. В конечном счете, некоторые функции парламентов и правительств могут де-факто принять на себя компьютерные компании и разработчики программного обеспечения. С помощью программного обеспечения и технических решений они смогут влиять на жизнь обществ, все больше зависящих от Интернета. Появление новых технологий искусственного интеллекта может привести к передаче машинам обязанности принимать решения по определенным вопросам. Сейчас идут острые споры о регулировании использования беспилотных автомобилей.

Современному обществу придется определить пределы замены людей машинами в повседневной жизни, а также ограничить возможности роботов принимать решения по вопросам политической и правовой организации нашего общества.

Аналогии

Хотя аналогии часто обманчивы, они менее обманчивы, чем что-либо другое.

Сэмюэл Батлер, английский поэт (1835—1902)

Аналогия помогает нам понимать новые явления через уже известные. Проведение параллелей между примерами из прошлого и сегодняшним днем, несмотря на связанные с этим риски, является ключевым познавательным процессом в праве и политике. Большинство судебных дел, связанных с Интернетом, решаются посредством аналогий, особенно в рамках англосаксонской системы прецедентного права. Однако использование аналогий в управлении Интернетом имеет ряд важных ограничений.

Во-первых, Интернет — широкое понятие, охватывающее разнообразные услуги: электронную почту (аналогия с телефоном), сетевые услуги (аналогия с теле- и радиовещанием), базы данных (аналогия с библиотекой) и социальные сети (аналогия с кафе и базарами). Любая аналогия с каким-либо одним аспектом Интернета может излишне упростить общее понимание данной технологии.

Во-вторых, по мере сближения разнообразных 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 остаются мощным и основным познавательным инструментом при разрешении судебных дел и создании режима управления Интернетом.

В третьих, аналогии имели огромное значение на ранних этапах развития Интернета, когда сеть была еще чем-то новым. Например, в первом издании книги (2004 г.) существо Интернета объяснялось посредством проведения аналогий. С развитием Интернета эта методика начала терять свою актуальность. В эпоху Интернета уже выросло новое поколение, для которого некоторые аналогии, использованные в том исследовании (например, сравнение с видеомагнитофоном), звучат архаично. Тем не менее аналогии продолжают играть важную роль в судебных процессах, связанных с Интернетом, а также при разработке политических мер, определяющих систему управления Интернетом. Ниже описаны аналогии, которые использовались при формировании системы управления Интернетом и позволяют понять текущие процессы в сфере регулирования цифровых технологий.

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.

Отличия: Передача данных в Интернете основана на использовании пакетов данных, а не электрических цепей (как при аналоговой 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), интерактивные услуги и т.д., не имеют сходства с телефоном.

Кем используется: Противниками какого-либо существенного регулирования материалов Интернета. Если Интернет схож с телефоном, то содержание данных, передаваемых по Интернету, как и телефонные разговоры, не может подлежать контролю, в отличие, например, от вещательных услуг. Эту аналогию также используют те, кто доказывает, что Интернет должен регулироваться, подобно другим видам связи (например, телефонная связь, почта),

национальными органами власти при координирующей роли международных организаций, таких как Международный союз электросвязи. В соответствии с этой аналогией система доменных имен должна быть организована и управляться наподобие системы нумерации в сетях телефонной связи[26].

Ситуация изменилась с появлением услуг IP-телефонии (VoIP), например, Skype, которые выполняют функцию телефона, используя при этом IP-протокол. Это противоречие привело к острым дискуссиям на 12-й Всемирной конференции по международной электросвязи (WCIT) в Дубае. Против того, чтобы считать IP-телефонию интернет-услугой, выступили те, кто настаивает на ее регулировании наподобие услуг телефонии на национальном и международном уровнях, в частности, при более активной роли 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.

Кем используется: Всемирная почтовая конвенция проводит 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 дневни-

ками. Интернет-провайдерам оказалось непросто разрешить эту проблему, вызвавшую бурю эмоций. Вместо того, чтобы согласиться с аналогией между письмами и электронной почтой, большинство провайдеров отказало в доступе, сославшись на соглашение о защите тайны корреспонденции, заключаемое с пользователями.

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

Интернет — телевидение

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

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

Кем используется: Эту аналогию используют те, кто стремится к установлению более строгого контроля над содержанием материалов Интернета. По их мнению, поскольку возможности Интернета как средства массовой информации сходны с возможностями телевидения, Интернет необходимо строго контролировать. Правительство США пыталось использовать эту аналогию в знаменитом деле «Рино против Американского союза за гражданские свободы» (Reno vs. ACLU)[27]. Источником этого дела стал принятый Конгрессом Акт о пристойности коммуникаций, предусматривавший тщательный контроль над содержанием материалов Интернета для предотвращения доступа детей к порнографическим материалам. Суд отказался признать правомочность аналогии с телевидением.

Интернет — библиотека

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

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

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

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

Интернет — видеомагнитофон, копировальный аппарат

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

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

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

Эта аналогия использовалась в судебных делах против разработчиков программного обеспечения для обмена файлами по принципу пиринга (непосредственно между компьютерами пользователей), такого как Grokster и StreamCast.

Интернет — магистраль

Общие черты: В реальном мире автомагистрали выполняют ту же роль в области транспорта, что и Интернет в области связи в виртуальном мире.

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

Кем используется: Аналогия с автомагистралью активно использовалась с середины 1990-х гг., после того, как А. Гор ввел в употребление термин «информационная супермагистраль» (information superhighway). Термин «магистраль» также использовался немецким правительством, чтобы оправдать введение в июне 1997 г. более строгого закона о контроле над содержанием Интернета:

> *Это либеральный закон, который не имеет ничего общего с цензурой, но четко обозначает, что может и не может делать провайдер. Интернет — это средство передачи и распространения знания... как и для магистралей, для него необходимы правила движения* [28].

> Автомагистрали и Интернет
>
> Бывший Генеральный секретарь МСЭ Хамадун Турэ использовал аналогию с автомагистралью, сравнив автомагистрали с телекоммуникационными сетями, а интернет-трафик — с грузовиками или машинами: «Я привел простой пример, сравнив Интернет и передачу данных с потоками грузовиков или машин на автомагистрали. То, что вы владеете автомагистралью, не дает вам прав собственности на грузовики и машины, проезжающие по ней, и, конечно, на товары, которые они перевозят, и наоборот. Это простая аналогия. Но для того, чтобы транспорт ехал без помех, при постройке дорог и мостов необходимо учесть вес, высоту и скорость грузовиков. В противном случае система не будет работать. По моему мнению, это отражает взаимосвязь между Интернетом и телекоммуникационными сетями. Они обречены на совместную работу»[29].

Интернет — открытое море

Общие черты: Изначально аналогия появилась благодаря тому, что Интернет, как и открытое море, находился за пределами юрисдикции государств.

Отличия: Между открытым морем и Интернетом нет ничего общего. Во-первых, интернет-данные всегда относятся к определенной юрисдикции. Даже если телекоммуникационные кабели, проложенные по дну Тихого или Атлантического океана, находятся в открытом море, большинство из них все равно принадлежит частным компаниям, которые, в свою очередь, подчиняются национальной юрисдикции страны регистрации. Даже если компа-

ния Microsoft разместит свои дата-центры в открытом море (такой вариант действительно рассматривался), все равно этот объект будет находиться в юрисдикции США, поскольку Microsoft зарегистрирована в США. Любое устройство, кабель или судно в открытом море подчиняются определенной национальной юрисдикции.

Кем используется: Аналогия с открытым морем используется в качестве аргумента в пользу ряда суждений. Иногда аналогия используется теми, кто выступает за международное регулирование Интернета. Практическим следствием этой аналогии является то, что к Интернету применима концепция римского права res communis omnium (пространство как общее достояние человечества, которое подлежит регулированию со стороны всех стран), которая используется в отношении открытого моря. Аналогия с открытым морем также используется как довод против регулирования Интернета на национальном уровне, поскольку Интернет представляет собой пространство, выходящее за рамки юрисдикции отдельной страны, как в случае с Антарктикой и космосом.

Классификация вопросов управления Интернетом

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

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

В итоговом отчете WGIG (2005) обозначены следующие важнейшие проблемы:

- вопросы, касающиеся инфраструктуры и управления важнейшими интернет-ресурсами;
- вопросы, касающиеся использования Интернета, включая спам, сетевую безопасность и киберпреступность;
- вопросы, связанные с Интернетом, но имеющие далеко идущие последствия, выходящие за рамки Интернета, за которые отвечают соответствующие действующие организации, например, вопросы прав интеллектуальной собственности или международной торговли;
- вопросы, касающиеся проблем развития в контексте управления Интернетом, в частности, укрепления потенциала развивающихся стран.

Повестка дня первого Форума по управлению Интернетом (IGF), проходившего в Афинах в 2006 г., включала в себя обсуждение следующих проблемных областей: доступ, безопасность, открытость и разнообразие. В ходе второго IGF, проходившего в Рио-де-Жанейро в 2007 г., в повестку дня была внесена пятая проблемная область — управление ключевыми ресурсами Интернета. Эти пять тем определяли повестку всех последующих форумов IGF.

Хотя подходы к классификации могут меняться, управление Интернетом затрагивает относительно неизменный набор из 40—50 конкретных проблем; актуальность каждой из них может изменяться. В частности, спам выступал в качестве отдельной проблемы в классификации WGIG 2004 г., однако со временем с точки зрения IGF его политическое значение снизилось, и спам стал всего лишь одной из не самых существенных тем, обсуждаемых в связи с проблемами безопасности.

В разработанной Diplo классификации аспектов управления Интернетом основные 40–50 проблем управления Интернетом разбиты на семь групп[30]:

- Инфраструктура
- Безопасность
- Правовые аспекты
- Экономика
- Развитие
- Социокультурные аспекты
- Права человека

Классификация (рис. 4) отражает как упомянутые выше политические подходы WGIG и IGF, так и результаты научных исследований в данной области. Классификация была разработана в 1997 г. и с тех пор регулярно уточнялась и дополнялась с учетом комментариев от участников образовательных программ Diplo (3000 выпускников на 2015 г.), результатов научных исследований, политической практики и поиска данных. Схожая классификация, в основе которой также лежат семь кластеров, используется в докладе «Карта вопросов относительно функционирования международной системы управления Интернетом», подготовленном секретариатом Комиссии по науке и технике в целях развития (КНТР) в связи с проведением межсессионного тематического заседания комиссии в ноябре 2014 г.[31]

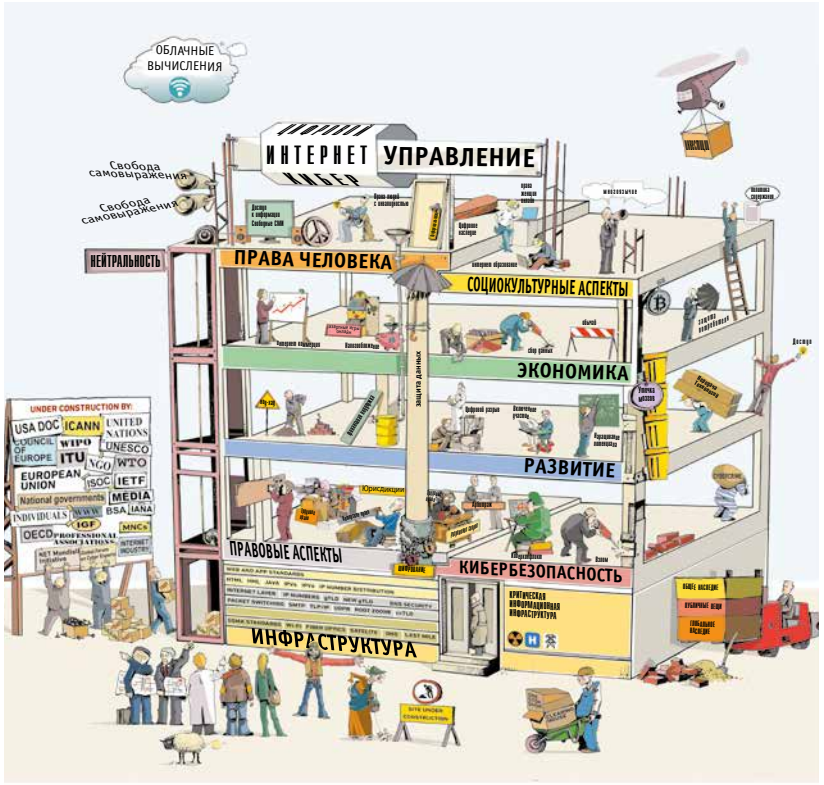


Рисунок 4. Строительство системы управления Интернетом

Характеристика, определение и описание концепции управления Интернетом

В предыдущих разделах мы описали различные подходы к разработке концепции управления Интернетом. Эта концепция остается открытой для различных интерпретаций, о чем свидетельствует приведенная выше схема (рис. 4). На ней изображено строящееся здание. Наверху размещена растяжка с надписью «Управление Интернетом», при этом слово «Интернет» находится во вращающемся сегменте, что позволяет без труда заменить «Управление Интернетом» выражением «Управление киберпространством» или «Управление цифровыми ресурсами». В политических дискуссиях используются и другие термины, в частности, «политика в области Интернета», «цифровая политика» и «кибердипломатия».

Трудности вызывает вопрос о том, что же именно входит в понятие «управление Интернетом». Одни полагают, что обеспечение кибербезопасности является одним из элементов управления Интернетом, другие считают кибербезопасность отдельной сферой деятельности. Для одних управление Интернетом сводится к вопросам, входящим в компетенцию ICANN (управление доменными именами, IP-адресами и т. д.), другие считают, что управление Интернетом охватывает намного более широкий круг вопросов.

Это не абстрактный спор. Выбор тех или иных трактовок задает тон дискуссий по вопросу о том, где, как и кто управляет Интернетом. Простых решений в споре о терминах и определениях нет. Разногласия будут всегда. В конечном счете, вряд ли мы когда-нибудь согласуем единый набор «правильных» терминов и определений.

В этой книге термин «управление Интернетом» используется в качестве собирательной концепции, охватывающей 40 вопросов управления Интернетом, разбитых на семь групп. В основе этого подхода лежит определение управления Интернетом по версии WGIG, а также использование этого термина в процессе WSIS, публикациях и научных исследованиях. Другие термины имеют свое научное и политическое обоснование.

Спор о «правильных» терминах и определениях вряд ли даст какие-либо ощутимые результаты. Тем не менее важно составить четкое представление

по вопросам, относящимся к каждому термину. Например, какие вопросы связаны с такими терминами как «управление Интернетом», «цифровая политика» или «управление киберпространством»? Относятся ли к таким вопросам кибербезопасность, интернет-торговля и защита неприкосновенности частной жизни в Интернете? Понимание содержания каждого термина — первый шаг к преодолению неразберихи политического процесса.

В конечном счете, благодаря органичной интеграции цифровых технологий в жизнь современного общества терминологические споры могут утратить свою актуальность. Интернет-торговля станет неотъемлемой частью торговли в целом. Кибербезопасность станет составным элементом политики безопасности. Чем больше цифровые технологии будут становиться неотъемлемой частью нашей повседневной жизни, тем более вероятно то, что проблема управления Интернетом сольется с более общей темой управления обществом.

Примечания к разделу 1

[1] Проведение Всемирной встречи на высшем уровне по вопросам информационного общества (World Summit on the Information Society — WSIS) было поддержано Резолюцией Генеральной ассамблеи ООН 56/183 от 21 декабря 2001 г. Предполагалось, что встреча пройдет в два этапа. Первый этап состоялся в Женеве 10–12 декабря 2003 г., второй этап в Тунисе 16–18 ноября 2005 г. Цель первого этапа – разработать и принять программное заявление и предпринять конкретные шаги, чтобы заложить основы информационного общества для всех с учетом различных интересов. Во встрече на высшем уровне и связанных с ней мероприятиях приняли участие более 19 тыс. участников из 174 стран. Адрес в Интернете: http://www.itu.int/wsis/basic/about.html [просмотрено 2 августа 2018 г.].

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

[3] Shannon, Victoria. "What's in an 'i'? Internet Governance" // International Herald Tribune, 3.12.2006 (адрес в Интернете: http://www.nytimes.com/2006/12/03/technology/03iht-btitu.3755510.html) [просмотрено 2 августа 2018 г.].

[4] Barlow JP. A declaration of the independence of cyberspace (адрес в Интернете: https://www.eff.org/cyberspace-independence) [просмотрено 2 августа 2018 г.].

[5] Об эволюции использования термина «Интернет» в ходе подготовки к саммиту WSIS см.: DiploFoundation. loFoundation (2003) The Emerging Language of ICT Diplomacy — Key Words (адрес в Интернете: https://www.diplomacy.edu/IGFlanguage/2004research) [просмотрено 2 августа 2018 г.].

[6] Working Group on Internet Governance (2005) Report (адрес в Интернете: http://www.wgig.org/docs/WGIGREPORT.pdf) [просмотрено 2 августа 2018 г.].

[7] Всемирная встреча на высшем уровне по вопросам информационного общества (2005), Тунисская программа для информационного общества (адрес в Интернете: http://www.itu.int/net/wsis/docs2/tunis/off/6rev1.html) [просмотрено 2 августа 2018 г.].

[8] В июне 2010 г. ICANN одобрила решение о создании домена верхнего уровня .xxx «для взрослых».

[9] Подробнее о сетевой нейтральности, см. образовательный видеоролик, размещенный по адресу: https://www.youtube.com/watch?v=R-uMbZFfJVU [просмотрено 2 августа 2018 г.].

[10] Clinton H (2010) Remarks on Internet freedom (адрес в Интернете: https://2009-2017.state.gov/secretary/20092013clinton/rm/2010/01/135519.htm [просмотрено 2 августа 2018 г.].

[11] См. пункт 123 Аддис-Абебской программы действий третьей Международной конференции по финансированию развития, которая прошла 13–16 июля 2015 г. (адрес в Интернете: http://www.un.org/esa/ffd/wpcontent/uploads/2015/08/AAAA_Outcome.pdf) [просмотрено 2 августа 2018 г.].

[12] World Bank (2016) World Development Report 2016: Digital Dividends (адрес в Интернете: http://www.worldbank.org/en/publication/wdr2016) [просмотрено 2 августа 2018 г.].

[13] Drake W et al. (2016) Internet Fragmentation: An Overview. (адрес в Интернете: http://www3.weforum.org/docs/WEF_FII_Internet_Fragmentation_An_Overview_2016.pdf) [просмотрено 2 августа 2018 г.].

[14] Global Commission on Internet Governance (2016) One Internet (адрес в Интернете: https://www.ourinternet.org/report) [просмотрено 2 августа 2018 г.].

[15] Wiener N (1948) Cybernetics: Or Control and Communication in the Animal and the Machine. Paris: Hermann & Cie, Cambridge, MA: Technology Press, and New York: John Wiley & Son.

[16] Gibson W (1984) Neuromancer. New York: Ace Books.

[17] Newitz A (2013) The bizarre evolution of the word 'cyber' (адрес в Интернете: http://io9.gizmodo.com/today-cyber-means-war-but-back-in-the-1990s-it-mean-1325671487) [просмотрено 2 августа 2018 г.].

[18] European Commission (2015) A Digital Single Market Strategy for Europe (адрес в Интернете: https://ec.europa.eu/digital-single-market/en/news/digital-single-market-strategy-europe-com2015-192-final) [просмотрено 2 августа 2018 г.].

[19] Цит. по Helfand D. Edpseak is in a class by itself // Los Angeles Times, 16.08.2001 (адрес в Интернете: http://articles.latimes.com/2001/aug/16/news/mn-34814) [просмотрено 2 августа 2018 г.].

[20] В подготовку данного раздела неоценимый вклад внес старший научный сотрудник фонда Diplo Альдо Маттеуччи, чья неортодоксальная позиция по управлению Интернетом диссонирует с деятельностью других исследователей фонда.

[21] Резолюция Генеральной Ассамблеи Организации Объединенных Наций A/70/125 (2015). Итоговый документ совещания высокого уровня Генеральной Ассамблеи, посвященного общему обзору хода осуществления решений Всемирной встречи на высшем уровне по вопросам информационного общества (адрес в Интернете: http://workspace.unpan.org/sites/Internet/Documents/UNPAN95735.pdf) [просмотрено 2 августа 2018 г.].

[22] NATO (2016) Warsaw Summit Communiqué (адрес в Интернете: http://www.nato.int/cps/en/natohq/official_texts_133169.htm) [просмотрено 2 августа 2018 г.].

[23] Broeders D (2015) The public core of the Internet. Amsterdam: Amsterdam University Press (адрес в Интернете: https://www.wrr.nl/publicaties/policy-briefs/2015/04/10/the-public-core-of-the-internet) [просмотрено 2 августа 2018 г.].

[24] Выступление посла Тригона на заседании Генеральной Ассамблеи ООН, посвященном Всемирной встрече на высшем уровне по вопросам информационного общества, Нью-Йорк, 15.12.2015 (адрес в Интернете: https://www.gov.mt/en/Government/Press%20Releases/Documents/pr152897a.pdf) [просмотрено 2 августа 2018 г.].

[25] Начало процессу WSIS было положено подготовительным заседанием, которое состоялось в июле 2002 г. в Женеве. Первая встреча на высшем уровне состоялась в Женеве (декабрь 2003 г.), а вторая в Тунисе (ноябрь 2005 г.).

[26] Волкер Китц поддерживает использование аналогии между управлением системами телефонной связи и распределением номеров и имен в Интернете. Kitz V. ICANN may be the only game in town, but Marina del Rey isn't the only town on Earth: Some thoughts on the so-called uniqueness of the Internet. 2004 (адрес в Интернете: https://smu.primo.exlibrisgroup.com/discovery/fulldisplay?docid=lexisnexis_lawreviews7CompLRev26TechJ281&context=PC&vid=01SMU_INST:01SMU&lang=en&search_scope=MyInst_and_CI&adaptor=Primo%20Central&tab=Everything&query=any,contains,CANN%20may%20be%20the%20only%20game%20in%20town,%20but%20Marina%20del%20Rey%20isn%E2%80%99t%20the%20only%20town%20on%20Earth&offset=0) [просмотрено 2 августа 2018 г.].

[27] US Supreme Court (1997) Decision in Reno vs American Civil Liberty Union (адрес в Интернете: https://supreme.justia.com/cases/federal/us/521/844/case.html) [просмотрено 2 августа 2018 г.].

[28] Цит. по Mock K and Armony L (1998) Hate on the Internet (адрес в Интернете: http://archive.is/M70XS) [просмотрено 2 августа 2018 г.].

[29] Выдержки из речи генерального секретаря МСЭ на встрече ICANN в Каире 6 ноября 2008 г. (адрес в Интернете: https://archive.icann.org/en/meetings/cairo2008/files/meetings/cairo2008/toure-speech-06nov08.txt) [просмотрено 2 августа 2018 г.].

[30] Термин «группа» (в англ. basket – корзина) вошел в дипломатический обиход в ходе переговоров в Организации по безопасности и сотрудничеству в Европе (ОБСЕ).

[31] CSTD (2015) Mapping of international Internet public policy issues (адрес в Интернете: http://unctad.org/meetings/en/SessionalDocuments/ecn162015crp2_en.pdf) [просмотрено 2 августа 2018 г.].

Раздел 2

Инфраструктура

Инфраструктура

К «инфраструктурной корзине» относятся основополагающие, в основном технические, вопросы, связанные с функционированием Интернета. Основным критерием отнесения того или иного вопроса к данной «корзине» является его значимость с точки зрения базовой технической функциональности Интернета. Данная группа включает в себя наиболее важные вопросы, без решения которых ни Интернет, ни «всемирная паутина» (WWW)[1] не могли бы существовать, и представлена следующими тремя уровнями, или слоями, как показано на рис. 5:

Рисунок 5. Уровни Интернета

1 телекоммуникационная инфраструктура, по которой передаются потоки интернет-данных (трафик).

2 Технические вопросы, связанные со стандартами (техническими и веб-стандартами) и важнейшими интернет-ресурсами (IP-номера, DNS, корневая зона).

3 Смежные вопросы, включая сетевую нейтральность, облачные вычисления, Интернет вещей и конвергентность.

Телекомуникационная инфраструктура[2]

Современное состояние

Телекоммуникационная инфраструктура обеспечивает передачу данных в Интернете: телефонные провода, оптоволоконные кабели, электромагнитные волны, включая спутниковую связь, радиосвязь и сети мобильной связи. Во многих случаях существующая телекоммуникационная инфраструктура, например, линии телефонной связи или сети мобильной связи, электроэнергетические системы[3], подводные кабели или спутниковая связь, используются для передачи пакетов данных в Интернете. Однако для передачи данных все больше используется инновационная телекоммуникационная инфраструктура, включая высокоскоростные подводные оптоволоконные кабели, сети мобильной связи пятого поколения (5G), а также такие инновационные беспроводные решения как проект Google Loon[4] по использованию высотных аэростатов для создания беспроводной сети, проект Television White Spaces[5] и технологии по развитию Интернета вещей.

> Наиболее распространенные технологии подключения к Интернету
>
> *Проводная телекоммуникационная инфраструктура*
>
> • Цифровые абонентские линии (DSL): использование существующих медных проводов телефонной связи для передачи данных и телефонного трафика.

- Сети кабельного телевидения: доступ в Интернет предоставляется провайдерами широкополосных кабельных служб с использованием сетей кабельного телевидения.
- Оптоволоконные сети: сети оптоволоконной связи пользуются наибольшей популярностью как основная инфраструктура Интернета благодаря способности волокна передавать значительные объемы данных на большие расстояния без существенной потери качества сигнала с увеличением расстояния.
- Интернет по электрической сети: пользователи получают доступ к высокоскоростному Интернету, подключив прибор к электросети.

Беспроводная телекоммуникационная инфраструктура

- Спутниковый Интернет: обеспечение доступа к Интернету в местах, где наземные системы подключения недоступны, а также для высокомобильных сообществ.
- Wi-Fi: подключение к беспроводным локальным вычислительным сетям (WLAN) при помощи радиочастот.
- WiMAX (Технология широкополосного доступа в микроволновом диапазоне): обеспечивает широкополосный беспроводной доступ на больших расстояниях; будучи альтернативным решением по сравнению с кабельными сетями и DSL, WiMAX может работать на лицензируемых и нелицензируемых частотах.
- Широкополосная передача цифровых данных по беспроводным каналам в сотовых сетях: одной из наиболее распространенных технологий является Global System for Mobile Communications (GSM), которая появилась в Европе и стала ведущим стандартом по всему миру с появлением сетей третьего (3G) и четвертого (4G) поколения, с перспективой появления сетей пятого поколения (5G).

Регулирование телекоммуникационной отрасли напрямую влияет на управление Интернетом. Телекоммуникационная инфраструктура регулируется как на национальном, так и на международном уровне. Ключевыми международными организациями в сфере регулирования телекоммуникаций являются, например, Международный союз электросвязи (МСЭ), который разработал подробные правила, регулирующие отношения между национальными операторами, распределение радиочастот и положение спутников,

а также Всемирная торговая организация (ВТО), сыгравшая ключевую роль в либерализации телекоммуникационных рынков по всему миру[6].

Два регламента международной электросвязи

Регламент международной электросвязи (РМЭ), подготовленный МСЭ в 1988 г., способствовал либерализации ценообразования и услуг по всему миру и сделал возможным инновационное использование таких базовых услуг, как международная аренда линий. Таким образом, была создана инфраструктурная база для быстрого развития Интернета в 1990-егг. В ходе Всемирной конференции по международной электросвязи 2012 г. в Дубае (WCIT-12) в РМЭ были внесены изменения. Новую версию РМЭ подписали 89 стран, преимущественно развивающихся, тогда как 55 государств, включая США и многие европейские страны, отказались это делать[7]. Таким образом, с 1 января 2015 г., когда новая версия РМЭ вступила в силу, действуют два международных режима регулирования электросвязи (РМЭ 1988 г. и РМЭ 2012 г.). К счастью, внесенные в 2012 г. поправки носят достаточно узкий характер и не затрагивают общего функционирования системы международной электросвязи. Однако это не означает, что решать проблему одновременного существования двух регламентов не нужно.

Роли ВТО и МСЭ существенно отличаются. МСЭ устанавливает детально разработанные добровольные технические стандарты, международные нормы, касающиеся непосредственно телекоммуникаций, и предоставляет помощь развивающимся странам в их соблюдении[8]. Большинство споров по вопросам регулирования связаны с попытками МСЭ решать пограничные вопросы, одновременно затрагивающие функционирование телекоммуникационной инфраструктуры и Интернета, например, IP-телефонию, кибербезопасность и цифровые идентификаторы объекта (Digital Object Architecture)[9]. ВТО же задает рамки общих правил рынка[10], а ее деятельность в сфере телекоммуникаций до сих пор не вызывала каких-либо существенных разногласий. Тем не менее, если ВТО станет более активно регулировать интернет-торговлю, это может спровоцировать дискуссии по вопросам, связанным с кибербезопасностью и защитой данных.

Вопросы

Магистральные интернет-кабели[11]

После того как в 1870 г. по дну Средиземного моря, Красного моря и Индийского океана до Индии был доведен первый телеграфный кабель, на донные кабели приходились основные объемы электросвязи. В настоящее время на подводные оптоволоконные кабели, проложенные практически по тем же маршрутам, что и телеграфные кабели, приходится 90% глобального интернет-трафика.

Подводные интернет-кабели связывают сетевые узлы. Так, большинство латиноамериканских кабелей ведет в Майями. Ключевые узлы Азии расположены в Сингапуре и Гонконге. К таким узлам также относятся Амстердам, Нью-Йорк и Сан-Франциско. Стратегически важные районы, например, Лусонский, Ормузский и Малаккский проливы, а также Суэцкий канал остаются наиболее уязвимыми районами с точки зрения прокладки интернет-кабелей и передачи данных. Географический фактор играет важную роль в обеспечении цифровой связи между Азией и Европой. Например, 95% трафика между Азией и Европой идет через Египет, как и в случае с морским транспортом, для которого огромное значение имеет Суэцкий канал. Поскольку значительная часть интернет-трафика приходится на подводные кабели, прокладка новых интернет-кабелей по суше считается важным шагом на пути диверсификации интернет-трафика, особенно между Азией и Европой.

Экономическая и социальная комиссия ООН для Азии и Тихого океана (ЭСКАТО) и Азиатский банк развития продвигают проект под названием «Азиатская магистраль», который заключается в создании трансконтинентальной транспортной инфраструктуры общей протяженностью 141 000 км[12]. Кроме того, Трансевроазиатская информационная магистраль (TASIM) должна связать Восточную Европу и Центральную Азию, что будет способствовать еще большей диверсификации межконтинентальных потоков данных. Проект нацелен на то, чтобы «повысить скорость соединения с восточноазиатскими партнерами и повысить стойкость Интернета», что также будет способствовать развитию регионального сотрудничества в Средней Азии[13].

Развитие цифровых технологий является важной составляющей инициативы «Один пояс, один путь». Этот компонент получил название «Цифровой шелковый путь»[14]. Реализация инфраструктурных проектов в области транспорта и энергетики может помочь улучшить цифровую связь путем прокладки оптоволоконных кабелей вдоль железных дорог и трубопроводов.

Ввод всех запланированных наземных кабелей, в частности, реализация инициативы по созданию «Цифрового шелкового пути», позволит впервые в истории переключить на наземные кабели значительный объем трафика, до сих передававшийся по подводным кабелям.

«Последняя миля» — местные линии связи

«Последней милей» (или, по-английски, «местной петлей», local loop) называется линия связи между компанией — поставщиком услуг Интернета (провайдером) и конечным пользователем. Проблемы с местными линиями связи (плохое состояние кабеля, отключение электроэнергии и т. п.) являются препятствием для более широкого распространения Интернета во многих, чаще развивающихся, странах. Одним из возможных недорогих решений проблемы «последней мили» может стать использование беспроводной связи. В последние годы компания Google экспериментировала с предоставлением интернет-доступа посредством аэростатов (проект Loon), а Facebook пыталась достичь такой цели посредством беспилотников. Помимо новых технологий, которые становятся все более доступными, решение проблемы местных линий связи зависит также от либерализации этого сегмента рынка телекоммуникаций, в том числе от предоставления возможности пользоваться местными телефонными сетями связи нескольким операторам (демонополизация «последней мили»).

Либерализация рынка телекоммуникаций

Исторически сложилось так, что инфраструктура и услуги связи предоставлялись на монопольной основе государственными операторами. За последние два десятилетия многие страны провели либерализацию услуг связи и способствовали появлению конкуренции в этой отрасли, дав возможность новым операторам выйти на рынок и создать свои сети

и услуги электронной связи. В процессе либерализации телекоммуникационного рынка новые поставщики услуг получили доступ к существующей (государственной) инфраструктуре. Политика либерализации сопровождалась приватизацией государственных телекоммуникационных операторов. В развивающихся странах этот процесс протекал медленнее. Такие страны часто сталкиваются с непростым выбором: провести либерализацию рынка телекоммуникационных услуг, снизить стоимость услуг связи и тем самым способствовать экономическому развитию или, напротив, сохранить монополию на телекоммуникационные услуги, приносящие существенный доход (в частности, благодаря международной системе взаиморасчетов между операторами связи, действовавшей в сфере традиционных услуг фиксированной телефонной связи). В этой связи по инициативе развивающихся стран в рамках Всемирной конференции по международной электросвязи 2012 г. (WCIT-12) и ряда других международных встреч рассматривался вопрос о распределении дохода от услуг интернет-связи.

Управление электромагнитным спектром

Хотя беспроводная связь нередко рассматривается как более удобное решение по сравнению с прокладкой проводной инфраструктуры, с использованием электромагнитных волн связана существенная проблема, которая заключается в ограниченности радиочастотного спектра. Теоретически, каждую частоту можно разбить на бесконечное множество сегментов. На практике, несмотря на постоянное совершенствование используемого нами оборудования с целью повышения эффективности использования спектра, ширина полосы не может быть меньше определенных величин. В противном случае возникают помехи со стороны оборудования, работающего на соседних частотах. Соответственно, требуется регулятор, который бы выделял полосы для одной или нескольких услуг радиосвязи и занимался распределением конкретных частотных сегментов среди операторов беспроводной связи, включая телестанции, радиопередатчики, операторов мобильной связи и интернет-провайдеров.

Как правило, за управление радиочастотным спектром каждой страны, то есть за тем, какие технологии используются в каждом сегменте радиочастотного спектра, какими операторами и на основании каких лицензий это делается, отвечают национальные регуляторы, которые координируют свою работу с аналогичными ведомствами стран ближнего и дальнего зарубежья на основании двухсторонних и региональных инициатив (например, Комитет по спектру радиочастот Европейского союза и Группа по политике в области спектра радиочастот) или в рамках международных учреждений (таких как МСЭ).

Так, в США, а также в большинстве стран Европейского союза, распределение радиочастот производится посредством проведения торгов в форме аукциона. В ЕС для гармонизации подходов отдельных стран к использованию радиочастот был разработан комплексный подход к управлению радиочастотами[15]. Лицензирование использования отдельных составляющих спектра и его предоставление тому, кто готов больше заплатить, например, мобильным операторам, обеспечивает использование спектра по назначению, а также является неплохим источником дохода для государства.

С развитием новых услуг связи, предусматривающих использование радиочастотного спектра, в особенности услуг беспроводного широкополосного доступа в Интернет и мобильной связи, вырос спрос на радиочастоты. Это вынудило власти по всему миру искать решения, которые могли бы обеспечить оптимальное использование спектра. Один из способов расширить пригодный для использования спектр радиочастот для цифровой связи заключается в освобождении спектра, который используется для аналогового телевещания. Для этого необходимо создать для вещательных компаний стимул отказаться от аналогового сигнала в пользу цифрового (что подразумевает существенные инвестиции в новое вещательное оборудование, а также закупку ресиверов для каждого абонента, при этом обеспечивая более высокое качество и возможность оказания дополнительных услуг), что позволило бы получить так называемый «цифровой дивиденд», то есть освободить существенную часть радиочастотного спектра для других услуг.

Объем радиочастотного спектра и связанные с этим ограничения меняются по мере развития технологий. Это дало основание некоторым группам потребовать ввести «открытый спектр» вместо существующих норм, то есть обеспечить открытый доступ для всех, как при использовании обычных Wi-Fi сетей (для создания сети Wi-Fi дома или где-нибудь еще лицензии не требуется). Однако у этой точки зрения два слабых места. Во-первых, те-

лекоммуникационные компании, в первую очередь в Европе, уже вложили огромные средства в приобретение прав на использование мобильных сетей третьего и четвертого поколений, так что введение «открытого спектра» было бы нечестно по отношению к ним и могло бы привести к их банкротству и дестабилизации телекоммуникационного рынка. Вторая проблема заключается в том, что общедоступность спектра не означает его использование как общественного блага с выгодой для всех. Более вероятной представляется ситуация, в которой спектр будут использовать субъекты, обладающие техническими возможностями для того, чтобы воспользоваться «открытым спектром» в собственных целях, в том числе в целях извлечения выгоды.

Поставщики интернет-услуг

Архитектура доступа в Интернет состоит из трех уровней. Поставщики интернет-услуг, подключающие конечных пользователей, составляют уровень 3. Уровни 1 и 2 состоят из оптовых поставщиков услуг широкополосной связи. Передача данных на уровне 1 осуществляется крупнейшими провайдерами услуг широкополосной связи. Они, как правило, заключают так называемые пиринговые соглашения об обмене данными с другими компаниями, работающими на том же уровне[16]. Основное различие между провайдерами, работающими на уровне 1 и уровне 2, заключается в том, что первые обмениваются трафиком друг с другом бесплатно, по принципу пиринга («равный с равным»), в то время как вторые вынуждены оплачивать передачу данных на уровень 1 соответствующим провайдерам[17]. Уровень1 обычно контролируется крупными компаниями — такими как AT&T, Verizon, Level 3 Communications, Vodafone и NTT Communications.

Вопросы

Телекоммуникационные монополии и поставщики интернет-услуг

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

Либерализация телекоммуникаций и роль поставщиков телекоммуникационных услуг

Существуют противоположные точки зрения на то, в какой степени провайдеры интернет-услуг и оптовые поставщики услуг широкополосной связи должны следовать существующим международным правилам. Развитые страны доказывают, что либеральные правила, предоставленные Всемирной торговой организацией 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 Всемирной торговой организации.

Роль интернет-провайдеров в обеспечении соблюдения требований закона

Поскольку конечные пользователи получают доступ в Интернет при посредничестве интернет-провайдеров, на такие компании может быть возложена обязанность по обеспечению непосредственного и полного соблюдения требований закона в отношении Интернета. Именно поэтому во многих странах интернет-провайдерам теперь отводится центральная роль в правоприменительной деятельности в таких областях как нарушения авторского права, защита детей в Интернете и в других областях.

Подробнее о роли посредников см. ***Раздел 4.***

Должна ли интернет-инфраструктура быть услугой общего пользования?

Интернет-трафик может передаваться по любому каналу связи. Однако на практике определенные мощности, например, магистрали уровня 1 (основные каналы данных, формирующие взаимосвязанные сети, и основные маршрутизаторы, использующие оптоволоконные кабели или спутниковые каналы), особенно важны для функционирования Интернета. Их центральное положение в структуре Интернета дает их владельцам возможность устанавливать цены и диктовать условия на предоставление своих услуг[18]. В конечном счете, само функционирование Интернета зависит от решений, принимаемых владельцами магистральных каналов передачи данных. Рост объемов интернет-трафика привел на этот рынок ряд новых участников, которые до этого не имели прямого отношения к телекоммуникационной отрасли. Например, Google, Facebook и Microsoft в последние годы финансировали прокладку подводных кабелей[19].

> Можно ли гарантировать надежность работы Интернета?
>
> Имеет ли глобальное сообщество пользователей Интернета право требовать от крупнейших интернет-провайдеров и телекоммуникационных операторов гарантий надежного функционирования критической инфраструктуры Интернета?
>
> На данный момент такой вид контроля не предусмотрен. Однако все идет к тому, что в будущем частные операторы интернет-инфраструктуры могут быть вынуждены соответствовать определенным требованиям общества.

Провайдеры услуг широкополосной связи и критическая инфраструктура

В начале 2008 г. в Средиземном море недалеко от Египта был поврежден один из основных кабелей, передающих интернет-трафик. Этот инцидент поставил под угрозу доступ к Интернету в обширном регионе, достигающем границ Индии. Два схожих инцидента произошли рядом с Тайванем и в Пакистане. Подобные события со всей ясностью демонстрируют, что инфраструктура Интернета — часть национальной и глобальной критической

инфраструктуры. Сбои в предоставлении интернет-услуг могут негативно сказаться на экономике и общественной жизни региона. Возможность нарушения работы Интернета ставит несколько вопросов

- Надежно ли защищены основные кабели, передающие интернет-трафик?
- Какова роль правительств государств, международных организаций и частных компаний в защите кабелей?
- Как мы можем снизить риски, связанные с возможным повреждением основных кабелей Интернета?

Протокол управления передачей / Интернет-протокол (TCP/IP)

Современное состояние

TCP/IP — основной технический стандарт, определяющий способ передачи данных по Интернету. Этот протокол основан на трех принципах:

- Пакетная коммутация: Сообщения дробятся на части небольшого размера — пакеты — и передаются в Интернете независимо друг от друга, а затем собираются в узле-приемнике.
- Сквозная передача данных: Это один из основных принципов работы Интернета, согласно которому действия и услуги, связанные с коммуникациями, происходят только при отправке и получении, тогда как при передаче сеть должна быть максимально нейтральной.
- Устойчивость к помехам: При отправке данных должны соблюдаться определенные условия, тогда как при приеме данных допускается определенная гибкость, чтобы получать информацию, которая не соответствует всем требованиям.

В вопросах управления Интернетом, связанных с протоколом TCP/IP, можно выделить два важных направления:

- внедрение новых стандартов,
- распределение IP-адресов.

Стандарты для TCP/IP устанавливаются Рабочей группой по проектиро-

ванию Интернета (IETF). Поскольку этот протокол имеет принципиальное значение для функционирования Интернета, он строго охраняется IETF. Любые изменения, вносимые в протокол TCP/IP, нуждаются в предварительном всестороннем обсуждении и подтверждении их эффективности для решения текущих проблем (принцип «работающего кода»).

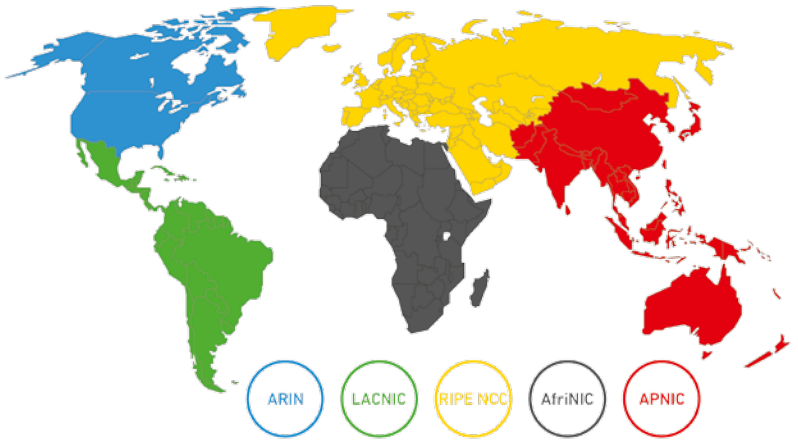


Рисунок 6. Региональные интернет-регистратуры

IP-адреса — это числовые адреса, которые должны иметь все компьютеры, подключенные к сети. Каждый адрес указывает на расположение объекта в сети посредством системы маршрутизации. Два компьютера, подключенные к Интернету, не могут иметь одинаковый IP-адрес.

Система распределения IP-адресов организована иерархически. «Наверху» находится Администрация по присвоенным именам в Интернете (Internet Assigned Numbers Authority, IANA), чьи функции на данный момент исполняет PTI, дочерняя структура ICANN[20]. PTI распределяет блоки IP-адресов между пятью региональными интернет-регистратурами[21]. Региональные интернет-регистратуры распределяют адреса между национальными и местными интернет-регистраторами, которые, в свою очередь, передают IP-адреса на более низкий уровень, небольшим интернет-провайдерам, компаниям и частным лицам.

Вопросы

Как преодолеть ограниченность IP-адресов: переход на протокол IPv6

На сегодняшний день при использовании введенного в 1983 г. IPv4 (интернет-протокола версии 4) общее количество IP-адресов составляет около 4 миллиардов. Изначально считалось, что этого будет достаточно для удовлетворения спроса на адреса. Однако в феврале 2011 г. IANA объявила, что блоков IP-адресов для распределения среди региональных интернет-регистратур больше нет.

Расход IP-адресов по IPv4 ускорился в последние годы в результате появления новых поколений устройств, подключенных к Интернету — таких как мобильные телефоны, карманные компьютеры, игровые приставки и бытовые электроприборы, а также в связи с ростом зоны покрытия. С развитием Интернета вещей вырос спрос на IP-адреса, поскольку каждому устройству Интернета вещей требуется собственный IP-адрес для подключения к Интернету. Озабоченность тем, что IP-адреса могут закончиться, что, в конечном счете, может помешать дальнейшему развитию Интернета, побудило техническое сообщество принять меры. В результате были осуществлены:

- Рационализация использования существующего запаса IP-адресов, что было достигнуто за счет использования технологии преобразования сетевых адресов (NAT), которая позволяет компьютерам частной сети (например, в рамках компании или организации) использовать для подключения к Интернету один адрес.
- Внедрение механизма бесклассовой адресации (Classless InterDomain Routing, CIDR) с целью приостановить расточительное распределение IP-адресов региональными регистратурами: схема работы, при которой один IP-адрес может обозначать большое количество уникальных IP-адресов (что делает распределение IP-адресов более экономным).
- Внедрение новой версии интернет-протокола, IPv6, которая предоставляет гораздо больший запас IP-адресов (более 340 000 000 000 000 000 000).

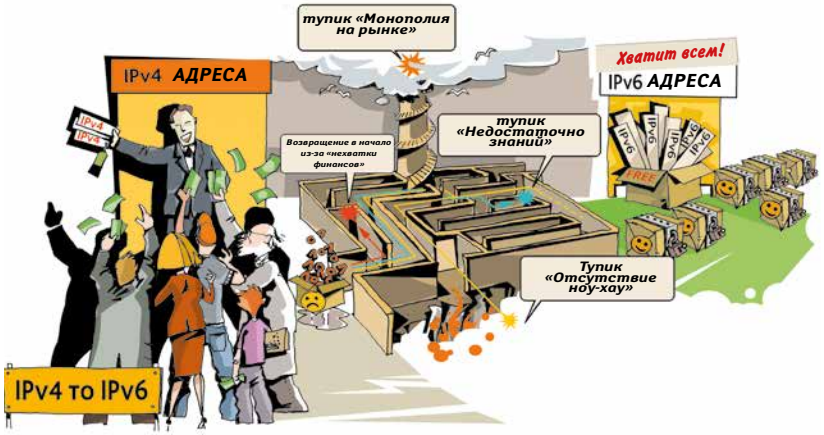


Рисунок 7. От IPv4 к IPv6

Действия технического интернет-сообщества в отношении потенциальной проблемы исчерпания IP-адресов представляют собой пример быстрого и упреждающего управления ситуацией. Технологии NAT и CIDR позволили преодолеть текущие сложности, однако оптимальным долгосрочным решением является переход на новую версию протокола IPv6.

Хотя IPv6 был разработан еще в 1996 г., его внедрение идет исключительно медленно. Не все осознают необходимость перехода, а также недостаток финансирования для инвестирования в новое оборудование в развивающихся странах (рис. 7). По мнению экспертов, если переход на IPv6 затянется, это может привести к так называемой технической фрагментации Интернета. В результате, Интернет по стандарту IPv4 будет существовать отдельно от Интернета по IPv6 из-за проблем с обратной совместимостью. В частности, об этом говорится в докладе, опубликованном в начале 2016 г. Всемирным экономическим форумом[22]. Согласно его авторам, всего лишь около 4% Интернета на тот момент времени использовало IPv6.

С технической точки зрения IPv4 и IPv6 могут сосуществовать. Большинство сетей, работающих на IPv6, поддерживают как адреса IPv6, так и IPv4. Тем не менее для гладкого перехода от одного протокола к другому необходимо задействовать ряд технических механизмов для обеспечения полноценной работы Интернета, сосуществования стандартов, преобразования

адресов и присвоения доменных имен. В разработанных IETF спецификациях по IPv6 описаны стратегии, инструменты и механизмы, которые могут обеспечить такой результат[23].

Политический план действий по переходу на IPv6, помимо проблем собственно перевода на новую версию протокола, должен решать проблемы справедливого распределения IP-адресов, для чего необходимо внедрение новых конкурентных механизмов, наилучшим образом удовлетворяющих потребности конечных пользователей. Даже с переходом на IPv6 проблема «искусственного» дефицита IP-адресов может снова появиться, если ответственные за их распределение на местном уровне организации, например, интернет-провайдеры, будут злоупотреблять своими полномочиями. В частности, они могут предоставлять IP-адрес только при условии приобретения других услуг, что сделает IP-адреса менее доступными и повысит их стоимость.

Переход с IPv4 на IPv6 подразумевает участие широкого круга заинтересованных лиц. Такие технические организации как IANA/PTI, региональные интернет-регистратуры и IETF должны обеспечить эффективное управление ресурсами IPv6 и разработать необходимые стандарты и характеристики по использованию IPv6. Интернет-провайдерам придется внедрить решения, обеспечивающие связь между IPv4 и IPv6, и сделать IPv6 доступным в своих сетях и услугах. Производители оборудования (операционных систем, сетевого оборудования и т. п.) и программисты (корпоративное ПО, смарт-карты и т. п.) должны будут обеспечить совместимость товаров и приложений с IPv6. То же самое касается поставщиков услуг для «информационного общества»[24].

Изменения в интернет-протоколах TCP/IP и кибербезопасность

Безопасность не входила в список важных вопросов для первых разработчиков Интернета в 1970-1980-х гг., поскольку в то время Интернет состоял из закрытой сети исследовательских институтов. Сейчас в мире три миллиарда интернет-пользователей. Глобальное распространение Интернета и его возрастающая коммерческая и общественная значимость привели к тому, что вопросы безопасности вышли на одно из первых мест в списке проблем управления Интернетом.

Хотя в IPv4 включена функция обеспечения сохранности IP-адресов

(IPSec), ее использование не является обязательным. В рамках IPv6 это требование стало обязательным, а IPSec стало неотъемлемой частью протокола, позволяя устанавливать подлинность, осуществлять шифрование и сжатие интернет-трафика без внесения изменений в какие-либо приложения[25].

С переходом на IPv6 можно снизить присущие протоколу IPv4 уязвимости с точки зрения безопасности, включая определение устройства, сохранность данных и конфиденциальность. Хотя в этих областях IPv6 обеспечивает более высокий уровень безопасности, из-за просчетов при его внедрении и конфигурации некоторые проблемы могут возникать даже чаще, чем при использовании IPv4[26]. Многие из этих проблем можно решить в ходе переходного периода. В частности, речь идет о недостаточной информированности о новом протоколе и непонимании его важности, зачастую препятствующих переходу компаний на IPv6[27].

Кроме того, некоторые опасаются, что IPv6 может ограничивать право на неприкосновенность частной жизни, поскольку каждому устройству, подключенному к Интернету, присваивается уникальный идентификатор. Однако такой идентификатор может быть не статичным, а динамичным, то есть время от времени меняться. Таким образом, многое будет зависеть от того, каким образом будет внедряться новый протокол.

Изменение TCP/IP и проблема ограниченной пропускной способности

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

В условиях постоянного развития сетевых технологий изменяется и характер проблем, о которых говорится в данном разделе. Техническое сообщество теперь задумывается о разработке интернет-протоколов нового

поколения, которые должны соответствовать реалиям постоянно меняющегося мира технологий. Например, в начале 2016 г. в рамках Европейского института по стандартизации в области электросвязи (ETSI) была создана рабочая группа, которой поручили «определить требования к протоколам нового поколения и сетевой архитектуре». Группа займется вопросами адресации, безопасности и аутентификации, требованиями к устройствам Интернета вещей, требованиями по распространению видео и материалов, а также требованиями в отношении интернет-торговли[28].

Система доменных имен (DNS)

Современное состояние

Система доменных имен (DNS) преобразует доменные имена (например, google.com — слова запоминаются легче, чем цифры) и превращает их в IP-адреса, которые компьютеры и другие устройства используют для идентификации интернет-ресурсов (упрощенная схема представлена на рис. 8).

С точки зрения инфраструктуры, DNS состоит из корневых серверов, серверов доменов верхнего уровня и множества DNS-серверов, расположенных в разных частях мира .

Домен верхнего уровня представляет собой верхний уровень иерархически организованной системы доменных имен. DNS включает в себя два типа доменов верхнего уровня. Первый тип — это так называемые родовые (или «общие» — gTLDs) домены; второй — национальные домены, основанные на кодах стран (ccTLDs). К родовым доменам верхнего уровня относятся такие адреса как .com, .info, .net, и .org, также появившиеся сравнительно недавно новые родовые домены верхнего уровня (с 2014 г.), например, .pub, .رازاب (bazaar), .rentals, .ngo или .游戏 (game). Если во многих родовых доменах верхнего уровня действует открытая регистрационная политика, что позволяет любому заинтересованному лицу или организации регистрировать доменные имена, существуют также родовые домены, предназначенные для определенных групп/секторов/сообществ. Например, регистрация в домене .aero доступна только участникам авиатранспортной отрасли, а в домене

.bank могут регистрироваться только уполномоченные банковские организации. Национальные домены верхнего уровня представляют двухбуквенные обозначения, отсылающие к конкретным странам или территориям (например, .uk — Соединенное Королевство, .cn — Китай, .br — Бразилия).

Рисунок 8. Система доменных имен (DNS)

Список адресов для каждого родового и национального домена верхнего уровня поддерживает регистратура (также именуется «координатор реестра»), главная обязанность которой заключается в том, чтобы осуществлять поддержку и администрирование базы данных всех доменных имен, зарегистрированных в соответствующем домене верхнего уровня. Например, администрированием домена .com занимается компания VeriSign, а домен .uk находится в ведении Nominet. Непосредственно регистрацией доменных имен конечных пользователей («администраторов») занимаются регистраторы. В большинстве случаев деятельность регистратуры и регистратора никак не пересекаются, однако есть исключения. Так, в некоторых национальных доменах координатор реестра может также выполнять функции регистратора. ICANN осуществляет общую координацию системы DNS:

- Координирует выделение и присвоение имен в корневой зоне DNS.
- Координирует разработку и претворение в жизнь политики регистрации доменных имен второго уровня в родовых доменах верхнего уровня.
- Содействует координированию работы и развитию корневых серверов DNS[30].

Подробнее о деятельности ICANN см. **Раздел 9.**

В случае с родовыми доменами верхнего уровня, ICANN заключает соглашения с регистратурами (на администрирование каждого родового домена верхнего уровня[31]) и занимается аккредитацией регистраторов[32]. Национальные домены верхнего уровня занимают особое положение, поскольку ICANN не устанавливает правила администрирования и управления такими доменами. Однако есть ряд регистратур национальных доменов верхнего уровня, которые заключили соглашения с ICANN (соглашение о подотчетности, меморандум о взаимопонимании или обмен письмами), основная цель которых заключается в том, чтобы оговорить принципы отношений сторон.

Вопросами оперативного управления системой DNS занимается PTI, подразделение ICANN.

Вопросы

Товарные знаки

Важным аспектом управления системой доменных имен является защита товарных знаков и разрешение споров. На заре Интернета регистрация доменных имен осуществлялась в порядке очередности по принципу «первым пришел — первым обслужен», что в результате породило явление, известное как киберсквоттинг: регистрация доменных имен с целью их последующей перепродажи владельцам прав на товарный знак. Единая политика

рассмотрения споров о доменных именах (Uniform Dispute Resolution Policy, UDRP), разработанная ICANN и Всемирной организацией интеллектуальной собственности (ВОИС), помогла существенно сократить количество случаев кибersквоттинга.

По вопросам интеллектуальной собственности см. ***Раздел 4.***

Неприкосновенность частной жизни и персональные данные

Соблюдение права на неприкосновенность частной жизни и защита персональных данных — еще один важный аспект управления системой DNS. Сейчас регистратуры ведут так называемые базы данных WHOIS, в которых приводится информация о зарегистрированных доменных именах, включая данные об администраторах доменов. Обеспечение открытого доступа к такой информации (имя, адреса электронной почты, почтовый адрес и т.п.) вызвало протест со стороны правозащитников, которые стали требовать изменения подхода к ведению базы WHOIS. Дискуссии по этому вопросу идут в ICANN на протяжении последних нескольких лет, и работа по изменению политики началась.

Создание новых родовых доменов верхнего уровня

В 2012 г. после шести лет консультаций и разработки новой политики ICANN запустила программу по новым родовым доменам верхнего уровня, открыв DNS для создания доменов помимо двадцати двух существовавших gTLD. В соответствии с этой программой, организация из любой страны могла подать заявку на работу в качестве регистратуры нового родового домена верхнего уровня, включая домены на алфавите, отличном от латинского, при условии соответствия ряду условий, изложенных в Руководстве по регистрации новых родовых доменов верхнего уровня. Появление новых gTLD было положительно встречено теми, кто воспринял эту программу как возможность активизировать конкуренцию и обеспечить потребителям более широкий выбор на рынке доменных имен. Другие заняли более осторожную позицию, в частности, по вопросу защиты товарных знаков в свете растущего числа gTLD, а также в связи с тем, что владельцам товарных знаков

пришлось регистрировать доменные имена во множестве доменов верхнего уровня, чтобы предотвратить случаи кибersквоттинга. Споры по вопросу о создании новых доменов продолжаются по сей день, но это не препятствует реализации программы. По состоянию на конец сентября 2016 г. в систему DNS было внесено 1186 таких доменов[33].

Однако споры о новых gTLD не ограничивались вопросами интеллектуальной собственности. Страны, представленные в Правительственном консультативном комитете (GAC) ICANN, обратили внимание на необходимость принимать меры, которые бы обеспечили защиту конечных пользователей и обеспечили конкуренцию при делегировании новых gTLD. Например, в отношении родовых доменов, представляющих регулируемые отрасли (таких как домены .bank и .pharm), страны предложили сделать так, чтобы регистрироваться в таких доменах могли только организации, обладающие необходимым разрешением на работу в соответствующей отрасли.

Еще одним камнем преткновения стала защита географических названий и обозначений: ICANN отказала компании Amazon (интернет-магазин) в регистрации домена .amazon, после того как страны Латинской Америки заявили о своем протесте в рамках GAC. Также в GAC серьезно дискутировался вопрос о делегировании доменов .wine/.vin. Швейцария и Франция собираются принять меры, которые будут препятствовать «неправомерной» регистрации доменных имен с указанием названий вин зарегистрированного географического происхождения (в некоторых юрисдикциях). Когда ICANN выделила консорциуму стран – членов Африканского союза домен .Africa, одна частная компания оспорила это решение.

Управление национальными доменами (ccTLD)

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

ми Палестинской автономии[34]. В оправдание своего решения о присвоении доменного имени .ps IANA сослалась на принцип регистрации доменных имен в соответствии со стандартом ISO 3166, как предлагал Джон Постел, один из «отцов-основателей» Интернета.

Второй вопрос: кто должен управлять национальными доменами? В настоящее время существует несколько моделей управления национальными доменами[35]. В некоторых случаях функции регистратуры исполняет государственное предприятие, например, надзорный орган страны в области телекоммуникаций, исследовательский институт при правительстве или государственный университет. Есть страны, где правила управления национальными доменами устанавливаются правительством, но функции управления делегируются частному сектору. В некоторых странах управлением национальными доменами занимаются частные компании без какого-либо вмешательства со стороны властей. Кроме того, существует ряд примеров регистратур национальных доменов, управление которыми осуществляется на многосторонней основе представителями различных групп заинтересованных лиц[36].

На заре Интернета власти не проявляли особого интереса к национальным доменам верхнего уровня. Однако постепенно ситуация изменилась. В некоторых странах власти решили установить контроль над национальными доменами, считая их национальным достоянием. Для этого был использован широкий набор политических подходов[37]. Передача новому институту права управления национальным доменом («переделегирование») одобряется ICANN только в том случае, если внутри страны был достигнут консенсус между всеми заинтересованными сторонами.

Третий вопрос связан с тем, что, в отличие от родовых доменов gTLD, ICANN не требует соблюдения каких-либо правил в вопросе о том, кто и как должен управлять национальными доменами ccTLD. ICANN ограничивается делегированием или переделегированием национальных доменов в соответствии с руководящими принципами, которые предусматривают наличие у регистратуры национального домена технических навыков для управления доменом и поддержку со стороны местного сообщества[38].

В 2005 г. Правительственный консультативный комитет (GAC) при ICANN принял Принципы и руководство GAC относительно делегирования и управления национальными доменами верхнего уровня[39], которые призваны регулировать отношениями между властями стран, национальными доменами и ICANN. Одним из основных, но не обязательных, принципов является субсидиарность. В соответствии с этим принципом, «политика управления национальными доменами верхнего уровня устанавливается местными властями, если только не доказано, что этот вопрос имеет международное значение и должен быть урегулирован на международном уровне».

Как было сказано ранее, ряд регистратур национальных доменов (в частности, в Бразилии, Чили, Голландии, Швеции и Соединенном Королевстве) заключили соглашения с ICANN, в которых изложены основные принципы их отношений. Многие регистратуры входят в Организацию поддержки национальных доменных имен (ccNSO) в рамках ICANN, в компетенцию которой входит разработка политики и консультирование Совета директоров ICANN по ряду вопросов, связанных с национальными доменами (например, ввод интернационализированных доменных имен – IDN). Некоторые регистратуры ccTLD не стремятся стать частью системы ICANN (в сентябре 2016 г. в ccNSO насчитывался 161 член, при этом в мире на тот момент существовало 240 национальных доменов верхнего уровня).

Некоторые операторы доменов создали организации регионального уровня (CENTR в Европе, AFTLD в Африке, APTLD в Азии, LACTLD в Южной Америке).

Интернационализированные доменные имена (IDN)

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

После долгих испытаний и политических споров в мае 2010 г. ICANN приступила к утверждению доменов верхнего уровня на разных языках, включая китайский, арабский и кириллицу. Интернационализированные доменные имена (IDN) появились в ряде стран и территорий в качестве эквивалентов национальным доменам верхнего уровня на латинице. Например, в Китае в дополнение к .cn появился .中国, а в России домен .ru был дополнен доменом .рф. Интернационализированные доменные имена также входят

в программу по созданию новых родовых доменов верхнего уровня, что позволяет регистрировать новые gTLD не только на латинице, но и с использованием других знаков. Например, теперь можно регистрировать доменные имена в доменах .сайт и .онлайн.

Появление IDN считается одним из главных успехов в области управления Интернетом. Однако пока не решены определенные технические сложности, связанные, в частности, с возможностью написания адреса электронной почты буквами любого алфавита. Дело в том, что домен верхнего уровня, указанный в адресе электронной почты, может уже быть интернационализированным доменным именем, тогда как начало адреса, то есть часть до знака @, должна все равно быть написана на латинице. Также сохраняются проблемы с распознанием IDN поисковыми системами. Помимо проблем технического характера, которыми занимаются специализированные группы в рамках ICANN, пока что IDN используется не очень широко. Для дальнейшего распространения интернационализированных имен необходимо повышать осведомленность о наличии такой возможности в странах, не использующих латиницу. Еще одним приоритетом должно быть создание услуг и контента для этих доменов.

Корневая зона и корневые серверы

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

Современное состояние

Чтобы проанализировать функции и надежность системы DNS, рассмотрим беспокоящую многих ситуацию, при которой корневые серверы будут отключены, и Интернет перестанет функционировать.

Занимая самое верхнее положение в иерархической структуре системы доменных имен, корневая зона представляет собой файл, содержащий перечень имен и IP-адресов всех доменов верхнего уровня, как gTLD, так и ccTLD, в системе DNS[40]. Управлением корневой зоной занимается PTI, дочернее предприятие ICANN, которому доверено исполнение функций IANA. PTI назначает операторов доменов верхнего уровня и ведет базу данных с их техническими и административными данными. Поддержкой и обновлением файла корневой зоны занимается VeriSign. Изначально эти функции исполнялись на основании соглашения о сотрудничестве между VeriSign и властями США. В рамках передачи функций обслуживания корневой зоны IANA это соглашение было заменено соглашением между ICANN и VeriSign.

Корневая зона DNS обслуживается корневыми серверами, которые также называют полномочными серверами, где хранятся копии файла корневой зоны. Мнение о том, что существует 13 корневых серверов, ошибочно. На самом деле, корневых серверов сотни[41], и найти их можно по всему миру. Цифра 13 связана с 13 разными именами главного узла[42]. В силу технических ограничений при проектировании DNS, их может быть только 13. Двенадцать организаций (6 научных и государственных институтов, 3 компании и 3 государственных учреждения) обеспечивают наличие последней версии файла корневой зоны на всех серверах.

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.

К тому же систему корневых серверов существенно укрепляет технология Anycast[43], копирующая содержимое этих серверов по всему миру. Такая структура дает массу преимуществ, включая повышенную надежность системы DNS и более быстрое получение информации об интернет-адресах (благодаря схеме Anycast выбирает ближайший к конечному пользователю сервер).

Таким образом, копии файла корневой зоны хранятся на сотнях доменных серверов, что делает внезапный и бесповоротный сбой в работе Интернета невозможным. 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.

Как уже было сказано, ведением и обновлением файла корневой зоны занимается VeriSign. Например, при согласовании нового родового домена верхнего уровня со стороны ICANN соответствующая информация передается VeriSign, которая вносит необходимые изменения в корневую зону (вносит новый родовой домен верхнего уровня в корневую систему) и предоставляет обновленный файл корневой зоны корневым серверам.

Вопросы

Альтернативные корневые серверы — возможности и ограничения

А почему ICANN обладает исключительным правом определять список доменов верхнего уровня и то, как они преобразуются в IP-адреса? Разве нет никаких альтернатив существующей системе DNS? Действуя по поручению IANA, ICANN через свое дочернее предприятие PTI осуществляет эксплуатацию и администрирование официальной корневой системой DNS, которая используется большинством интернет-пользователей для преобразования доменных имен в IP-адреса. Однако существуют организации, которые предлагают альтернативные корневые системы DNS (Alt Roots). Такие организации предлагают свой набор доменов верхнего уровня, который обычно существенно отличается от перечня доменов ICANN, но для их использования пользователям нужно изменить свои сетевые настройки, чтобы перейти с универсальных на альтернативные корневые серверы. Одним из первых альтернативных корневых серверов стал основанный в 1995 г. AlterNIC, который действовал до создания ICANN в 1998 г.

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.

В настоящее время существует целый ряд альтернативных DNS серверов, включая Google DNS, Open DNS, Advantage DNS и ScrubIT[44].

В 2015 г. появился еще более амбициозный проект под названием Yeti DNS Project, суть которого заключается в «создании параллельной экспериментальной корневой системы DNS по протоколу IPv6, чтобы выявить пределы работы корневой системы DNS»[45].

Создание альтернативного корневого сервера не является технически сложной задачей. Основной вопрос заключается в том, сколько «последователей» будет у альтернативного сервера, или, точнее, сколько компьютеров в Интернете будет обращаться к нему с запросами. Без пользователей альтернативная система DNS теряет смысл.

Концептуальный спор: единая корневая система против альтернативной

На протяжении долгого времени принцип единой корневой системы считался одним из основных и незыблемых постулатов в области управления Интернетом, который не подлежал ни пересмотру, ни даже обсуждению. Против идеи создания альтернативы единой системе выдвигались различные аргументы. Один из них состоит в том, что в существующей системе использование DNS властями страны в целях цензуры невозможно. Однако этот довод не состоятелен. Властям не нужен контроль над системой DNS или файлом корневой зоны для введения цензуры. Они могут использовать более действенные инструменты, основанные на фильтрации интернет-трафика.

Более убедительным представляется аргумент, согласно которому появление любой альтернативной корневой системы может привести к фрагментации, а то и распаду Интернета. Несмотря на то, что во всех корневых системах используется одна система IP-адресов, подходы к их присвоению и трансформации различаются. Так, если в нескольких корневых системах может появиться одно и то же доменное имя, оно может быть преобразовано в разные IP-адреса. Поскольку большинство альтернативных корневых систем не совместимы между собой или с системой ICANN, их сосуществование нарушит принцип «универсальной разрешимости», согласно которому должен быть только один способ передачи доменного имени с помощью IP-адреса, если только альтернативные системы не будут использоваться исключительно в личных целях и не будут общедоступными. С точки зрения системы DNS, это может мешать связи между различными частями Интернета. Фрагментация Интернета может создать угрозу для основной функции сети как единой глобальной коммуникационной системы. Насколько реальна эта угроза?[46]

Сетевой нейтралитет

Своим успехом Интернет во многом обязан принципу сетевого нейтралитета. С самых первых дней работы всемирной паутины весь интернет-трафик передавался на одних условиях и без какой-либо дискриминации, вне зависимости от того, исходил ли он от стартапа или от крупной компании. Новым компаниям и первопроходцам не нужно было получать разрешения или обладать авторитетом для того, чтобы внедрять свои инновации в Интернете. С развитием и распространением новых цифровых услуг, в частности, сервисов, требующих высокой скорости передачи данных, например, потокового видео высокого разрешения, некоторые интернет-компании (телекоммуникационные компании и интернет-провайдеры) стали отдавать предпочтение определенным видам трафика, например, своим собственным услугам или услугам своих деловых партнеров, исходя из коммерческих соображений. Такой подход они оправдывали необходимостью финансировать дальнейшее развитие интернет-услуг. Сторонники сетевого нейтралитета решительно осудили такую политику. По их мнению, это нарушает принцип свободного доступа к информации и свободы в Интернете и препятствует инновациям.

Сетевой нейтралитет имеет огромное значение. В дискуссию о сетевом нейтралитете включился широкий круг участников, от президента США Барака Обамы до рядовых правозащитников. Решение этого вопроса может сыграть определяющую роль в развитие Интернета.

Современное состояние

Важно понимать, что понятия сетевого нейтралитета и управления сетевым трафиком не тождественны. Технологии управления сетевым трафиком использовались еще со времен использования коммутируемого подключения через модем для того, чтобы решить проблему несоответствия доступной пропускной способности потребностям пользователей. Для обеспечения высокого качества обслуживания операторы (телекоммуникационные компании и интернет-провайдеры), которых также часто называют поставщиками, применяли различные методы управления трафиком, позволяющие отдавать приоритет определенным видам трафика. Например, интернет-трафик IP-телефонии (Skype) может обладать приоритетом по отношению к отправке сообщений по электронной почте, поскольку любые задержки при голосовой связи заметны в отличие от незначительных задержек во время переписки по электронной почте.

Управление интернет-трафиком имеет особое значение в настоящее время в связи с растущим спросом на услуги, требующие высокоскоростного подключения. Так, все больше пользователей регулярно делает звонки и видеозвонки по Интернету (Skype, Google Hangout, видеосвязь), играют в сетевые игры, смотрят телепередачи и фильмы с высоким разрешением (например, через Hulu или Netflix). Большое значение решения по управлению интернет-трафиком имеют и в области беспроводной связи, что объясняется ростом числа мобильных устройств, а также техническими ограничениями радиочастотного спектра[47]. При этом эти решения становятся все более сложными и технически совершенными. Они призваны распределять интернет-трафик таким образом, чтобы обеспечить высокое качество связи, предотвращать перегрузку, задержки и искажения.

Первым спорным моментом в проблеме сетевого нейтралитета является вопрос о том, допустимо ли в принципе управление интернет-трафиком. Приверженцы строгого соблюдения принципа сетевого нейтралитета считают, что «все единицы информации равны», и не следует отдавать предпочтение каким-либо видам интернет-трафика. Против такой точки зрения выступили телекоммуникационные компании и интернет-провайдеры, указав на необходимость обеспечения равенства при доступе пользователей к интернет-услугам, что делает обращение со всеми видами трафика на равных условиях невозможным. Например, если видеотрафик и электронная почта будут доставляться на равных условиях, пострадает качество проигрывания потокового видео, а секундные задержки при доставке писем по электронной почте останутся незамеченными. Против этого не могут возразить даже адепты строгого нейтралитета.

Вопросы

Участники спора о сетевом нейтралитете постепенно пришли к выводу, что управлять трафиком все же нужно. Главный вопрос заключается в том, в ка-

кой степени такое регулирование допустимо. Помимо вопросов технического характера, предметом самых жарких споров стали экономический и правозащитный аспекты дискуссии об управлении трафиком и сетевом нейтралитете.

Экономическая составляющая

В последние несколько десятилетий многие крупные сетевые операторы, в том числе телекоммуникационные компании и интернет-провайдеры, изменили свои модели ведения бизнеса. Помимо предоставления доступа в Интернет для домохозяйств и корпоративных клиентов, они стали предлагать услуги IP-телефонии и IP-телевидения, услугу «видео по запросу», порталы по скачиванию музыки и видео и т. д. Теперь такие компании конкурируют не только между собой, стараясь опередить соперников по стоимости, качеству и скорости подключения к интернету, но и с компаниями в сегменте OTT — контент- и сервис-провайдерами, такими как Google, Facebook, Netflix и Skype.

Управление трафиком в контексте оказания услуг или предоставления контента в Интернете может стать эффективным инструментом конкурентной борьбы. Для этого необходимо передавать определенные пакеты данных в приоритетном порядке в соответствии с коммерческими предпочтениями компании. Так, оператор может замедлить или полностью перекрыть интернет-трафик, исходящий от конкурента (например, Skype и Google Voice), в своей сети, при этом обеспечив приоритет пакетам данных своей собственной услуги (IP-телефония или интернет-телевидение)[48].

В то же время операторы отмечают необходимость наращивания инфраструктурных инвестиций в связи с ростом запросов к пропускной способности интернет-соединений, что в основном связано с распространением услуг OTT. По их мнению, поскольку операторы сегмента OTT больше других нуждаются в наличии высокоскоростного подключения и извлекают наибольшую выгоду из развития инфраструктуры, создание многоуровневой модели, в которой такие провайдеры взяли бы на себя часть затрат, гарантировало бы высокое качество услуг для клиентов OTT сегмента. Это еще один пример управления интернет-трафиком из экономических, а не технических соображений.

В стремлении увеличить доходы телекоммуникационные компании стали разрабатывать новые модели ведения бизнеса и обслуживания. Например, мобильные операторы предлагают безлимитный (бесплатный) трафик при использовании определенных приложений или услуг. В некоторых тарифах трафик, потраченный при использовании таких приложений или услуг, не учитывается в общем трафике абонента. В некоторых случаях пользователи могут получить доступ к определенным услугам, даже не оформляя подписку на какой-либо пакет услуг. Несмотря на растущую популярность такой модели обслуживания по всему миру, она вызывает достаточно много нареканий. С одной стороны, она приносит особую пользу в развивающихся и наименее развитых странах, где стоимость услуг мобильного Интернета значительно превышает средний доход. Один из основных аргументов в пользу предоставления бесплатного доступа к определенным видам трафика заключается в снижении стоимости доступа к информации в Интернете (по тарифу) и обеспечивает частичный доступ к Интернету пользователям, не имеющим средств для оформления подписки на тариф (при условии предоставления бесплатного доступа). Сторонники такой модели утверждают, что доступ хоть к какой-нибудь информации лучше отсутствия всякого доступа. Кроме того, предоставление пользователям бесплатного доступа к некоторым видам приложений может способствовать спросу на доступ к Интернету, что может побудить операторов инвестировать в строительство и развитие инфраструктуры.

С другой стороны, противники такого подхода утверждают, что бесплатный трафик для определенных услуг и приложений дает им приоритет по сравнению с другими, что нарушает принцип сетевого нейтралитета, препятствует конкуренции и инновациям. Некоторые даже высказывали опасения, что такая модель может нарушать права пользователей, а именно право на получение информации (в качестве части права свободно выражать свое мнение).

Споры о такой модели обслуживания разгорелись с новой силой в 2014 г. с появлением услуги Free Basics, разработанной компанией Facebook для рынка развивающихся и наименее развитых стран. Эта услуга дает абонентам мобильной связи возможность пользоваться такими приложениями, как Wikipedia и AccuWeather (и Facebook) в добавление к оплаченному интернет-трафику. В результате развернувшейся дискуссии в некоторых странах (включая Индию и Египет) услуга была отключена.

В то же время, помимо предоставления бесплатного доступа к определенным услугам, телекоммуникационные компании также предлагают «специализированные услуги», которые предоставляются сейчас или могут появиться в будущем, и требуют высокоскоростного соединения и, таким образом, особого режима управления трафиком. Например, это может быть потоковое видео высокого разрешения или электронная медицина.

Вот уже многие годы центральное место в спорах о сетевом нейтралитете занимают предложения по созданию многоуровневого Интернета. Одним из них стал проект «Открытый Интернет»[49], с которыми выступили компании Verizon и Google в 2010 г. В проекте предлагается вынести коммерческие услуги на уровень «дополнительных интернет-услуг». По утверждению сторонников такой модели, этот подход обеспечит более широкий выбор для пользователей и будет способствовать инвестициям в развитие инфраструктуры. Противники такой идеи опасаются, что это приведет к отказу от политики «негарантированной доставки» (best effort), поскольку на «экономическом» и «коммерческом» уровнях обслуживания предполагается использовать одни и те же каналы (например, сети беспроводной и проводной связи).

В то же время, работа Интернета меняется под влиянием рынка. Чтобы снизить стоимость передачи данных и повысить скорость, контент-провайдеры решили приблизиться к своим пользователям за счет создания «сетей доставки контента» (Content Delivery Networks – CDN), то есть буферных серверов, расположенных невдалеке от региональных точек обмена интернет-трафиком или при крупных региональных телекоммуникационных компаниях. Это позволяет улучшить качество работы сети и снизить издержки. Изначально только крупные контент-провайдеры могли позволить себе создание CDN и нуждались в таком решении. Однако с появлением дата-центров и услуг облачного хранения, это решение стало доступно всему рынку. Таким образом, используя облачное хранение, любой может арендовать CDN для обслуживания пользователей по всему миру.

Многоуровневый Интернет

В настоящее время доставка интернет-трафика осуществляется по принципу «негарантированной доставки», то есть без гарантии определенного качества обслуживания, скорости или времени доставки пакетов данных. В сетях такого типа пользователи совместно используют доступные пропускные способности, в результате чего скорость соединения (битрейт) может меняться в зависимости от загрузки в соответствующий момент времени[50]. Соответственно, управление трафиком играет важную роль с точки зрения качества обслуживания конечных пользователей.

Концепция многоуровневого Интернета заключается в создании «коммерческого» уровня, под которым понимается совокупность особых услуг, качество которых гарантировано. Сторонники такого подхода считают, что такой уровень мог бы работать параллельно с «экономическим» уровнем (Интернет в его существующем виде), который продолжит работать в соответствии с принципом «негарантированной доставки». Компании OTT сегмента получат возможность выбирать, распространять ли свои услуги на коммерческом уровне за плату или бесплатно в сетях с негарантированной доставкой.

Правозащитная проблематика

Последствия отказа от принципа сетевого нейтралитета будут не только экономическими. Интернет превратился в один из столпов современного общества и гаранта соблюдения основных прав человека, включая доступ к информации, свободу выражения мнений, право на услуги здравоохранения и образования. Таким образом, отход от концепции открытого Интернета может привести к ущемлению основных прав.

Кроме того, появление возможности управлять сетевым трафиком в зависимости от его источника или назначения, услуги или контента может дать властям возможность отфильтровывать интернет-трафик предосудительного или нежелательного содержания с точки зрения политических, идеологических, религиозных, культурных и иных ценностей. Это может привести к тому, что управление интернет-трафиком станет орудием политической цензуры.

Пользователи или клиенты?

Споры по теме сетевого нейтралитета сопровождаются терминологической дискуссией. Сторонники сетевого нейтралитета чаще говорят о «пользователях» Интернета, тогда как другие участники спора, в первую очередь компании, предпочитают использовать слово «клиент». Интернет-пользователей нельзя считать просто клиентами. Термин «пользователь» подразумевает активное участие в развитии Интернета при помощи социальных сетей, ведения блогов и другими способами, а также участие в определении будущего Интернета. С другой стороны, в области интернет-услуг, как и в любой другой сфере, клиенты могут решать, приобретать ли предложенные услуги или нет. Основой их статуса в Интернете является контракт с интернет-провайдером и правила защиты прав потребителей. Что касается работы Интернета, то в этих вопросах клиенты участвовать не должны.

Основные участники и их аргументы

Позиции основных участников спора о сетевом нейтралитете постоянно меняются. В число наиболее активных сторонников сетевого нейтралитета входят защитники прав потребителей, некоторые технологические компании и многие крупные интернет-компании, включая Google, Yahoo!, Vonage, eBay, Amazon, EarthLink, а также разработчики программного обеспечения, такие как Microsoft.

К противникам сетевого нейтралитета относятся крупнейшие телекоммуникационные компании, интернет-провайдеры, производители сетевого оборудования и аппаратного обеспечения, создатели видеоконтента и мультимедийные компании. В основе их аргументации против регулирования интернет-трафика лежат принципы рыночной экономики и удовлетворение запросов потребителей. Несмотря на то, что телекоммуникационные операторы обычно выступают против любых правил в области сетевого нейтралитета,

Европейская ассоциация сетевых операторов (European Telecommunications Network Operators — ETNO) на Всемирной конференции по международной электросвязи WCIT-12 потребовала на международном уровне запретить странам принимать меры по обеспечению сетевого нейтралитета. Однако их коллеги из компания Verizon в США выступили против такой инициативы[51].

Четыре аргумента в споре о сетевом нейтралитете приводятся в Таблице 1.

Таблица 1. Основные аргументы в споре о сетевом нейтралитете

Аргумент	Сторонники сетевого нейтралитета	Противники сетевого нейтралитета
Прошлое/ настоящее	Новые интернет-компании появились благодаря открытой архитектуре Интернета, пользователям выгодны инновационные разработки и разнообразные услуги, ставшие доступными благодаря сетевому нейтралитету. Сетевой нейтралитет сохранит архитектуру Интернета, обеспечивающую стремительное и прорывное развитие Интернета.	Управление трафиком неизбежно, а настоящего нейтралитета никогда не было. Кроме того, уже существуют услуги, не соответствующие принципу сетевого нейтралитета, например, частные виртуальные сети (VPN). Без ограничений, связанных с соблюдением сетевого нейтралитета, интернет-компании смогут создавать новые услуги для своих клиентов с гарантированным качеством обслуживания.
Экономика	Отказ от сетевого нейтралитета превратит Интернет в систему, подобную кабельному телевидению, когда горстка крупных компаний контролирует доступ и распространение контента и решает, что смотреть пользователям и сколько это стоит. Возможности для роста новых компаний и небольших предприятий, в частности, в развивающихся странах, будут закрыты. Поставщики сегмента OTT уже выплачивают телекоммуникационным компаниям огромные суммы за доступ к Интернету и инвестируют в развитие инфраструктуры, например, в создание буферных серверов.	Без предусмотренных сетевым нейтралитетом ограничений в соглашениях с поставщиками контента и услуг, телекоммуникационные компании увеличат свои доходы и смогут увеличить инвестиции в развитие инфраструктуры. Развитие инфраструктуры будет способствовать появлению новых услуг и инновационных решений, отвечающих запросам потребителей, что пойдет на пользу всем. Поставщики сегмента OTT также выиграют от инновационных решений на основе качественных услуг, если будут сняты ограничения, связанные с сетевым нейтралитетом.
Этика	В создании Интернета принимало участие большое число добровольцев, они же обеспечивали его развитие на протяжении многих лет. Они не жалели времени и усилий на разработку всех аспектов Интернета, от протоколов до контента. Интернет – не просто бизнес, это часть глобального человеческого наследия. Нельзя допустить, чтобы плодами работы сотен и тысяч талантов воспользовалась горстка компаний, которые откажутся от сетевого нейтралитета и сделают Интернет частью своих бизнес-проектов. Таким образом, творческим вкладом большой группы людей воспользуются единицы.	Принцип сетевого нейтралитета вызывает вопросы с точки зрения этики: операторы инвестируют в обслуживание и расширение инфраструктуры Интернета для создания новых услуг, а всеми преимуществами от развития Интернета пользуются компании, работающие с контентом, включая Google, Facebook и Amazon.
Регулирование	Власти должны обеспечить сетевой нейтралитет в интересах общества. При любой форме саморегулирования операторы найдут возможность нарушить этот принцип. Рыночные механизмы неэффективны, поскольку крупные телекоммуникационные компании контролируют основные инфраструктуры Интернета. Даже при наличии выбора этот принцип реализуется не всегда, поскольку пользователи должны знать технические и правовые аспекты этой проблемы и осознавать последствия своих решений.	Интернет развивался в условиях минимального регулирования либо полного отсутствия контроля. Жесткое государственное регламентирование затормозит творческий процесс и развитие Интернета. В основе рынка лежит свобода выбора. Если пользователи недовольны обслуживанием, они могут сменить провайдера. Возможность выбора и рыночные механизмы вытеснят с рынка некачественные предложения и обеспечат успех добросовестных поставщиков услуг.

Основные принципы

В последние годы в центре политических споров и внимания регуляторов находились следующие ключевые составляющие концепции сетевого нейтралитета[52]:

- Прозрачность: Операторы обязаны предоставлять полную и точную информацию о подходах к управлению сетью, возможностях и качестве обслуживания в понятной для обычного пользователя форме.
- Доступ: Пользователи должны обладать [неограниченным] доступом к любому [законному] контенту, услугам и приложениям [с минимальной гарантией доставки в соответствии с указаниями регулятора] и возможностью подключать любую аппаратуру, которая не наносит вреда сети.
- Отказ от дискриминации: Операторы обязаны предотвращать любые случаи дискриминации [или допускать дискриминацию в разумных пределах] в отношении трафика по следующим признакам:
  - происхождение получателя или отправителя;
  - вид контента, приложения или услуги [в соответствии с принципом честной конкуренции: отказ от дискриминации в отношении неугодных конкурентов или услуг OTT-провайдеров];
  - под словом «разумный» понимается любая деятельность, приносящая общественную пользу (обеспечение качества обслуживания, безопасность или устойчивость сети, содействие инновациям и инвестициям, снижение издержек и т. п.) и не преследующая исключительно коммерческие цели.

На международных форумах, включая глобальный Форум по управлению Интернетом и Европейский диалог об управлении Интернетом (EuroDIG), также обсуждаются следующие вопросы:

- Защита свободы выражения мнений, права доступа к информации и выбора.
- Обеспечение минимального качества обслуживания, безопасности и устойчивости сети.
- Сохранение стимулов для инвестиций.
- Содействие инновациям [включая возможности для создания новых бизнес-моделей и инновационных компаний, в том числе появление новичков].
- Определение прав, распределение ролей и обеспечение подотчетности всех задействованных сторон (провайдеры, регуляторы и пользователи), включая право на апелляцию и возмещение.
- Предотвращение действий по подрыву свободной конкуренции.
- Создание рыночной среды, которая бы позволяла пользователям без особых сложностей выбирать и менять сетевого оператора.
- Защита интересов пользователей, находящихся в неблагоприятных условиях, включая инвалидов, а также пользователей и компаний из развивающихся стран.
- Обеспечение разнообразия контента и услуг.

Политические подходы

В ходе спора о сетевом нейтралитете на первый план вышел еще один вопрос: какова роль законодательной власти и регуляторов в отношении услуг широкополосного доступа и деятельности операторов? Одна из основных проблем, с которой столкнулись регуляторы, заключается в том, следует ли действовать упреждающе для предотвращения возможных нарушений принципа сетевого нейтралитета или реагировать по факту, когда нарушение уже имело место. Политикам и регуляторам также необходимо решить, следует ли прибегать к инструментам «жесткого права», то есть оформлять соответствующие положения на законодательном уровне, или ограничиться «мягким правом» (руководства и регламенты)[53].

Развитые страны

В США Федеральная комиссия по связи (Federal Communications Commission – ФКС) приняла серию регламентов, обеспечивающих соблюдение сетевого нейтралитета. Эти правила вступили в силу в июне 2015 г. Они дают возможность ФКС регулировать услуги широкополосного доступа, как если бы это была одна из коммунальных услуг, и вводят запрет для операторов проводной и беспроводной связи прибегать к неразумным подходам, которые, по мнению ФКС, могут нарушить принцип открытости Интернета. Речь идет о таких действиях, как блокирование законного контента, приложений, услуг и устройств; создание помех при передаче законного интернет-трафика или снижение качества передачи в зависимости от контента, приложения или услуги (регулирование скорости); приоритетная передача определенных видов контента, приложений или услуг за плату[54]. Телекоммуникационные операторы оспорили эти правила в суде, заявив, что они отри-

цательно скажутся на их инновационной деятельности и инвестициях в развитие инфраструктуры. Хотя в июне 2016 г. федеральный апелляционный суд отклонил их доводы[55], провайдеры, скорее всего, продолжат бороться с правилами ФКС.

В ЕС в ноябре 2015 г. был принят Регламент по открытому доступу в Интернет (Regulation on open Internet access), согласно которому интернет-провайдеры обязаны относиться к любому трафику одинаково при предоставлении доступа к интернет-услугам без какой-либо дискриминации, ограничений или вмешательства, и безотносительно тому, кто отправляет, получает контент, кто получает к нему доступ или распространяет его, какие приложения или услуги используются и с помощью какого оборудования[56]. В этом регламенте также фигурирует концепция «специализированных услуг», согласно которой операторы могут «оказывать не только услуги интернет-доступа, но и другие услуги, оптимизированные под определенный контент, приложения или услуги или их сочетание, и требующие оптимизации для обеспечения определенного уровня качества при использовании контента, приложений или услуг»[57]. В августе 2016 г. Совет европейских регуляторов рынка электронной связи (BEREC) опубликовал рекомендации национальным регуляторам о том, как следует исполнять регламент ЕС. В частности, речь идет о тщательном мониторинге и обеспечении «соблюдения правил, гарантирующих передачу трафика на равных условиях без дискриминации при оказании услуги доступа в Интернет и соблюдения прав конечных пользователей»[58].

В Бразилии[59], Чили[60], Словении[61] и Голландии[62] соблюдение сетевого нейтралитета гарантировано на законодательном уровне. В Норвегии власти сделали выбор в пользу «мягкого регулирования»: национальный регулятор подготовил рекомендации по сетевому нейтралитету (в сотрудничестве с представителями отрасли, включая интернет-провайдеров, отраслевые организации, контент-провайдеров и ассоциаций по защите прав потребителей)[63].

Развивающиеся страны

В силу инфраструктурных ограничений и недостаточной пропускной способности в развивающихся странах их регуляторы уделяют основное внимание вопросу справедливого использования, в частности, проблемам

доступности цен и обеспечения равноправного доступа для всех. Некоторые страны настаивают на необходимости отказа от трансграничной дискриминации. По их мнению, трафик должен доставляться на равных условиях вне зависимости от того, из какой страны он исходит. Кроме того, в ряде стран немалое внимание уделяется культурным, политическим и этическим аспектам, что приводит к различиям в трактовке понятий «надлежащего» и «ненадлежащего» использования.

Также высказываются опасения, что внедряемые в развитых странах инновационные модели могут негативно сказаться на развивающихся рынках. Предоставление приоритета крупным интернет-компаниям станет существенной преградой для новых компаний и конкурентов, угрозой для инноваций, местного контента и услуг, а также разнообразия средств информации. Как упоминалось ранее, некоторые страны активно проводят политику сетевого нейтралитета и запрещают предоставлять бесплатный доступ к определенным видам контента или приложений. Другие меры касаются предоставления национальным телекоммуникационным компаниям права взимать плату с международных OTT-провайдеров за приоритетное обслуживание, что увеличивает доходы действующих телекоммуникационных операторов. Можно также пойти в противоположном направлении и гарантировать соблюдение принципа сетевого нейтралитета на законодательном уровне, чтобы привлечь OTT-операторов в страны за пределами США.

Международные организации и НПО

Многие международные организации и ассоциации интернет-пользователей также сформулировали свою позицию по вопросу о сетевом нейтралитете. В Декларации Комитета министров Совета Европы о сетевом нейтралитете 2010 г. и Рекомендациях Комитета министров по защите прав на свободу выражения мнений и неприкосновенность частной жизни применительно к сетевому нейтралитету 2016 г. подчеркивается важность соблюдения таких основных прав, как свобода выражения мнений и право на информацию[64]. Организация «Общество Интернет» (Internet Society, ISOC) ставит во главу угла интересы потребителя и придает особое значение таким вопросам, как обеспечение свободы выражения мнений, право выбора и предотвращение

дискриминации[65]. Форум «Трансатлантический потребительский диалог» (Trans Atlantic Consumer Dialogue — TACD), в котором принимают участие организации по защите прав потребителей из США и ЕС, также требует отказа от дискриминации в отношении операторов, призывая США и ЕС отстаивать принципы открытости и нейтралитета Интернета[66]. Большое внимание вопросам сетевого нейтралитета и создания многоуровневого Интернета было уделено в рамках WCIT-12. Сетевой нейтралитет не был включен в число согласованных принципов, изложенных в Итоговом документе конференции NETmundial 2014 г., однако дискуссии по этому вопросу были продолжены, в том числе в рамках Форума по управлению Интернетом.

Особую озабоченность у неправительственных организаций вызывает будущее некоммерческого контента и услуг. Они требуют, чтобы в любых сетях такой трафик передавался на тех же условиях, что и коммерческий контент и услуги. НПО также подчеркивают важность соблюдения прав социально обездоленных групп, в особенности людей с ограниченными возможностями, на использование без каких-либо ограничений контента, услуг и приложений (включая требующих высокоскоростного доступа).

Нерешенные вопросы

В споре о сетевом нейтралитете все еще много нерешенных вопросов:

- Как найти баланс между преимуществами, которые дает Интернет обществу, и правами пользователя (человека), с одной стороны, и правом провайдеров развивать собственные сети, с другой ?
- Будут ли пользователи иметь неограниченный выбор в отсутствие регулирования на открытом рынке, как этого хотят провайдеры? Будут ли пользователи в состоянии сделать сознательный выбор?[68] Должны ли регуляторы выступать гарантами соблюдения прав пользователей, и если да, то какими полномочиями они должны обладать?
- Как различные подходы в области права и регулирования влияют на рынок широкополосного доступа, инвестиции и инновации?
- Каковы будут последствия от введения сетевого нейтралитета или отказа от этого принципа в развивающихся странах?
- Чем может обернуться переход Интернета на многоуровневую структуру с точки зрения конкуренции, инноваций, инвестиций и прав человека?
- Можно ли считать предоставление бесплатного доступа к определенным услугам или контенту или создание сетей доставки контента свидетельством создания «многоуровневого Интернета»?
- Станет ли «многоуровневый Интернет» и появление новых услуг прибыльным бизнесом для OTT-провайдеров? Смогут ли они адаптировать эту модель к потребностям пользователей в развивающихся странах или нет?
- Смогут ли телекоммуникационные операторы перестроить свои бизнес-модели и наращивать доходы, не нарушая принципа сетевого нейтралитета (по примеру iTunes, Google и других OTT-провайдеров, и в случае партнерств между OTT-провайдерами и операторами)?
- Исчезнет ли необходимость в регулировании трафика из соображений технического характера (качества) по мере усовершенствования технологий передачи данных?
- Как растущая зависимость от облачных технологий и развитие Интернета вещей повлияют на споры о сетевом нейтралитете, и наоборот?
- Следует ли перейти в споре об управлении интернет-трафиком с уровня интернет-провайдеров на уровень управления контентом и приложениями их поставщиками, например, компаниями Google, Apple или Facebook?
- Продолжат ли защитники прав потребителей отстаивать принцип сетевого нейтралитета?
- В случае отказа от сетевого нейтралитета, какие принципы будут применяться в будущем при отстаивании прав потребителей?

Технические и сетевые стандарты

Технические стандарты

Технические стандарты в Интернете призваны обеспечить не только выход в Интернет аппаратного и программного обеспечения, произведенного

различными компаниями, но и их максимально эффективную интеграцию и совместимость. Таким образом, стандарты способствуют разработке техническим сообществом, в том числе производителями, совместимого между собой аппаратного и программного обеспечения. Как уже объяснялось ранее по тексту, главным техническим стандартом Интернета является протокол TCP/IP.

Выработка технических стандартов инфраструктуры

Разработка стандартов для конкретной отрасли может длиться десятилетиями. Чтобы оперативно реагировать на изменения, связанные с применением ИКТ-компаниями новых технологий, МСЭ оптимизировал процесс разработки стандартов, сократив сроки до нескольких месяцев. Однако на внедрение значимых стандартов все равно уходят годы. Например, стандарт по работе сетей пятого поколения (5G) появится только в 2020 г. [69]

Помимо МСЭ, технические стандарты все в большей степени устанавливаются частными и профессиональными институтами. Так, техническими и инженерными аспектами развития Интернета занимается Совет по архитектуре Интернета (Internet Architecture Board — IAB), тогда как большинство стандартов внедряется Рабочей группой по проектированию Интернета (Internet Engineering Task Force, IETF) в соответствии с формальной процедурой запроса комментариев (Request for Comments, RFC). При этом и IAB, и IETF функционируют в рамках международной профессиональной организации «Общество Интернета» (Internet Society, ISOC).

В число других организаций, занимающихся вопросами стандартизации, входят Институт инженеров по электротехнике и электронике (IEEE), который, в частности, разрабатывает стандарты WiFi (IEEE 802.11b), организация WiFi Alliance, в обязанности которой входит сертификация оборудования, совместимого со стандартом WiFi, а также Ассоциация GSM (Groupe Speciale Mobile Association — GSMA), которая занимается стандартами для сетей мобильной связи. Сама роль этих институтов, а именно установление и внедрение стандартов на столь быстро развивающемся рынке, дает им возможность оказывать на его развитие существенное влияние.

Открытые стандарты в Интернете позволяют разработчикам создавать новые сервисы без получения дополнительных разрешений или лицензий.

В качестве примеров открытых стандартов можно привести www и ряд интернет-протоколов. Созданию открытых стандартов способствует целый ряд организаций. Например, инициатива Open Stand направлена на разработку открытых и глобальных рыночных стандартов при поддержке IEEE, IETF, IAB и «Общества Интернета».

Технологии, стандарты и политика

Организации, занимающиеся установлением и внедрением стандартов на столь быстро развивающемся рынке, оказывают существенное влияние на его развитие.

Технические решения могут иметь далеко идущие экономические и социальные последствия, изменяя баланс сил между конкурирующими фирмами или странами. При этом значение стандартов для Интернета невозможно переоценить. Например, разрабатывая стандарты и программное обеспечение, программисты могут влиять на ситуацию с обеспечением и защитой прав человека (например, право на информацию, неприкосновенность частной жизни и защиту данных).

Попытки установить официальные стандарты выводят частные технические решения разработчиков той или иной системы на общественное поле; таким образом, «битвы» по поводу стандартов могут выявить скрытые надежды и конфликты интересов. Сам пыл, с которым заинтересованные стороны спорят по поводу тех или иных решений в отношении стандартов, служит для нас признаком того, что за чисто техническими решениями скрывается более глубокий смысл.

Сетевые стандарты

Сетевые стандарты можно охарактеризовать как набор официальных стандартов и технических спецификаций для Всемирной сети (WWW). Они обеспечивают возможность получения доступа к контенту с использованием любых устройств и конфигураций и тем самым задают основные правила по разработке сайтов и интернет-приложений. Основным стандартом в области контента и приложений является теговый язык разметки гипертекста HTML

(HyperText Markup Language). Его текущей версией является HTML5. Еще одним языком обмена структурированной информацией является XML. В целях оформления интернет-страниц в сочетании с HTML используются Cascading Style Sheets (CSS). Кроме того, существует eXtensible HTML (XHTML), расширенная версия HTML с более строгими правилами.

Эволюция сетевых стандартов

К концу 1980-х гг. «битва» за сетевые стандарты завершилась. TCP/IP постепенно стал основным сетевым протоколом, оттеснив другие: поддерживавшийся МСЭ протокол X-25 (часть архитектуры Взаимодействия открытых систем) и многие фирменные стандарты, такие как разработанный IBM стандарт SNA. Хотя Интернет и облегчил коммуникацию между разнообразными сетями за счет использования TCP/IP, в системе еще не было общих стандартов приложений.

Решение было разработано Тимом Бернерсом-Ли и его коллегами в лаборатории CERN в Женеве и представляло собой новый стандарт обмена информацией по Интернету, названный HTML (по сути, упрощение существовавшего стандарта ISO, называвшегося SGML). Любой появляющийся в Интернете контент должен был сначала пройти преобразование по стандарту 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. Изначально HTML позволял работать только с текстом и изображениями, однако новые интернет-приложения требовали более сложных технологий для управления базами данных, работы с видео и анимацией. Такое разнообразие приложений требовало существенных усилий по стандартизации, чтобы гарантировать адекватное отображение любого размещенного в Интернете материала большинством браузеров.

Стандартизация приложений вступила в новую фазу с появлением языка XML, предоставившего большую гибкость в установлении стандартов для содержимого интернет-страниц. Появились и новые группы XML-стандартов. Например, стандарт для распространения материалов по беспроводной связи называется Wireless Mark-up Language (WML).

Установление сетевых стандартов

Стандартизация приложений осуществляется преимущественно в рамках Консорциума «всемирной паутины» (W3C), возглавляемого Тимом Бернерсом-Ли. Разработка стандартов представляет сложный процесс, в котором решение принимаются на основе консенсуса, исходя из принципов справедливости, подотчетности и качества. Когда консенсус достигнут, стандарты публикуются в виде Рекомендаций[70].

Стандарты W3C создают открытую платформу для разработки приложений, что позволяет разработчикам создавать разнообразный интерактивный контент. Согласно стандартам W3C, «несмотря на постоянно меняющиеся границы между различными платформами, ведущие отраслевые компании придерживаются единого мнения, что краеугольным камнем данной платформы станет HTML5»[71].

Интересно отметить, что, несмотря на свою большую важность для Интернета, W3C пока не привлек к себе достаточного внимания в дискуссиях по управлению Интернетом.

Облачная обработка данных

Что такое «облачная обработка данных» и как она работает?

Облачную обработку данных (рис. 9) можно охарактеризовать как переход от хранения данных на жестких дисках наших компьютеров к хранению в облаке (например, с использованием больших «серверных ферм»). Такой подход дает возможность получить доступ к данным и услугам с использо-

ванием любого устройства в любой точке мира (при условии подключения к Интернету). В то же время сам факт хранения наших данных третьим лицом, при том, что копии и фрагменты наших данных могут одновременно находиться в нескольких юрисдикциях, вызывает озабоченность с точки зрения права на неприкосновенность частной жизни и конфиденциальности персональных данных. Облачное хранение должно соответствовать гораздо более высоким требованиям в области безопасности по сравнению с персональными компьютерами, поскольку взлом системы облачного хранения позволяет получить доступ к огромным массивам данных.

Начало облачной обработке данных положили серверы электронной почты (Gmail, Yahoo!), социальные сети (Facebook, Twitter) и интернет-приложения (Wikis, блоги, Google Docs). При этом системы облачного хранения все шире используются не только среди обычных пользователей, но и в корпоративном программном обеспечении. Мы переносим все больше данных с жестких дисков в облако. Самыми крупными компаниями в области облачной обработки данных являются Google, Microsoft, Apple, Amazon и Facebook, которые уже создали или планируют создать «серверные фермы».

Рисунок 9. Облачная обработка данных

В определенном смысле, появление технологий облачной обработки данных ознаменовало завершение одного из циклов развития компьютерных технологий. На заре компьютерного века существовали мощные универсальные ЭВМ и «тупые» рабочие станции с ограниченным функционалом. Весь вычислительный потенциал был сконцентрирован в мощных серверах. Переход от мощных серверов к персональным компьютерам произошел, когда IBM, Apple и Microsoft начали производить персональные компьютеры. Произошла повсеместная децентрализация вычислительных мощностей. Мы стали хранить данные на дискетах и жестких дисках, запускать приложения (от текстовых редакторов до игр) на наших компьютерах. Затем появились сетевые технологии, позволившие соединить отдельные компьютеры: сначала в рамках компаний и организаций (посредством локальных сетей LAN), а затем и по всему миру, в том числе посредством Интернета. На начальном этапе развития Интернета (до 2005 г.), всемирная паутина преимущественно использовалась для обмена данными, хранившимися в памяти компьютеров, а компьютеры могли запускать основные приложения, например, текстовые редакторы.

С появлением в течение последних десяти лет социальных сетей, а также смартфонов и планшетных ПК произошел еще один серьезный сдвиг: перенос программного обеспечения и растущего объема данных на мощные «облачные» серверы. Начало этому процессу положили службы электронной почты, такие как Gmail. Затем появились решения по облачному хранению фотографий, текстовых файлов и других цифровых ресурсов, а также возможность использовать облачные версии программного обеспечения (например, Google Docs или Microsoft Office 365). Сейчас большинство цифровых активов размещено на централизованных облачных серверах. Таким образом, круг замкнулся. Все начиналось с централизованной сетевой архитектуры, появление персональных компьютеров привело к рассредоточению данных, а развитие облачных технологий вернуло нас к централизованному хранению.

Облачные технологии делятся на три уровня: аппаратное обеспечение, программное обеспечение промежуточного уровня и конечные программные продукты. В сфере облачных технологий существует три вида услуг:

- «Программное обеспечение как услуга» (SaaS): поставщик облачных услуг предоставляет пользователю доступ к программному обеспечению, то есть возможность пользоваться приложениями (и полученными с их помощью данными) с любого устройства, подключенного к Интернету. В таком случае пользователь лишен каких-либо рычагов контроля в отношении облачных ресурсов, и его действия ограничены использованием доступного приложения. Это наиболее распространенный формат обслуживания: приложение конечного пользователя выступает в качестве отправной точки. В качестве примера можно привести Twitter или приложение для использования локальной организацией центральной базы данных.
- «Платформа как услуга» (PaaS): пользователи могут самостоятельно разрабатывать приложения и запускать их на арендованных облачных платформах. Таким образом, пользователи могут самостоятельно выбирать аппаратное обеспечение. Однако они все равно лишены возможности менять настройки сервера или хранилища. Стандартизация имеет важное значение при использовании платформы, поскольку позволяет программистам создавать продукты для широкого круга потребителей и дает пользователям возможность выбора.
- «Инфраструктура как услуга» (IaaS): наименее используемое облачное решение, требующее продвинутых навыков в области информационных технологий. В то же время эта технология обеспечивает максимальную свободу выбора ресурсов. При использовании IaaS поставщик предоставляет только аппаратное обеспечение (вычислительные мощности и хранение), тогда как пользователь сам настраивает работу системы, включая операционное программное обеспечение.

Право и регулирование облачной обработки данных

Облачные серверы как элементы ключевой информационной инфраструктуры

Большинство интернет-приложений работает через облачные серверы. Когда облачных технологий не было, при потере соединения услуга

становилась недоступной — мы просто не могли отправить сообщение по электронной почте или просмотреть интернет-страницы. Однако с появлением облачных решений мы не сможем даже набрать текст или сделать расчет, поскольку эти операции осуществляются облачными приложениями. Таким образом, облачные услуги востребованы миллионами интернет-пользователей и компаний, что дает основания считать облачные серверы частью критической инфраструктуры глобальной сети и большинства стран мира.

Безопасность и шифрование

Тот факт, что один облачный оператор обслуживает тысячи или даже миллионы потребителей, не может оставить равнодушными различных злоумышленников, будь то преступники, террористы, кибершпионы или кто-то еще, которые попытаются воспользоваться уязвимостью таких приложений.

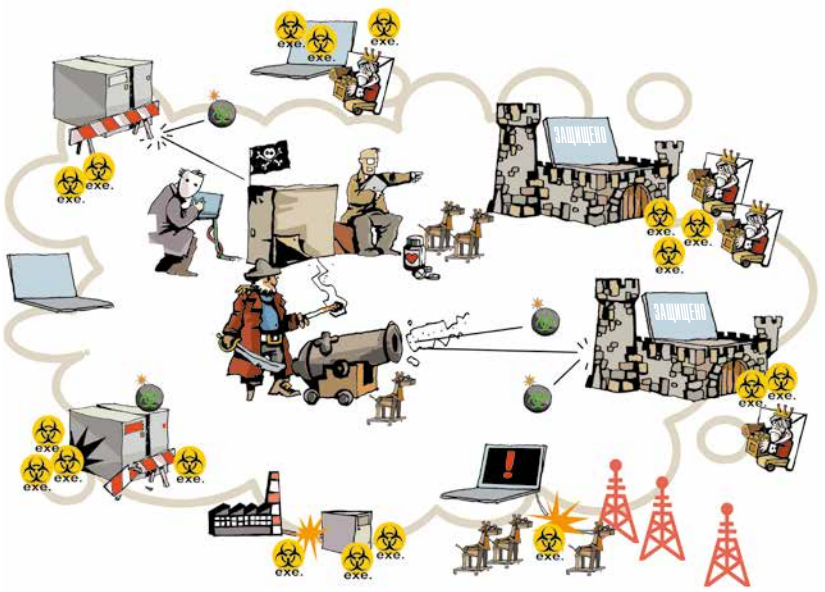


Рисунок 10. Обеспечение безопасности облака

Существует хорошо известная триада информационной безопасности: конфиденциальность, целостность и доступность данных и системы. Эта

модель отлично подходит для классификации возможных угроз безопасности, с которыми сталкиваются пользователи облачных решений. Для обеспечения безопасности облачных систем необходимо учесть ряд факторов: предоставление права доступа к определенным сегментам данных и услуг, обеспечение сквозного шифрования в облаке, обеспечение безопасности каждого сегмента ИКТ-системы и сети, связывающей облачный сервер с пользователями, шифрование данных между облаком и конечными пользователями и резервное облачное хранение данных (рис. 10).

Обеспечение конфиденциальности и защита данных

В облаке хранится все больше и больше персональных данных. Соответственно, вопросы обеспечения конфиденциальности и защиты данных становятся все более актуальными. Можем ли мы контролировать наши текстовые файлы, электронную почту и другие данные? Могут ли операторы облачных услуг использовать эти данные без нашего разрешения? Будет ли у нас доступ к нашим данным?

Вопросы защиты конфиденциальности и защиты персональных данных в контексте облачных технологий вызывают особую озабоченность у ЕС. Реагируя на рост оборота цифровых данных между Европой и Америкой, ЕС и США предприняли попытку гармонизировать режимы защиты конфиденциальности и обеспечить соблюдение американскими облачными операторами требований ЕС в отношении защиты персональных данных и конфиденциальности его граждан. В октябре 2015 г. Суд Европейского союза объявил недействительным соглашение о «безопасной гавани» (Safe Harbour), и в июле 2016 г. вступило в силу новое соглашение о правилах обмена конфиденциальной информацией между ЕС и США (Privacy Shield), которое, как предполагается, должно решить проблему. Однако пока неясно, насколько эффективным окажется это соглашение.

Большие данные

Феномен «больших данных» (big data) неразрывно связан с облачными вычислениями. Несмотря на ажиотаж вокруг этой темы, обработка больших данных играет огромную роль в современных цифровых технологиях, и их значение будет только возрастать по мере развития Интернета вещей, когда машины, бытовая техника и даже одежда будут заниматься сбором данных. Обработка такой информации позволит нам перейти на новые модели экономического развития. Соответственно, будет расти и спрос на облачные ресурсы.

Например, в дополнение к облачным технологиям ведется разработка решений в области так называемых «туманных вычислений» (fog computing) с целью уменьшения объемов данных, передаваемых в облако для обработки и анализа. Как отмечают в компании Cisco, туманные технологии позволяют физически приблизить облако к «вещам», являющимся источником данных; обрабатывать данные, не удаляясь от источника, сократить период ожидания (латентность)[72]; освободить основную сеть от гигабайтов трафика и сохранить конфиденциальные данные в рамках сети[73].

Локализация данных

Все больше и больше информации переводится в цифровой формат, и власти многих стран начинают высказывать обеспокоенность фактом хранения своих данных за рубежом. В некоторых странах приняты или обсуждаются меры, обязывающие хранить данные внутри страны (поставщики облачных услуг и/или их данные должны храниться на территории страны).

Мотивы введения правил по локализации хранения данных могут быть разными — как политическими, так и экономическими. Меры по локализации экономических данных часто обусловлены политикой протекционизма. Коль скоро данные являются главным ресурсом интернет-экономики, страны стараются сделать так, чтобы этот ресурс не покидал их территории и использовался для развития национальной экономики через посредство обработки информации и управления данными.

Власти могут требовать, чтобы определенные виды данных обрабатывались и хранились на территории страны, из соображений необходимости защиты данных и обеспечения безопасности, что вынуждает поставщиков услуг работать в рамках национального законодательства. Кроме того, в ряде стран сейчас рассматривается вопрос о создании государственных

облачных платформ для обработки и хранения правительственных/официальных данных. Требование в отношении локализации данных может быть обусловлено заинтересованностью властей отдельных стран в том, чтобы осуществлять контроль над политической жизнью. Достичь этой цели проще, если дата-серверы находятся в национальной юрисдикции.

Поставщики облачных услуг стараются находить решения, в том числе технического характера, чтобы соблюсти требования по локализации, не лишая своих клиентов возможности пользоваться облачными услугами. Например, в марте 2016 г. компания Oracle запустила новую услугу облачных вычислений, позволяющую компаниям размещать облачные серверы Oracle в собственных дата-центрах. По заявлению Oracle, эта новая услуга разработана для удовлетворения запросов организаций, которые еще не перешли на облачные технологии из-за нормативно-правовых требований по локализации облачных серверов[74].

Стандарты и совместимость

Поскольку поставщиков облачных услуг много, проблема разработки стандартов как никогда актуальна. Особо важны стандарты для обеспечения совместимости при передаче данных от одного облака к другому (например, от Google к Apple). Один из обсуждаемых вариантов решения этой проблемы заключается в том, чтобы принять открытые стандарты, которыми бы руководствовались все основные участники рынка облачных технологий. Однако к общему знаменателю в этом вопросе прийти будет непросто, поскольку крупные компании в этом сегменте считают свои фирменные стандарты одним из своих конкурентных преимуществ. И все же существует ряд инициатив, направленных на обеспечение совместимости. Например, в 2013 г. Open Group, в которую входят такие компании как Fujitsu, IBM и Oracle, опубликовала Руководство по переносимости и совместимости облачных вычислений (Guide to Cloud Computing Portability and Interoperability), в котором изложены рекомендации пользователям о том, как обеспечить совместимость при работе с облачными продуктами и услугами, а также рекомендации поставщикам и органам по стандартизации о том, как должны меняться стандарты и подходы для обеспечения большей совместимости[75].

В рамках IEEE создана «Инициатива IEEE по облачным вычислениям», которая, в частности, занимается выработкой стандартов совместимости облачных технологий.

Интернет вещей

Концепция Интернета вещей заключается в расширении круга подключенных к Интернету устройств, которые больше не ограничиваются компьютерами, мобильными телефонами, планшетами и электронными книгами, и включают автомобили, бытовую технику, одежду, объекты городской инфраструктуры и медицинские приборы.

По существующим оценкам, к 2020 г. в мире будет от 20 до 100 млрд. устройств с выходом в Интернет. Соответственно, на них будет приходиться существенный объем данных, представляющих особую ценность. По прогнозу международной исследовательской и консалтинговой компании International Data Corporation (IDC), к 2020 объем «цифровой вселенной» вырастет до 44 секстибайт (секстибайт — триллион гигабайт), и на устройства Интернета вещей будет приходиться 10% от этого объема[76].

Согласно прогнозам, финансовые показатели в сегменте Интернета вещей будут стремительно расти. Производители планируют наращивать выпуск подключенных к сети устройств. Так, по прогнозу компании Verizon, объем международного рынка устройств Интернета вещей может вырасти с 591,7 млрд. долл. в 2014 г. до 1,3 трлн. долл. в 2019 г., а совокупные темпы годового прироста составят 17%[77].

В начале 2016 г. МСЭ и компания Cisco Systems подготовили доклад, в котором говорится, что Интернет вещей может способствовать повышению уровня жизни по всему миру и достижению целей устойчивого развития. В докладе отмечается растущая роль Интернета вещей в таких областях, как здравоохранение, образование, водоснабжение и водоотведение, поддержание жизнеспособности, снижение негативных последствий изменения климата и загрязнения окружающей среды, управление энергоресурсами и энергетика[78].

Устройства Интернета вещей нередко являются составляющими более масштабных систем, например «умных домов» и «умных городов». Такие устройства собирают огромные объемы данных и в то же время дают возможность по-новому использовать такие данные. В своей работе устройства Интернета вещей используют существующую структуру Интернета, а не какую-ту отдельную или отличную среду.

К наиболее распространенным видам сенсоров и компонентов, используемых в системе Интернета вещей, относятся:

- радиочастотные метки-идентификаторы (RFID) — электронные блоки, которые крепятся к чему-нибудь (одежде, домашним животным, посылкам) для отслеживания их местоположения.
- Универсальные товарные коды (UPC) — используются почти на все товарах в супермаркетах.
- Электронные коды продукта (EPC) — уникальные идентификаторы любого физического объекта в любой точке мира в любое время. EPC по своей сути похож на UPC, только представлен не в физической, а электронной форме.

Наряду с этим исследователи продолжают изучать другие способы подключения устройств Интернета вещей. Например, в опубликованной в июне 2016 г. статье[79] группа исследователей предлагает использовать светодиодные лампы для подключения друг к другу устройств Интернета вещей. Они утверждают, что такая система позволит решить проблему нехватки радиочастотного ресурса (поскольку многие устройства Интернета вещей используют радиочастоты).

Хотя по своему размеру единицы данных, исходящих от устройств Интернета вещей, относительно невелики, в совокупности получается огромный объем в силу количества таких устройств, а также возможности хранения и обработки данных в облаке. Таким образом, облачным технологиям суждено сыграть огромную роль в развитии Интернета вещей.

Сферы применения Интернета вещей

К наиболее развитым сферам применения Интернета вещей относятся:

- Домашняя автоматизация: обеспечение доступа к домашней бытовой технике из любой точки мира. Никаких единых протоколов или отраслевого стандарта для интерфейса прикладного программирования не существует.
- Транспорт: Использование систем Интернета вещей для отслеживания таких показателей, как расход топлива, местонахождение, время, расстояние, для определения потребности в обслуживании автомобилей и оптимизации использования ресурсов (например, парка автомобилей). В скором времени технологии Интернета вещей найдут применение в беспилотных автомобилях некоторых автопроизводителей (например, Tesla и Toyota), а также в таких компаниях, как Google и Uber.

Интернет вещей также все больше используется в энергетике, инфраструктуре, сельском хозяйстве, обрабатывающей промышленности, а также при разработке пользовательских приложений. Концепция «умного города» предусматривает внедрение ИКТ с целью улучшения качества и эффективности городских услуг и инфраструктуры и повышения качества жизни горожан.

Частный сектор и государство

Самые значимые инициативы в области Интернета вещей исходят от частного сектора. Пока технологические компании, такие как Cisco и Intel, расширяют ассортимент услуг, телекоммуникационные компании создают крупномасштабные сети, призванные способствовать популяризации соответствующих устройств Интернета вещей[80]. Кроме того, компании из различных отраслей стали создавать альянсы по разработке решений в сегменте Интернета вещей. Например, фонд Open Connectivity Foundation стремится обеспечить совместимость устройств Интернета вещей друг с другом вне зависимости от производителя, используемой операционной системы, чипа или физического исполнения. В работе фонда принимают участие представители различных отраслей, включая автомобильную промышленность, бытовую технику, здравоохранение, промышленность и т. п. В качестве еще одного примера можно привести альянс LoRa, который занимается разработкой стандартов в области Интернета вещей. Так, альянс разработал спецификацию LoRaWAN (сети с боль-

шим радиусом действия), которая призвана обеспечить совместимость устройств Интернета вещей.

Огромный потенциал сегмента Интернета вещей становится все более очевидным для властей на национальном и наднациональном уровнях. Например, ЕС выступил с инициативой принятия рабочей программы «Горизонт 2020. Рабочая программа 2016/2017: Тестирование и внедрение крупномасштабных пилотных проектов в области Интернета вещей», суть которой заключается в выделении финансирования на реализацию программ по продвижению Интернета вещей в Европе. В США Национальное управление по телекоммуникациям и информации (NTIA) рассматривает вопрос о пересмотре технологической политики и нормативной базы Интернета вещей, стремясь понять, какую роль в продвижении Интернета вещей должны играть государство и частный сектор. В Китае правительство создало институт Chengdu Internet of Things Technology Institute для финансирования через эту организацию исследований, связанных с Интернетом вещей.

Основные вопросы

Интернет вещей генерирует огромные массивы данных, в связи с чем вопрос о хранении и защите конфиденциальной информации приобретает особое значение. Некоторые устройства Интернета вещей собирают и передают персональные данные (например, устройства медицинского назначения), однако защищенность таких устройств (обеспечение их безопасности)[81], а также обработка и анализ собранных данных вызывают серьезную озабоченность. Если данные с одного устройства Интернета вещей не нарушают требований конфиденциальности, то объединение этих данных с данными других устройств, их последующая обработка и анализ могут привести к разглашению конфиденциальной информации.

В свете отсутствия надзора весьма проблематичен и вопрос о том, кто будет владеть этими данными. Многие приложения, используемые в сегменте Интернета, а также получаемые с их помощью данные запатентованы. Из-за изменения требований в области безопасности и защиты неприкосновенности частной жизни (в отношении данных, протоколов и устройств) может потребоваться разработать новые регламенты. Эта сфера требует разработки единых подходов на глобальном уровне, возможно, даже в большей степени, чем любой другой вопрос, связанный с управлением Интернетом. Придется заключать новые общественные договоры.

Поскольку Интернет вещей занимает центральное место в инициативах по разработке искусственного интеллекта, будь то внедрение роботов, беспилотных автомобилей и других цифровых систем, способных принимать решения и оценивать ситуацию, существуют также вопросы этического характера. Власти и частный сектор все активнее подчеркивают необходимость обсуждения этических принципов в области Интернета вещей и искусственного интеллекта и способов реализации этих принципов.

Этические вопросы

Интернет вещей, обработка больших данных и искусственный интеллект ставят перед нами вопросы этического характера. При этом речь идет не только о безопасности и неприкосновенности частной жизни, но и этических аспектах принятия решений автоматизированными системами. Например, компания Jigsway, дочерняя компания Google, разработала систему искусственного интеллекта Conversation AI с целью выявления злоупотреблений и случаев домогательств в Интернете. Хотя это решение, по идее, призвано бороться со злоупотреблениями в общественном пространстве Интернета, с его использованием связан фундаментальный вопрос: может ли машина определять, какие выражения пристойны, а какие нет? [82]

Споры об этических аспектах использования новых цифровых технологий ведутся как в деловой среде, так и на государственном уровне. Ряд крупных технологических компаний (IBM, Facebook, Google, Microsoft, Amazon и DeepMind) создали проект по искусственному интеллекту Partnership on Artificial Intelligence, в рамках которого ведется работа по обеспечению сохранности конфиденциальной информации, безопасности, выработка этических принципов внедрения решений в области искусственного интеллекта, а также обсуждение этических аспектов использования новых цифровых технологий[83]. В первой половине 2016 г. Парламент Европейского союза опубликовал проект доклада

по робототехнике, в котором, в частности, рассматриваются этические аспекты внедрения новых технологий в области робототехники. Авторы доклада рекомендуют принять «руководство по разработке, производству и использованию роботов» в соответствии с такими принципами как «делать во благо», «не навреди» и автономность, а также с учетом необходимости соблюдения права на человеческое достоинство и соблюдения прав человека, равенства, справедливости и равноправия, отказа от дискриминации и стигматизации»[84]. В США в октябре 2016 г. принят Национальный стратегический план по исследованиям в области искусственного интеллекта и его разработке (National Artificial Intelligence Research and Development Strategic Plan), авторы которого подчеркивают необходимость «определить, как наилучшим образом спроектировать архитектуру систем искусственного интеллекта с учетом этических принципов»[85]. В парламенте Соединенного Королевства подготовлен доклад по робототехнике и искусственному интеллекту, авторы которого призывают правительство взять на себя инициативу в решении этических вопросов, связанных с использованием автономных систем, включая решения в области искусственного интеллекта[86].

Конвергенция

Телекоммуникационная отрасль, телерадиовещание и другие смежные сегменты в силу исторических обстоятельств до недавнего времени развивались независимо друг от друга в связи с различиями в технологиях и нормативно-правовых режимах. Широкое и все возрастающее использование Интернета привело к сближению (конвергенции) телекоммуникаций, теле- и радиовещания, а также систем передачи информации. Сегодня с помощью Интернета можно делать телефонные звонки, слушать радио, смотреть телепрограммы и обмениваться музыкой. Всего несколько лет назад эти задачи выполнялись различными системами.

В сфере традиционных коммуникаций основным направлением конвергенции является интернет-телефония (VoIP). Растущая популярность программ интернет-телефонии, таких как Skype, WhatsApp и Viber, обусловлена низкой стоимостью, возможностью объединить линии голосового общения и передачи данных, а также доступностью продвинутых инструментов для персональных компьютеров и мобильных устройств. Благодаря YouTube и аналогичным сервисам Интернет сближается с традиционными мультимедийными и развлекательными услугами. Развитие IP-телевидения также способствует сближению мультимедийных услуг и сетей, основанных на использовании IP-протокола.

В то время как с технической точки зрения процесс сближения различных платформ идет стремительно, его экономические и правовые последствия проявятся лишь через некоторое время.

Взаимодействие на международном уровне в основном сводится к обмену передовым опытом в области конвергенции. Для изучения этой темы в рамках Сектора развития электросвязи МСЭ (Telecommunication Development Sector — ITU-D) была создана исследовательская группа. В Совете Европы рабочий комитет по СМИ и информации занимается проблемой сосуществования и взаимодействия традиционных и новых медиа, что является одним из аспектов конвергенции. В целом, конвергенция напрямую связана с такими темами, как сетевая нейтральность, Интернет вещей, роль посредников, интернет-торговля, защита прав потребителей и налогообложение.

Вопросы

Экономические последствия конвергенции

С экономической точки зрения, конвергенция технологий начала перекраивать традиционные рынки, сделав компании, ранее действовавшие в разных областях, прямыми конкурентами. Из-за конвергенции руководители и владельцы компаний теперь страдают «синдромом Uber», под которым понимается выход на рынок конкурента с совершенно иной бизнес-моделью, в результате чего традиционные участники рынка оказываются неконкурентоспособными[87]. Именно это произошло, когда на рынок такси вышла инновационная технологическая компания Uber. Обычные таксомоторные парки и таксисты по всему миру стали подавать против нее иски, поскольку

на Uber не распространялись нормативно-правовые требования, действовавшие в отношении других участников рынка.

В этих условиях компании используют различные стратегии, наиболее распространенными из которых являются слияния и поглощения, когда небольшие OTT-провайдеры, недавно вышедшие на рынок, объединяются с более крупными компаниями или приобретаются ими. С недавних пор OTT-провайдеры и телекоммуникационные компании также стали переходить на модель взаимовыгодного партнерского взаимодействия. Сотрудничество с OTT-провайдерами дает конкурентное преимущество телекоммуникационным компаниям, а также приносит пользу их клиентам, а услуги OTT-провайдеров становятся более заметными и доступными благодаря сотрудничеству с телекоммуникационными операторами[88].

Регулирование в вопросах конвергенции

Правовая система наиболее медленно адаптируется к переменам, связанным со сближением технологий. Каждый из сегментов — телекоммуникации, теле- и радиовещание, передача данных — имеет собственную нормативную базу. Сближение этих областей порождает несколько вопросов, относящихся к управлению и регулированию:

- Что произойдет с существующими национальными и международными нормативно-правовыми режимами в таких областях, как телефонная связь или телерадиовещание?
- Существует ли необходимость в создании новых нормативно-правовых режимов для конвергентных услуг, или же они должны регулироваться таким же образом, как и, например, традиционные услуги электросвязи?
- Какие правила следует ввести для поставщиков конвергентных услуг в том, что касается обеспечения конкуренции и защиты прав потребителей?
- Должно ли регулирование процесса конвергенции осуществляться органами власти (государственными органами власти и международными организациями) или же методами саморегулирования?

Эти вопросы решаются по-разному в различных странах. Так, некоторые страны, например, государства Европейского союза, Индия и Кения, придерживаются гибкого подхода при регулировании процесса конвергенции, решая возникающие вопросы на основе принципов сетевого нейтралитета, то есть пользователям предоставляется возможность выбора любого типа приложений или услуг, доступных в IP-сетях. В ряде других стран было принято решение создать новые режимы регулирования услуг, появившихся в результате конвергенции. В Корее был принят Закон о мультимедийной вещательной деятельности в Интернете (Internet Multimedia Broadcasting Business Act), который содержит положения о лицензировании услуг IP-телевидения и его качестве. В некоторых странах допускается саморегулирование процесса конвергенции. Например, в Австралии Альянс связи (Communications Alliance, представляет различные компании в сфере телекоммуникаций) разработал ряд регламентов в области IP-телефонии[89].

Однако есть страны, где конвергентные услуги, в особенности IP-телефония попросту запрещены (или были запрещены на определенном этапе) на законодательном уровне или блокируются поставщиками телекоммуникационных услуг. В число таких стран входят, в частности, Марокко, Белиз и Объединенные Арабские Эмираты.

Примечания к разделу 2

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

[2] Действуя в духе технологической нейтральности, вместо термина «телекоммуникации» ЕС использует термин «электронные средства связи», который охватывает, в частности, интернет-трафик по электросети, которая не относится к телекоммуникационной инфраструктуре.

[3] Передачу интернет-трафика по электросети иногда называют «Интернет из розетки» (англоязычный термин — Power Line Communication, PLC). Использование линий электропередачи сделает Интернет более доступным для многих пользователей. Для получения дополнительной информации об этой технологии, см.: Palet J. Addressing the Digital Divide with IPv6-enabled

Broadband Power Line Communication" // Internet Society, ISOC Member Briefing, № 13 (адрес в Интернете: http://www.isoc.org/briefings/013) [просмотрено 3 августа 2018 г.].

[4] Проект «Loon» компании Google ставит целью обеспечение доступа к широкополосному интернету в самых удаленных точках планеты в отсутствие телекоммуникационной инфраструктуры. Компания запускает множество аэростатов в стратосферу на высоту около 20 км. Каждый запущенный аэростат представляет базовую станцию, обеспечивающую сигнал для конечных пользователей. Эти аэростаты связаны между собой и с базовым станциями на земле высокоскоростными линиями, которые предоставляются партнерами по телекоммуникационным услугам.

[5] Согласно определению МСЭ, неиспользуемый частотный спектр телевидения это «сегмент радиочастотного спектра, который не используется при телевещании, также именуемый «промежуточный». Поскольку неиспользуемые частоты относятся к сегменту спектра, который обеспечивает «высокие показатели распространения сигнала в диапазоне УВЧ (ТВ) (высокое качество приема на улице и внутри помещений и вне линии прямой видимости)», по мнению сотрудника Бюро радиосвязи МСЭ Кристиана Гомеса, неиспользуемый частотный спектр считается альтернативной, низковольтной технологией, которую можно было бы использовать для обеспечения широкополосного доступа в сельской местности, а также для межмашинной коммуникации в области Интернета вещей. Подробнее см.: ITU (2012) Digital Dividend: Insights for Spectrum Decisions (адрес в Интернете: http://www.itu.int/ITU-D/tech/digital_broadcasting/Reports/DigitalDividend.pdf) [просмотрено 3 августа 2018 г.], а также Gomez C (2013) TV White Spaces: Managing spaces or better managing inefficiencies? (адрес в Интернете: https://www.itu.int/en/ITU-D/Conferences/GSR/Documents/GSR_paper_WhiteSpaces_Gomez.pdf) [просмотрено 3 августа 2018 г.].

[6] Либерализация телекоммуникационных рынков государств-участников ВТО была формально закреплена в 1998 г. в рамках Базового соглашения о телекоммуникациях. После принятия этого Соглашения более 100 государств начали процесс либерализации, связанный с приватизацией национальных телекоммуникационных монополий, введением конкуренции и установлением национальных регулирующих механизмов. Формальное название соглашения — «Четвертый протокол Генерального соглашения по торговле услугами» (принят 30 апреля 1996 г. и вступил в силу 5 февраля 1998 г. Адрес в Интернете: http://www.wto.org/english/tratop_e/serv_e/4prote_e.htm) [просмотрено 3 августа 2018 г.].

[7] МСЭ. Подписанты Заключительных актов Всемирной конференции по международной электросвязи (WCIT-12) (адрес в Интернете: http://www.itu.int/osg/wcit-12/highlights/signatories.html) [просмотрено 3 августа 2018 г.].

[8] Подробнее о деятельности МСЭ в области Интернета см. http://www.itu.int/en/action/internet/Pages/default.aspx [просмотрено 3 августа 2018 г.].

[9] Архитектура цифровых объектов — проект, инициированный Робертом Каном (один из изобретателей протокола TCP/IP), с целью присвоить уникальные идентификаторы каждому цифровому объекту (данным и устройствам). Подразумевается, что такие идентификаторы не меняются вне зависимости от того, где расположен объект в сети, кто им владеет, на какой технологии он основан и т. д. Обязанность по регулированию Архитектуры цифровых объектов возложена на швейцарскую Ассоциацию управления цифровыми объектами (DONA). В рамках МСЭ и исследовательских групп Сектора электросвязи МСЭ принята в качестве стандарта для облачных вычислений и устройств Интернета вещей. Некоторые страны – члены МСЭ выступают за принятие стандартов Архитектуры цифровых объектов для борьбы с подделкой устройств, в то время как другие считают, что, создав возможность отслеживания устройств, Архитектура цифровых объектов будет использоваться для отслеживания и контроля над потоками информации, а также действиями пользователей. Подробнее см.: Corporation for National Research Initiatives (2010) A Brief Overview of the Digital Object Architecture and its Application to Identification, Discovery, Resolution and Access to Information in Digital Form (адрес в Интернете: http://www.cnri.reston.va.us/papers/Digital_Object_Architecture_Brief_Overview.pdf) [просмотрено 3 августа 2018 г.]; Javed D (2016) ITU IoT Standards: Gateway to Government Control? (адрес в Интернете: https://www.wileyconnect.com/home/2016/9/20/itu-iot-standards-gateway-to-government-control) [просмотрено 3 августа 2018 г.].

[10] Более подробно о роли ВТО в области телекоммуникаций см.: https://www.wto.org/english/tratop_e/serv_e/telecom_e/telecom_e.htm [просмотрено 3 августа 2018 г.].

[11] При подготовке данного раздела использовалась работа Kurbalija J (2016) From harmonising cyberpolicies to promoting twi-plomacy: How diplomacy can strengthen Asia-Europe's digital connectivity // Asia-Europe Foundation. ASEF Outlook Report 2016/2017. Connectivity: Facts and Perspectives, Volume II: Connecting Asia and Europe (адрес в Интернете: http://www.asef.org/images/docs/ASEF%20Outlook%20Report%202016-2017%20Vol2.pdf) [просмотрено 3 августа 2018 г.].

[12] UNESCAP (2014) Problems and Challenges in Transit Connectivity Routes and International Gateways in Asia //Discussion paper series, 2014/1 (адрес в Интернете: https://www.unescap.org/sites/default/files/Discussion%20Paper-Transit-Connectivity_0.pdf)[просмотрено 3 августа 2018 г.].

[13] Verda M (2014) Trans-Eurasian Information Super Highway (адрес в Интернете: http://sam.az/uploads/PDF/TRANS-EURASIAN%20INFORMATION%20SUPER%20HIGHWAY.pdf) [просмотрено 3 августа 2018 г.].

[14] Термин «Цифровой шелковый путь» используется в качестве собирательного понятия, охватывающего различные проекты по сотрудничеству между Азией и Европой в сфере цифровых технологий. См. подробнее: Jia L and Shuang G. Digital Silk Road to span Eurasia // China Daily Europe, 10.07.2015 (адрес в Интернете: http://europe.chinadaily.com.cn/epaper/2015-07/10/content_21241323.htm) [просмотрено 3 августа 2018 г.]; Zhao Huanxin Z. Web companies asked to support 'digital Silk Road' // China Daily Europe. 08.09.2015 (адрес в Интернете: http://www.chinadaily.com.cn/business/2015chinaarabforum/2015-09/08/content_21823475.htm) [просмотрено 3 августа 2018 г.]. «Цифровой шелковый путь» является частью инициативы «Один пояс, один путь», суть которой заключается в создании наземного и морского «Шелкового пути», связывающего Китай с регионами Юго-Восточной Азии, Южной Азии, Ближнего Востока, Восточной Африки и Средиземного моря. Проект охватывает 60 стран с общим населением 4,4 млрд., то есть 63% мирового населения. См. подробнее: Arase D (2015) China's Two Silk Roads Initiative: What It Means for Southeast Asia // Southeast Asian Affairs, 41, pp. 25-45; Tsao R (2015) One belt one road: A historical perspective // Chinese American Forum. 31(1) pp. 11-14.

[15] Подробнее о политике ЕС в области распределение радиочастот см. http://ec.europa.eu/digital-agenda/en/what-radio-spectrum-policy [просмотрено 5 августа 2018 г.].

[16] Применительно к сетевым технологиям, пирингом называется добровольное соглашение между отдельными интернет-сетями по созданию условий для обмена трафиком пользователей таких сетей. По своей сути, пиринг является системой безвозмездного обмена трафиком, то есть ни одна из сторон не платит за трафик. Вместо этого они получают доход от своих пользователей. Пиринг предусматривает наличие физической связи между сетями и обмен информацией о сетевых маршрутах по протоколу BGP. Часто это сопровождается заключением пиринговых соглашений различного вида, от простого подтверждения подключения до многостраничных договоров (источник: Wikipedia).

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

[18] В статье Spaink K (2002) Freedom of the Internet, our new challenge. 2002 (адрес в Интернете: http://www.spaink.net/english/osce_internetfreedom.html) [просмотрено 5 августа 2018 г.] упоминаются два взаимосвязанных случая. В первом случае, иск был подан в отношении интернет-страницы с сомнительными материалами нацистского толка. Хостинг этой страницы обеспечивала шведская компания Flashback. Суд постановил, что на странице не было нарушений законодательства Швеции по противодействию нацизму. Тем не менее один из активистов антифашистского движения инициировал масштабную кампанию против Flashback, тем самым оказав давление на интернет-провайдера Flashback, компанию Air2Net, и на магистрального оператора MCI/WorldCom. В результате MCI/WorldCom решила отключить Flashback несмотря на отсутствие каких-либо правовых оснований. Попытки Flashback найти альтернативного провайдера не увенчались успехом, поскольку почти все операторы работали через одного и того же магистрального оператора MCI/WorldCom. Второй случай произошел в Голландии. Небольшой голландский интернет-провайдер Xtended Internet был отключен своим американским провайдером более высокого уровня под давлением сайентологического лобби.

[19] Metz C. Facebook and Microsoft are laying a giant cable across the Atlantic // Wired, 26 мая 2016 г. (адрес в Интернете: http://www.wired.com/2016/05/facebook-microsoft-laying-giant-cable-across-atlantic/) [просмотрено 5 августа 2018 г.].

[20] IANA считается одной из старейших организаций по регулированию Интернета. Ее история началась в 1970-е гг., когда функции ассоциации выполнял один человек — специалист в области вычислительных систем Джонатан Постел, который тогда работал в Университете Южной Калифорнии. С 1998 г. функции IANA выполняет ICANN на основании договора с правительством США. После истечения срока действия этого договора 1 октября 2016 г. эти функции продолжила исполнять ICANN силами своего нового подразделения PTI. Функции IANA делятся на три категории: доменные имена (управлением корневыми DNS, домены .int и .arpa и ресурсы IDN), интернет-ресурсы (координация глобального пула IP-адресов и автономных номеров, в первую очередь, их предоставление региональным интернет-регистраторам) и распределение протоколов (управление системой исчисления интернет-протоколов в сотрудничестве с другими организациями по стандартизации). Подробнее см. https://www.iana.org/about [просмотрено 5 августа 2018 г.].

[21] В настоящее время действуют следующие национальные интернет-регистратуры: Американский регистр номеров Интернета (ARIN), Азиатско-Тихоокеанский сетевой информационный центр (APNIC), Реестр адресов Интернета для стран Латинской Америки и Карибского бассейна (LACNIC), Координационный центр распределения IP ресурсов сети Интернет в Европейском регионе (RIPE NCC — охватывает Европу и Ближний Восток) и Информационный центр африканской сети (AFRINIC). Подробное описание системы региональных интернет-регистратур см. http://www.ripe.net/internet-coordination/internet-governance/internet-technical-community/the-rir-system [просмотрено 5 августа 2018 г.].

[22] Drake W et al.. Internet Fragmentation: An Overview (адрес в Интернете: http://www3.weforum.org/docs/WEF_FII_Internet_Fragmentation_An_Overview_2016.pdf) [просмотрено 5 августа 2018 г.].

[23] Например, в 2000 г. Рабочая группа по проектированию Интернета (IETF) разработала технический стандарт RFC 2893 «Механизмы перехода для узлов и маршрутизаторов IPv6», в котором описываются механизмы перехода, «позволяющие обеспечить полную совместимость узлов с IPv4, что должно значительно упростить разворачивание IPv6 и в дальнейшем обеспечить переход всего Интернета на IPv6» (адрес в Интернете: https://www.ietf.org/rfc/rfc2893.txt) [просмотрено 5 августа 2018 г.].

[24] 8 июня 2011 г. был успешно проведен Международный день IPv6. После этого крупнейшие интернет-провайдеры, производители сетевого оборудования и интернет-компании по всему миру решили совместными усилиями обеспечить совместимость своих товаров и услуг с IPv6 не позднее 6 июня 2012 г., когда состоялась мировая премьера IPv6. К 2016 г., то есть четыре года спустя, глобальный трафик по IPv6 вырос более чем на 500%. Подробнее см. http://www.worldipv6launch.org [просмотрено 5 августа 2018 г.].

[25] См. комплексное и узкоспециализированное исследование по вопросу о безопасности TCP/IP: Chambers C et al. TCP/IP Security, Department of Computer and Information Science. Ohio State University (адрес в Интернете: http://www.linuxsecurity.com/resource_files/documentation/tcpip-security.html) [просмотрено 5 августа 2018 г.].

[26] Bavisi J (2011) What Security Issues does IPv6 Pose? // eSecurity Planet (адрес в Интернете: http://www.esecurityplanet.com/trends/article.php/3935356/What-Security-Issues-Does-IPv6-Pose.htm) [просмотрено 5 августа 2018 г.].

[27] Ashford W. IPv6: The security risks to business // Computer Weekly. 29 августа 2011 г. (адрес в Интернете: http://www.computerweekly.com/feature/IPv6-The-security-risks-to-business) [просмотрено 5 августа 2018 г.].

[28] Подробнее о группе см. http://www.etsi.org/technologies-clusters/technologies/next-generation-protocols [просмотрено 5 августа 2018 г.].

[29] Одним из немногих документов о структуре управления системой DNS является RFC 1591. Адрес в Интернете: http://www.ietf.org/rfc/rfc1591.txt [просмотрено 5 августа 2018 г.].

[30] ICANN (2016) Bylaws for Internet Corporation for Assigned Names and Numbers. Адрес в Интернете: https://www.icann.org/resources/pages/governance/bylaws-en [просмотрено 5 августа 2018 г.].

[31] Перечень действующих соглашений с регистратурами см. https://www.icann.org/resources/pages/registries/registries-agreements-en [просмотрено 5 августа 2018 г.].

[32] Регистраторы, желающие оказывать услуги по регистрации доменов в gTLD с прямым доступом к реестрам gTLD, должны быть аккредитованы в ICANN. Перечень таких регистраторов см. https://www.icann.org/registrar-reports/accredited-list.html [просмотрено 5 августа 2018 г.].

[33] Статистику по новым gTLD, включая перечень делегированных имен см. https://newgtlds.icann.org/en/program-status/statistics [просмотрено 5 августа 2018 г.].

[34] Отчет IANA о выделении ccTLD Палестине, см. https://www.iana.org/reports/2000/ps-report-22mar00.html [просмотрено 5 августа 2018 г.].

[35] Данные о регистратурах национальных доменов верхнего уровня приведены в Базе данных корневой зоны IANA. Адрес в Интернете: http://www.iana.org/domains/root/db [просмотрено 5 августа 2018 г.].

[36] Успешным примером многостороннего подхода к управлению национальными доменами считается опыт Бразилии. В деятельности национального регулятора по доменам могут принимать участие все ключевые участники, включая органы власти, деловое сообщество и гражданское общество. Подробнее см.: Alfonso C (2004) BR: CCTLD An asset of the commons, in MacLean D (ed) Internet Governance: A Grand Collaboration. New York: UN ICT Task Force, pp. 291—299. С отрывками можно ознакомиться здесь: http://books.google.ro/books?id=pEFAypES4t0C&printsec=frontcover&hl=ro#v=onepage&q&f=false [просмотрено 5 августа 2018 г.].

[37] Например, ЮАР использовала суверенное право как основание для

восстановления контроля над своим национальным доменом. Был принят закон, который гласит, что использование национального домена, выходящее за рамки, обозначенные правительством ЮАР, будет расцениваться как преступление. Напротив, опыт Камбоджи, где правительство забрало полномочия по управлению национальным доменом у неправительственной организации, часто называется примером неудачной передачи полномочий. Правительство снизило качество услуг и ввело более высокие тарифы, что усложнило регистрацию камбоджийских доменов. Для получения более подробной информации, см.: Klien N (2004) Internet Governance: Perspectives from Cambodia in MacLean D (ed) Internet Governance: A Grand Collaboration. New York: UN ICT Task Force, pp. 227–237. С отрывками можно ознакомиться здесь: http://books.google.ro/books?id=pEFAypES4t0C&printsec=frontcover&hl=ro#v=onepage&q&f=false [просмотрено 5 августа 2018 г.].

[38] Подробнее о делегировании и переделегировании национальных доменов верхнего уровня см. Delegating or redelegating a country-code top-level domain (ccTLD). Адрес в Интернете: http://www.iana.org/help/cctld-delegation [просмотрено 5 августа 2018 г.].

[39] ICANN GAC (2005) Principles for the Delegation and Administration of Country Code Top-Level Domains CANN GAC. Адрес в Интернете: https://gacweb.icann.org/display/GACADV/ccTLDs?preview=/28278844/28475457/ccTLD_Principles_0.pdf [просмотрено 5 августа 2018 г.].

[40] Файл корневой зоны находится в открытом доступе. http://www.iana.org/domains/root/files [просмотрено 5 августа 2018 г.].

[41] Список серверов корневой зоны, точек их подключения к сети и местоположения, а также регулирующих организаций см. http://www.root-servers.org/ [просмотрено 5 августа 2018 г.].

[42] Перечень 13 организаций, управляющих корневой зоной системы DNS, см. http://www.iana.org/domains/root/servers [просмотрено 5 августа 2018 г.].

[43] ISC Inc. (2003) Hierarchical Anycast for Global Distribution. Адрес в Интернете: http://ftp.isc.org/isc/pubs/tn/isc-tn-2003-1.html [просмотрено 5 августа 2018 г.].

[44] См. подробнее: Das D. List of top 4 alternative DNS servers to your ISP. 2015. Адрес в Интернете: http://www.snaphow.com/4402/list-of-top-4-alternative-dnsservers-to-your-isp/ [просмотрено 5 августа 2018 г.].

[45] Подробнее о проекте Yeti DNS см. https://yeti-dns.org [просмотрено 5 августа 2018 г.].

[46] Комплексный анализ проблем, связанных с альтернативными корневыми системами, см. Bertola V. Oversight and multiple root server systems. Адрес в Интернете: http://wgig.org/docs/book/Vittorio_Bertola%20.pdf [просмотрено 5 августа 2018 г.].

[47] Проблему нехватки пропускной способности каналов передачи данных призваны решать такие технологии передачи сигнала как стандарт беспроводной связи Long Term Evolution (LTE) или технология спектрального уплотнения каналов DWDM за счет увеличения пропускной способности (до терабита в секунду). Однако спрос все равно будет всегда опережать предложение.

[48] The Economist. America insists on net neutrality: The rights of bits. 24.09.2009. Адрес в Интернете: http://www.economist.com/node/14517422 [просмотрено 5 августа 2018 г.].

[49] Полный текст предложения компаний Verizon и Google «Открытый Интернет» см.: http://www.google.com/googleblogs/pdfs/verizon_google_legislative_framework_proposal_081010.pdf [просмотрено 5 августа 2018 г.].

[50] Скорость (битрейт), оговоренная в договоре с интернет-провайдером, на самом деле представляет максимальную, а не гарантированную скорость подключения.

[51] McCullagh D. European ISPs defend UN Internet tax // Cnet. 20.08.2012. Адрес в Интернете: http://news.cnet.com/8301-13578_3-57496581-38/european-isps-defendu.n-internet-tax/ [просмотрено 5 августа 2018 г.].

[52] Нерешенные на настоящий момент вопросы, которые будут предметом переговоров в будущем, указаны в квадратных скобках.

[53] Radunović V (2012) Network neutrality in law — a step forwards or a step backwards? // Diplo Blog. Адрес в Интернете: https://www.diplomacy.edu/content/network-neutrality-law-%E2%80%93-step-forwards-or-step-backwards [просмотрено 5 августа 2018 г.].

[54] Federal Communications Commission (2015) Open Internet Order. Адрес в Интернете: https://apps.fcc.gov/edocs_public/attachmatch/FCC-15-24A1.pdf[просмотрено 5 августа 2018 г.].

[55] Дело рассматривалось в Апелляционном суде Округа Колумбия. Текст решения суда см.: https://www.cadc.ucourts.gov/internet/opinions.nsf/3F95E49183E6F8AF85257FD200505A3A/$file/15-1063-1619173.pdf [просмотрено 5 августа 2018 г.].

[56] Регламент Европейского парламента и Совета Европейского союза 2015/2120 от 25 ноября 2015 г. об установлении мер относительно открытого доступа в Интернет и изменении Директивы 2002/22/ЕС об универсальных услугах и правах пользователей в отношении сетей электронных коммуникаций и услуг и Регламента (ЕС) 531/2012 о роуминге общественных сетей мобильной связи в пределах Союза. Адрес в Интернете: http://eur-lex.europa.eu/legalcontent/en/TXT/?uri=CELEX%3A32015R2120 [просмотрено 8 августа 2016 г.].

[57] Когда BEREC в июне 2016 г. опубликовал проект регламента о внедрении новых правил по сетевому нейтралитету национальными регуляторами, крупные европейские телекоммуникационные компании в ответ заявили, что реализация положений проекта «приведет к значительной неопределенности в том, что касается дохода от инвестиций в создание сетей пятого поколения (5G)». По их утверждению, в основе 5G лежит принцип сетевого сегментирования, который делает возможным сосуществование в рамках одной платформы широкого спектра бизнес-моделей с гарантией высокого качества обслуживания. С их точки зрения, предложение «чрезмерно директивно, заставляет телекоммуникационные компании проявлять излишнюю осторожность, что затруднит разворачивание сетей 5G и противоречит свойственной этому стандарту связи гибкости в реагировании в режиме реального времени на изменение запросов конечных пользователей за счет сегментирования». Другие организации, включая Европейский вещательный союз, не согласились с такой точкой зрения, заявив, что жесткие правила по обеспечению сетевого нейтралитета сыграют ключевую роль в разработке «открытой и совместимой технологической платформы связи 5G». См. подробнее: Patterson G et al. Manifesto for timely deployment of 5G in Europe (2016). Адрес в Интернете: http://telecoms.com/wp-content/blogs.dir/1/files/2016/07/5GManifestofortimelydeploymentof5GinEurope.pdf [просмотрено 5 августа 2018 г.]; и European Broadcasting Union. EBU response to the public consultation of draft BEREC guidelines on implementation of net neutrality rules. 2016. Адрес в Интернете: https://www.ebu.ch/files/live/sites/ebu/files/Publications/Positionpapers/EBU_response_BEREC_consultation_NN_guidelines_final_version_18072016.pdf [просмотрено 5 августа 2018 г.].

[58] Body of European Regulators for Electronic Communications. Guidelines on the Implementation by National Regulators of European Net Neutrality Rules. 2016. Адрес в Интернете: https://berec.europa.eu/eng/document_register/subject_matter/berec/regulatory_best_practices/guidelines/6160-berec-guidelines-on-the-implementation-by-national-regulators-of-europe-an-net-neutrality-rules [просмотрено 5 августа 2018 г.].

[59] Английская версия Кодекса по защите прав человека в Интернете в Бразилии (Marco Civil). Адрес в Интернете: https://www.giplatform.org/resources/text-brazilsnew-marco-civil [просмотрено 5 августа 2018 г.].

[60] TechnoLlama (2012) Chile enforces net neutrality for the first time, sort of. Адрес в Интернете: https://www.technollama.co.uk/chile-enforces-net-neutrality-for-the-first-time-sort-of [просмотрено 5 августа 2018 г.].

[61] European Digital Rights (2013). Slovenia has a net neutrality law. Адрес в Интернете: https://edri.org/edrigramnumber11-2slovenia-net-neutrality/ [просмотре но 5 августа 2018 г.].

[62] Electronic Frontier Foundation (2012) The Netherlands passes net neutrality legislation. Адрес в Интернете: https://www.eff.org/deeplinks/2012/05/netherlands-passes-net-neutrality-legislation [просмотрено 5 августа 2018 г.].

[63] Norwegian Communications Authority (2009). Guidelines for Internet neutrality. Адрес в Интернете: https://eng.nkom.no/technical/internet/net-neutrality/net-neutrality/_attachment/9222?_ts=1409aa375c1 [просмотрено 5 августа 2018 г.].

[64] Полный текст Декларации Комитета министров Совета Европы о сетевом нейтралитете 2010 г. см.: https://wcd.coe.int/ViewDoc.jsp?id=1678287 [просмотрено 5 августа 2018 г.]. Текст Рекомендаций Комитета министров по защите прав на свободу выражения мнений и неприкосновенность частной жизни применительно к сетевому нейтралитету 2016 г. см.: https://wcd.coe.int/ViewDoc.jsp?p=&Ref=CM/Rec(2016)1&Language=lanEnglish&Ver=original&Back-colorInternet=C3C3C3&BackColorIntranet=EDB021&BackColorLogged=F5D383&direct=true [просмотрено 5 августа 2018 г.].

[65] Internet Society. Net Neutrality. Адрес в Интернете: http://www.internetsociety.org/net-neutrality [просмотрено 5 августа 2018 г.].

[66] TACD (2015) Resolution on the open and neutral Internet. Адрес в Интернете: http://tacd.org/wp-content/uploads/2015/06/TACD-INFOSOC-Resolution-on-Net-Neutrality-2015-GREEN.pdf [просмотрено 5 августа 2018 г.].

[67] Global Multistakeholder Meeting on the Future of Internet Governance (2015) NETmundial Multistakeholder Statement. Адрес в Интернете: http://netmundial.br/netmundial-multistakeholder-statement/ [просмотрено 5 августа 2018 г.].

[68] Radunović V (2012). Can free choice hurt open Internet markets? // Diplo Blog. Адрес в Интернете: http://www.diplomacy.edu/blog/can-free-choice-hurt-open-internet-markets [просмотрено 5 августа 2018 г.].

[69] International Telecommunication Union (2016) ITU towards 'IMT for 2020 and beyond' (адрес в Интернете: http://www.itu.int/en/ITU-R/study-groups/rsg5/rwp5d/imt-2020/Pages/default.aspx) [просмотрено 5 августа 2018 г.].

[70] Текущую вервию стандартов, проектов стандартов и предложений по стандартам Интернета см. в директории Official Internet Protocol Standards: https://www.rfc-editor.org/standards) [просмотрено 5 августа 2018 г.].

[71] World Wide Web Consortium. Standards. Адрес в Интернете: http://www.w3.org/standards/ [просмотрено 5 августа 2018 г.].

[72] Под латентностью применительно к компьютерным сетям понимается время, которое требуется пакету данных для прохождения от одной точки к другой в пределах сети.

[73] Cisco (2015) Fog Computing and the Internet of Things: Extend the Cloud to Where the Things Are. Адрес в Интернете: https://www.cisco.com/c/dam/en_us/solutions/trends/iot/docs/computing-overview.pdf [просмотрено 5 августа 2018 г.].

[74] Oracle (2016) Oracle Unveils Suite of Breakthrough Services to Help Simplify Cloud Adoption by Global Corporation. Адрес в Интернете: https://www.oracle.com/corporate/pressrelease/oracle-cloud-at-customer-032416.html [просмотрено 5 августа 2018 г.].

[75] The Open Group (2013) Cloud Computing Portability and Interoperability. Адрес в Интернете: http://www.opengroup.org/cloud/cloud_iop/ [просмотрено 5 августа 2018 г.].

[76] IDC (2014) The Digital Universe of Opportunities: Rich Data and the Increasing Инфраструктура Value of the Internet of Things. Адрес в Интернете: http://www.emc.com/leadership/digital-universe/2014iview/digital-universe-of-opportunities-vernon-turner.htm [просмотрено 5 августа 2018 г.].

[77] Verizon (2016) State of the Market: Internet of Things 2016. Адрес в Интернете: http://www.verizon.com/about/our-company/state-of-the-market-internet-of-things [просмотрено 5 августа 2018 г.].

[78] IITU, Cisco Systems (2016) Harnessing the Internet of Things for Global Development. Адрес в Интернете: https://www.itu.int/en/action/broadband/Documents/Harnessing-IoT-Global-Development.pdf [просмотрено 5 августа 2018 г.].

[79] Schmid S et al. (2016) EnLighting: An Indoor Visible Light Communication System Based on Networked Lights Bulbs. Адрес в Интернете: https://s3-us-west-1.amazonaws.com/disneyresearch/wp-content/uploads/20160615205959/EnLighting-An-Indoor-Visible-Light-Communication-System-based-on-Networked-Light-Bulbs-Paper.pdf [просмотрено 5 августа 2018 г.].

[80] В Голландии в июле 2016 г. местная телекоммуникационная компания KPN запустила сеть межмашинного взаимодействия LoRa для обслуживания устройств Интернета вещей. В Южной Корее работа над созданием коммерческой сети для устройств Интернета вещей ведут компании Samsung и SK Telecom.

[81] В сентябре и октябре 2016 г. крупнейшие сайты оказались недоступными в ходе двух DDoS-атак, организованных с использованием устройств Интернета вещей. В атаках против сайта американского специалиста в области безопасности и французского интернет-оператора были задействованы более миллиона устройств Интернета вещей. Вторая атака была направлена против систем, использующих услуги DNS-оператора Dyn, против которого было зафиксировано три атаки за один день. Эти атаки сказались на работе Twitter, PayPal, Netflix, Airbnb, Amazon, CNN, а также ряда интернет-изданий. См. подробнее: Rash W. Weak Devices security turns IoT into powerful weapon in DDos attacks // Eweek, 01.10.2016. Адрес в Интернете: http://www.eweek.com/security/weak-device-security-turns-iot-into-powerful-weapon-in-ddos-attacks.html [просмотрено 5 августа 2018 г.]. Wikipedia (2016) 2016 Dyn cyberattack. Адрес в Интернете: https://en.wikipedia.org/wiki/2016_Dyn_cyberattack [просмотрено 5 августа 2018 г.].

[82] Greenberg A. Inside Google's Internet Justice League and its AI-powered war on trolls // Wired, 19.09.2016. Адрес в Интернете: https://www.wired.com/2016/09/inside-googles-internet-justice-league-ai-powered-war-trolls/ [просмотрено 5 августа 2018 г.].

[83] Romm T Tech companies launch new AI coalition // Politico, 11.10.2015. Адрес в Интернете:http://www.politico.com/story/2016/10/tech-companies-launch-new-ai-coalition-229600 [просмотрено 5 августа 2018 г.].

[84] European Parliament Committee on Legal Affairs (2016) Draft report with recommendations to the Commission on Civil Law Rules on Robotics. (адрес в Интернете: http://www.europarl.europa.eu/oeil/popups/ficheprocedure.do?reference=2015/2103(INL)&l=en) [просмотрено 5 августа 2018 г.].

[85] US National Science and Technology Council (2016) The National Artificial Intelligence Research and Development Strategic Plan. Адрес в Интернете: https://obamawhitehouse.archives.gov/sites/default/files/whitehouse_files/microsites/ostp/NSTC/national_ai_rd_strategic_plan.pdf [просмотрено 5 августа 2018 г.].

[86] UK Parliamentary Committee on Science and technology (2016) Robotics and artificial intelligence. Адрес в Интернете: https://publications.parliament.uk/pa/cm201617/cmselect/cmsctech/145/145.pdf [просмотрено 5 августа 2018 г.].

[87] IBM Institute for Business Value (2016) Redefining Boundaries. Insights from the Global C-suite Study. Адрес в Интернете: https://public.dhe.ibm.com/com-

mon/ssi/ecm/gb/en/gbe03695usen/ GBE03695USEN.PDF [просмотрено 5 августа 2018 г.].

[88] Подробнее о сотрудничестве между поставщиками телекоммуникационных услуг и OTT-провайдерами см.: Body Body of European Regulator for Electronic Communications (2016) Report on OTT services. Адрес в Интернете: http://www.stibbe.com/~/media/03%20news/newsletters/brussels/bru%20tmt%20berec%20report%20on%20ott%20services.pdf [просмотрено 5 августа 2018 г.].

[89] Подробнее о правовых и нормативных подходах к вопросам конвергенции см.: ITU, infoDev. Impact of Convergence. Адрес в Интернете: http://www.ictregulationtoolkit.org/toolkit/6.4 [просмотрено 5 августа 2018 г.].

Раздел 3

Безопасность

Безопасность

Кибербезопасность

Интернет был изначально создан для использования ограниченным кругом лиц, в основном инаучным сообществом. Они открыто общались между собой, а о безопасности никто не задумывался.

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

Для современного общества Интернет с его 3 млрд. пользователей стал критически важным объектом инфраструктуры, а наличие уязвимостей в Интернете свидетельствует об уязвимости общества в целом. Растет взаимосвязанность финансового сектора, государственных услуг, сферы безопасности, школ, больниц, а также граждан, что также обусловлено развитием Интернета.

Кроме того, в киберпространстве находят свое отражение межгосударственные противоречия, что иногда приводит к киберинцидентам. Такие события, в особенности кибериниденты, связанные с критически важными объектами инфраструктуры, могут иметь негативные последствия для государства, его экономической жизни и благосостояния населения. Например, если Швейцария подвергнется кибератаке общенационального масштаба, потери могут превысить 500 млн. евро в день[1].

Классификация вопросов кибербезопасности

Вопросы кибербезопасности можно классифицировать по трем критериям:

- тип действий. Классификация, основанная на типе действий, может включать: перехват данных, нарушение целостности данных, нелегальный доступ, внедрение шпионского программного обеспечения, изменение данных, информационную диверсию, нарушение нормального предоставления услуг (DoS-атаки) и кражу личности.

- Тип злоумышленника. Типы возможных злоумышленников: преступники, анархисты, хакеры, революционеры, террористы, спецслужбы, оборонные и военные ведомства.
- Тип цели. Потенциальные цели весьма многочисленны: начиная с индивидов, частных компаний, организаций гражданского общества и государственных учреждений до объектов основной инфраструктуры Интернета (телекоммуникационные операторы, интернет-провайдеры, точки обмена трафиком, дата-центры), критически важных объектов инфраструктуры (энерго- и водоснабжение, промышленные объекты, объекты транспортной инфраструктуры и т. п.), а также военных объектов.

Для регулирования сферы кибербезопасности разработаны специальные принципы, приняты документы и созданы специализированны ведомства. Концепция кибербезопасности охватывает ряд областей:

- Защита ключевых объектов информационной инфраструктуры (Critical information infrastructure protection — CIIP) имеет все большее значение, поскольку в современном мире критически важные объекты инфраструктуры, включая энергетику, водоснабжение, связь и финансовый сектор, зависят от Интернета и других компьютерных сетей для обмена информацией. К ключевым объектам информационной инфраструктуры (CII — critical information infrastructure) относится не только оборудование и средства связи между устройствами (сетевая безопасность), но и протоколы, дата-центры и ключевые ресурсы Интернета.
- Киберпреступностью называются преступления, совершенные в Интернете или с помощью компьютерных систем. К ним относятся как традиционные виды преступлений, совершенные с использованием киберпространства (например, различные виды мошенничества), преступления, связанные с технологическим прогрессом (например, мошенничество с банковскими картами, растление и эксплуатация несовершеннолетних с использованием Интернета), так и новые виды преступлений, появившиеся вместе с Интернетом (DoS-атаки и автоматизированное накручивание переходов по рекламным ссылкам), а также коммерциализация, преимущественно на теневом рынке, инструментов, позволяющих совершать другие преступления (вирусы и ботнеты). Наиболее активно международное сотрудничество идет по

вопросу о борьбе с растлением и эксплуатацией несовершеннолетних с использованием Интернета. Повышение уровня безопасности для всех пользователей, в особенности детей, посредством образования и повышения осведомленности, является важным аспектом деятельности по предотвращению преступлений, мошенничества или домогательств. Это и называется «безопасностью в Интернете».

- Киберконфликты или, на языке обывателей, кибервойны, находятся в центре внимания СМИ, но не вызывают интереса у регуляторов и законодательной власти. Сотрудничество по вопросам киберконфликтов осуществляется в трех основных областях: правила поведения в киберконфликтах (в частности, применимы ли существующие нормы права и, в первую очередь Гаагские конвенции, к киберпространству, и если нет, то какие новые правовые инструменты необходимо создать?); оружие и вопросы разоружения (как включить кибероружие в процесс разоружения?); и гуманитарное право (каким образом обеспечить применение Женевских конвенций в отношении киберконфликтов?). На первый план в политической жизни и дипломатических отношениях выходят вопросы экономического кибершпионажа, взлома информационных систем с целью организации утечек документов по политическим вопросам и подрывная деятельность, которую можно рассматривать как военные действия. Все больше Интернетом пользуются террористы для распространения информации, связи, пропаганды и осуществления терактов, то есть речь идет о кибертерроризме. Как правило, этот вопрос рассматривается как проблема национальной и глобальной безопасности, несмотря на то, что преследование таких преступников осуществляется в соответствии с нормами национального уголовного права.

Угрозы в области кибербезопасности

Угрозы безопасности могут исходить от разных людей и организаций, руководствующихся разными мотивами. Когда мишенью становятся физические лица, преступники стараются получить доступ к данным и персональной информации, как правило, с целью получения денег или каких-то других активов. Наиболее распространенными угрозами для интернет-пользователей

являются различные виды вредоносного программного обеспечения, включая вирусы и шпионское ПО, фишинг и электронное мошенничество. Для проникновения в корпоративные и государственные системы в целях шпионажа используются более сложные решения. Чтобы спровоцировать сбой в работе сторонней системы или сети, можно использовать набор киберсредств и атак.

Средства, используемые в атаках, которые направлены на нарушение конфиденциальности, целостности и доступности данных и систем, становятся все более разнообразными и технически совершенными.

К вредоносному программному обеспечению (зловредам) относятся вирусы, шпионское программное обеспечение и другие виды нежелательного программного обеспечения, установленного на цифровые устройства без разрешения или исполняющего действия без санкции пользователя, как правило, в пользу автора атаки. Такие программы могут наносить вред устройствам и могут использоваться для кражи персональных данных, отслеживания и контроля над действиями в сети, рассылки спама и мошенничества, а также для заражения других сетевых устройств. Кроме того, они могут без разрешения распространять некорректную интернет-рекламу.

К такому вредоносному программному обеспечению относятся вирусы, трояны, рекламное ПО и шпионское ПО. Вирусы могут распространяться сами по себе и заражать другие устройства без ведома пользователя. Хотя некоторые вирусы ничем не проявляют себя, большинство разрабатываются с целью захвата данных или оказания влияния на работу устройств (переформатирование жесткого диска, использование памяти компьютера и т.п.). Троян представляет собой программу, содержащую зловредное ПО или вредоносный контент, обеспечивающий преступнику возможность обхода системы безопасности, проникновения в устройство и удаленного запуска программ. Троянами могут пользоваться киберворы и хакеры, стремящиеся получить доступ к системе. Как правило, пользователей обманом заставляют скачать и запустить троян на своем устройстве с использованием различных психологических уловок. После активации троян дает возможность киберпреступникам шпионить за пользователями, красть конфиденциальную информацию и получить несанкционированный доступ к их системам.

Рекламное ПО предназначено для сбора маркетинговой и иной информации без ведома пользователя или перенаправления поисковых запросов

на определенные рекламные сайты. Шпионское ПО используется для слежки за пользователями, негласного сбора информации о них и ее передачи заинтересованным лицам. К такой информации могут относиться история просмотра сайтов, информация о браузере и системе, IP-адрес компьютера, а также такая конфиденциальная информация, как адреса электронной почты и пароли. Кроме того, вредоносное ПО может применяться для перехвата браузеров, то есть изменения настроек браузера без разрешения пользователя. Такие программы могут создавать ярлыки на рабочем столе, отображать всплывающую рекламу, а также менять домашнюю страницу или поисковую систему по умолчанию.

Ботнеты (бот-сети) представляют собой сети зараженных устройств, исполняющих определенные действия без ведома их владельцев. Устройства становятся частью ботнета в результате заражения определенным видом вредоносного ПО, дающего возможность злоумышленнику удаленно контролировать устройство жертвы. Ботнеты используются для совершения различных видов преступлений и атак: рассылки спама, заражения вредоносным ПО новых устройств, накручивания просмотров рекламы или кражи идентичности. Пожалуй, наибольшее беспокойство вызывает использование ботнетов для проведения DDoS-атак (рис. 11).

Рисунок 11. Ботнет

По мнению исследователей и компаний, занимающихся вопросами кибербезопасности, ботнеты могут стать самой большой угрозой безопасности

Интернета, поскольку они способны усугублять действие вирусов и других вредоносных программ, способствовать краже информации и увеличению мощности сетевых атак. Чтобы наглядно показать масштаб этой угрозы, можно привести пример ботнета Simda, который был обезврежен в апреле 2015 г.: в зараженную сеть входили компьютеры в 190 странах и 14 командных серверов из 5 стран[2].

Сетевые атаки (DoS-атаки) заключаются в отправке на атакуемый ресурс (компьютер или сайт) огромного количества запросов, превышающих пропускную способность сети, приложения или службы, что приводит к ошибке «отказ в обслуживании» и лишает пользователей доступа к ресурсу. Как правило, мишенью таких атак становятся компании, а не физические лица. Распределенными сетевыми атаками «отказ в обслуживании» (DDoS-атаки) называются атаки, в которых для вывода из строя одной мишени используется множество зараженных компьютеров.

Обычно DoS-атаки не приводят к краже информации или нарушению безопасности. Однако они наносят пострадавшей организации или лицу финансовый урон, вызывают простои (становятся недоступными определенные сетевые услуги, прекращают работу сайты, электронная почта не доставляется на определенные адреса и т. п.).

Фишингом называется одна из разновидностей социальной инженерии, цель которой состоит в том, чтобы обманным путем побудить людей сделать то, что они в ином случае делать не будут, как то: предоставить доступ к конфиденциальной информации (например, имени пользователя и паролю), открыть неизвестный файл или перейти по ненадежной ссылке. Иногда авторы атаки выдают себя в переписке по электронной почте, социальных сетях или в других интернет-услугах за существующие и пользующиеся доверием организации (например, банк), тем самым провоцируя получателя раскрыть свои персональные данные или конфиденциальную информацию.

Электронное мошенничество — вид мошенничества, основанный на использовании злоумышленниками одного или нескольких интернет-ресурсов, например, электронной почты и сайтов, для доставки жертве обманных предложений (как правило, речь идет о коммерческих или инвестиционных предложениях, обещаниях легкого заработка, недобросовестных услугах в области здравоохранения или больших скидках в интернет-магазинах). Та-

кой вид мошенничества часто сводится к мошенничеству с использованием электронной почты или социальных сетей.

Политика и надзор в области кибербезопасности

Вопросам кибербезопасности посвящено множество инициатив на национальном, региональном и международном уровнях. На национальном уровне растет количество законодательных актов и судебных дел в области кибербезопасности, которые направлены на борьбу с киберпреступностью, а также на защиту критически важной информационной инфраструктуры от саботажа и атак террористов или враждующих сторон. Сложно найти развитую страну, где не выдвигались бы какие-либо инициативы, связанные с кибербезопасностью. На региональном и международном уровнях существует множество инициатив и программ.

Международная деятельность в области кибербезопасности

Организация Объединенных Наций

Вопросы кибербезопасности обсуждаются в ООН уже достаточно давно. В 1998 г. Российская Федерация внесла на рассмотрение Первого комитета Генеральной Ассамблеи ООН проект резолюции о достижениях в сфере информатизации и телекоммуникаций в контексте международной безопасности[3]. В 2004 г. в рамках ООН была создана Группа правительственных экспертов (UN GGE), которой было поручено выявить существующие и потенциальные угрозы в области кибербезопасности и способствовать сотрудничеству для их нейтрализации. Срок полномочий группы продлевался в 2009, 2011, 2013 и 2015 гг. В своем докладе 2013 г. Группа правительственных экспертов подтвердила применимость сложившихся норм международного права к использованию ИКТ государствами. В докладе за 2015 г. указано, что государствам не следует заниматься или умышленно поддерживать деятельность с использованием ИКТ, направленную на нанесение ущерба критически важным объектам инфраструктуры или иным образом затрудняющую ее использование[4].

Еще одной возможной площадкой для обсуждения вопросов кибербезопасности на высоком дипломатическом уровне стала Конференция ООН по разоружению. Пока план работы по этому направлению не согласован, несмотря на предложения ряда членов, включая Китай, включить вопросы кибербезопасности в повестку конференции[5].

Управление по наркотикам и преступности ООН (УНП ООН) играет ведущую роль в борьбе с киберпреступностью. Некоторые нормативно-правовые документы, подготовленные УНП ООН, например Конвенция Организации Объединенных Наций против транснациональной организованной преступности (UNTOC), не используются в достаточной степени в области борьбы с киберпреступностью. Как правило, речь идет об организованной (с участием не менее трех человек) и трансграничной (охватывает несколько государств или ведется группой в одной стране с последствиями для другой страны) преступности.

Международный союз электросвязи

По решению Всемирной встречи на высшем уровне по вопросам информационного общества (WSIS) 2005 г., обязанность по ведению дальнейшей работы по Направлению деятельности С5 «Укрепление доверия и безопасности при использовании ИКТ» Тунисской повестки была возложена на МСЭ.

В сферу компетенции МСЭ входит ряд аспектов проблемы кибербезопасности. Однако организация правомочна принимать решения (или, скорее, устанавливать стандарты) лишь по немногим вопросам в области безопасности и телекоммуникационной инфраструктуры. В основном МСЭ занимается исследовательской деятельностью, проведением информационных кампаний и подготовкой кадров.

Одной из наиболее заметных инициатив МСЭ является «Глобальная программа кибербезопасности» (Global Cybersecurity Agenda — GCA)[6], которая начала осуществляться по инициативе Генерального секретаря МСЭ в 2007 г. в целях поддержки международного сотрудничества в деле укрепления доверия и безопасности в информационном обществе. GCA призвана повысить эффективность взаимодействия всех заинтересованных сторон и является продолжение существующих инициатив в этой области, не пытаясь дублировать их функции. В сотрудничестве с Международным многосторон-

ним партнерством против киберугроз (International Multilateral Partnership against Cyber Threats — IMPACT) МСЭ также оказывает поддержку в деле реализации решений и программ в сфере кибербезопасности. Деятельность GCA осуществляется по пяти основным направлениям: правовые меры, меры технического и процедурного характера, организационные структуры, подготовка кадров и международное сотрудничество.

МСЭ также разработал программу «Глобальный индекс кибербезопасности» (Global Cybersecurity Index — GCI), многостороннюю инициативу по оценке деятельности стран в области обеспечения кибербезопасности[7].

Форум по управлению Интернетом

Вопросы кибербезопасности занимали важное место в повестке IGF начиная с первой встречи форума в 2006 г. Этой проблеме была посвящена одна из основных сессий и ряд семинаров на IGF в ноябре 2015 г. в г. Жуан-Песоа, Бразилия, в ходе которых особое внимание было уделено вопросам безопасности, шифрования и укрепления доверия[8]. В целом, вопросам, связанным с кибербезопасностью, была посвящена пятая часть всех мероприятий в рамках IGF 2015 г. В 2016 г. темой Форума по обмену передовым опытом IGF (IGF Best Practice Forum) была выбрана кибербезопасность с акцентом на активизацию сотрудничества и взаимодействия заинтересованных сторон в этой области. Хотя IGF не правомочен принимать решения или разрабатывать рекомендации, проведение форума дает возможность его участникам открыто обсуждать его темтатику, сотрудничать друг с другом, обмениваться информацией и добровольными регламентами, разработанными в рамках IGF Best Practice Forum. Форум публикует доклад по итогам каждой тематической сессии.

Глобальная конференция по киберпространству

Глобальная конференция по киберпространству (Global Conference on Cyberspace — GCCS) представляет собой серию конференций о принципах «управления поведением пользователей киберпространства»[9]. Иногда такие конференции называют «лондонским процессом», поскольку первая конференция состоялась в Лондоне в 2011 г. Вторая конференция прошла в Будапеште в 2012 г., третья — в Сеуле в 2013 г., а четвертая состоялась в Гааге в 2015 г.

На конференции GCCS собираются официальные лица разных стран, в том числе на уровне министров, а также представители компаний и гражданского общества. Хотя никаких заключительных документов по итогам GCCS не принимается, за исключением «Заявления председателя», и такие конференции не связаны с подписанием каких-либо формальных договоров, проведение таких мероприятий является отличной возможностью обсудить насущные вопросы в духе сотрудничества и провести переговоры по возможным будущим соглашениям, которые планируется заключить в других форматах.

По итогам конференции GCSC 2015 г. был учрежден Глобальный форум по киберэкспертизе (Global Forum on Cyber Expertise — GFCE), призванный способствовать обмену опытом, выявлению недостатков и дополнению существующих программ по наращиванию потенциала. В работе форума принимают участие представители национальных правительств, международных компаний и частного сектора, которые разрабатывают различные инициативы по наращиванию потенциала и подготовке кадров в области кибербезопасности в сотрудничестве с техническим, гражданским и академическим сообществом. Участники конференции 2015 г. приняли «Гаагскую декларацию», в которой подчеркивается необходимость продолжения деятельности по наращиванию потенциала в этой области, обмену передовым опытом и расширению международного сотрудничества[10].

НАТО

Будучи организацией по обеспечению коллективной безопасности, в вопросах кибербезопасности НАТО уделяет особое внимание кибероборонe. Стремительное изменение характера угроз по мере растущей зависимости от технологий и Интернета не осталось незамеченным членами НАТО. Вопросы кибероборонe стали неотъемлемой частью стратегий и программ альянса, что было зафиксировано даже на уровне доктрины этой организации. В 2016 г. 28 стран – членов НАТО признали киберпространство четвертой оперативной средой наравне с сухопутным, морским и воздушным пространством[11].

Действующая версия «Официальной политики НАТО в сфере кибероборо-

роны» (NATO Policy on Cyber Defence) была принята в 2014 г. В этом документе, среди прочего, изложен процесс оказания содействия странам-членам по информированию населения, подготовке кадров и проведению учений и подчеркнута необходимость дальнейшего развития сотрудничества со странами-партнерами, международными организациями и представителями частного сектора. Хотя основной целью кибероборонs признается защита средств связи и информационных систем, находящихся в собственности организации или используемых ею, не меньшее значение имеет надежность и безопасность национальной инфраструктуры стран – членов НАТО.

В 2009 г. в Центре повышения квалификации в области кибероборонs НАТО (Cooperative Cyber Defence Centre of Excellence — CCD COE) стартовал так называемый «таллиннский процесс» – серия «исследовательских и образовательных программ по международному праву в области киберпространства», включавшая научно-практические семинары по «Таллинскому руководству по применению международного права к кибервойнам», в котором излагались предложения в отношении применения норм международного права к киберпространству[12]. Кроме того, Центр повышения квалификации в области кибероборонs подготовил «Рамочное руководство по национальной кибербезопасности» (National Cyber Security Framework Manual), в котором собрана подробная справочная и теоретическая информация, необходимая для понимания различных аспектов национальной кибербезопасности на разных уровнях. Вопросы национальной кибербезопасности рассматриваются на четырех уровнях: политическом, стратегическом, операционном и тактическом/техническом. Каждый уровень имеет свою специфику, которая анализируется в отдельном разделе руководства. В руководстве также приводятся примеры институционального оформления системы национальной кибербезопасности от координационных органов высокого уровня до органов по преодолению кризисов, связанных с киберпространством, и аналогичных ведомств[13].

Деятельность в области кибербезопасности на региональном уровне

На региональном уровне все больше и больше организаций осознают важность темы кибербезопасности и занимаются разработкой стратегий, рекомендаций и конвенций, включая Конвенцию о киберпреступности Совета Европы, Стратегию АТЭС по обеспечению безопасности в интернет-пространстве, Стратегию кибербезопасности ЕС, Решение по мерам укрепления доверия ОБСЕ и Африканскую конвенцию по кибербезопасности.

Европа

Одним из первых регионов, занявшихся проблемой кибербезопасности, стала Европа. Принятая Советом Европы Конвенция о киберпреступности[14] вступила в силу 1 июля 2004 г. Этот документ стал основой для многих других нормативно-правовых документов по вопросам кибербезопасности на региональном и национальном уровнях по всему миру. Конвенция была ратифицирована европейскими странами, а также США, Канадой, Японией и рядом других неевропейских государств, и остается важнейшим международным правовым документом в области цифровых технологий. Поскольку конвенцию ратифицировали отдельные страны за пределами Европы, обсуждался вопрос о придании ей статуса международной конвенции по кибербезопасности. Однако некоторые страны не выражают желания стать участниками конвенции по разным причинам: от чисто символических (не участвовали в разработке документа) до существенных (например, возможность трансграничных расследований).

В ЕС существует два основных документа по вопросам кибербезопасности: Стратегия кибербезопансости и Директива по безопасности сети и информационных систем (NIS Directive). В стратегии закреплены стратегические приоритеты и описаны действия, направленные на решение проблем безопасности в киберпространстве с акцентом на достижение киберустойчивости к угрозам, существенное снижение уровня преступности в киберпространстве, разработку политики кибероборонs и средств ее обеспечения, а также промышленных и технологических ресурсов для кибербезопасности, и разработка последовательной международной политики ЕС в отношении киберпространства[15]. В директиве нашли свое отражение меры, которые должны принять страны – члены ЕС для обеспечения высокого уровня кибербезопасности на всей территории союза. К таким мерам относятся, в частности, принятие национальных стратегий по сетевой и ин-

формационной безопасности, определение полномочных органов власти в этой области и создание групп реагирования на инциденты, связанные с компьютерной безопасностью (Computer Security Incident Response Teams — CSIRTs), и выявление операторов основных услуг, которые обязаны принять соответствующие меры[16].

Работа в области кибербезопасности ведется и в рамках ОБСЕ. В частности, организация занимается разработкой мер по укреплению доверия. Обычно такие инициативы направлены на улучшение межгосударственных отношений, обеспечение мирного урегулирования конфликтов или предотвращение военной конфронтации. Серьезного внимания заслуживают два решения Постоянного совета ОБСЕ по мерам укрепления доверия применительно к киберпространству. В 2013 г. ОБСЕ приняла первый пакет мер по укреплению доверия с целью снижения риска начала конфликтов из-за ИКТ[17]. Речь идет о добровольных мерах, включая обмен мнениями и передовым опытом в отношении угроз, содействие сотрудничеству с компетентными органами на национальном уровне, проведение консультаций с целью снижения риска возникновения недопонимания и возможных трений либо конфликта, развитие национальной нормативно-правовой базы по обмену информацией и согласование терминологии по вопросам кибербезопасности. В 2016 г. был принят второй пакет мер по укреплению доверия, распространивший их, в частности, на сотрудничество в формате государственно-частного партнерства (ГЧП)[18].

В ближайшее время в рамках ОБСЕ может быть согласован очередной пакет мер по укреплению доверия. Кроме того, по мере включения указанных мер доверия в дипломатический оборот, не исключено, что такие инициативы могут стать предметом обсуждения в Группе правительственных экспертов ООН.

Америка

В 2003 г. Организация американских государств (ОАГ) приняла Межамериканскую стратегию кибербезопасности (Inter-American Cyber-Security Strategy)[19], в рамках которой планировалось объединить усилия трех связанных с организацией объединений: Межамериканского комитета по борьбе с терроризмом (CICTE), Объединения министров юстиции и других министров или генеральных прокуроров Американского континента (REMJA) и Межамериканской телекоммуникационной комиссии (CITEL). Данные группы ведут работу со странами-членами по реализации программ, направленных на предотвращение киберпреступности и защиту объектов критической инфраструктуры посредством законодательных инициатив и административных мер. В состав REMJA входит Рабочая группа по киберпреступности, которая проводит семинары по подготовке кадров стран-членов в области разработки законодательных и административных мер в отношении киберпреступности и электронных улик[20].

Азия

В Азии вопросы кибербезопасности, принятия мер по укреплению доверия в этой области и борьбы с киберпреступностью находятся в ведении Регионального форума по безопасности Ассоциации стран Юго-Восточной Азии (АСЕАН). В 2012 г. на форуме было принято министерское заявление о необходимости активизации регионального сотрудничества по вопросам безопасности ИКТ[21]. В 2013 г. вопросы кибербезопасности снова оказались на повестке форума с акцентом на борьбу с терроризмом и транснациональной преступностью. По итогам совещания Старших должностных лиц по международной преступности было решено создать Рабочую группу по киберпреступности[22].

Серьезное внимание вопросам кибербезопасности уделяет Шанхайская организация сотрудничества (ШОС), в состав которой входят Китай, Россия и страны Центральной Азии. В рамках ШОС заключено соглашении о сотрудничестве по обеспечению международной информационной безопасности. Кроме того, в конце 2011 г. члены ШОС внесли в ООН документ «Правила поведения в области обеспечения международной информационной безопасности (МИБ)», а в 2015 г. представили его обновленную версию[23].

Африка

Центральное место в африканской политике по кибербезопасности занимает разработка Конвенции Африканского союза по кибербезопасности

и защите персональных данных[24]. В настоящее время конвенция находится на стадии ратификации. В целом, основной проблемой африканских стран является наращивание потенциала учреждений национального и регионального уровня по обеспечению кибербезопасности.

Двухсторонняя деятельность

Все больше стран используют двухсторонние каналы для решения проблем в области кибербезопасности в различных форматах, от двухсторонних договоров и соглашений о взаимодействии до неофициальных консультаций. Так, США заключили договоры о взаимной правовой помощи по вопросам кибербезопасности более чем с 20 странами. Многие государства заключили двусторонние соглашения о сотрудничестве в области кибербезопасности, которые предусматривают обмен информацией и координация действий.

Кроме того, страны, играющие ведущую роль в области кибербезопасности, используют двухсторонние каналы для активизации сотрудничества и предотвращения конфликтов. Например, Китай ведет диалог по этой проблематике как с США, так и с ЕС. Австралия поддерживает контакты по вопросам функционирования киберпространства с Китаем, США, Южной Кореей, Индией и Новой Зеландией. Индия и Россия ведут диалог по вопросам кибербезопасности, а в 2016 г. между этими странами было заключено официальное соглашение по сотрудничеству в этой области.

Инициативы технического и научного сообществ

Компьютерные группы реагирования на чрезвычайные ситуации (CERT) и Группы реагирования на инциденты, связанные с компьютерной безопасностью (CSIRT), играют центральную роль в техническом сотрудничестве по вопросам кибербезопасности. Группы CERT разных стран взаимодействуют друг с другом на региональном уровне. Координацией работы международной сети национальных групп CERT занимается Форум групп реагирования на инциденты и обеспечения безопасности (FIRST).

Инициативы частного сектора

Значительное число инициатив по повышению уровня безопасности в Интернете исходит от частного сектора, в частности, от крупнейших производителей программного и аппаратного обеспечения. С одной стороны, их участие в деятельности по укреплению международной кибербезопасности обусловлено необходимостью усовершенствования технологий и регулирования, но, с другой стороны, повышение доверия среди конечных пользователей к их технологиям соответствует их собственным коммерческим интересам.

Так, компания Microsoft подготовила пакет норм в области киберпространства для снижения уровня конфликтности в сети[25], став первой компанией, выступившей с такой инициативой, ведь обычно вопросами поддержания международного мира занимаются дипломаты и государства. Microsoft в сотрудничестве с ассоциацией High Technology Crime Investigation Association (HTCIA), создала портал сообщества по борьбе с преступлениями в цифровом пространстве (Digital Crimes Community Portal) для оказания помощи правоохранительным органам в проведении расследований.

Компания Cisco разработала ряд решений по сетевым сертификатам безопасности для профессионалов и организаций, занимающихся информационными технологиями.

В транснациональных компаниях по созданию программного и аппаратного обеспечения, включая Microsoft, SAP и Cisco, отделы внешних связей и сотрудничества с университетами активно развивают отношения с ведущими университетами, государственными ведомствами, профессиональными организациями и отраслевыми партнерами с целью содействия исследовательской и образовательной деятельности и инновациям. Такое сотрудничество реализуется в рамках различных программ: это совместные исследовательские проекты научно-исследовательских институтов и филиалов компаний на местах, выделение исследовательских грантов, помощь с проведением конференций, финансирование диссертационных работ и другие виды сотрудничества с университетами, учреждениями и школами по распространению инноваций.

Основные трудности на пути преодоления проблем в области кибербезопасности

Терминологическая путаница в области кибербезопасности

Интернет как направление государственной политики — сфера достаточно новая. Поэтому неудивительно, что в этой области до сих пор сохраняется терминологическая путаница, от достаточно безобидных вопросов, как использование различных приставок или частиц (кибер-/электронный/цифровой/сетевой/виртуальный) до фундаментальных разногласий, когда использование разных терминов является отражением различий в подходах. Что касается вопросов кибербезопасности, то здесь вероятность возникновения недопонимания весьма высока. Рассмотрим, например, кибербезопасность в качестве одной из сфер государственной политики. В Китае, России и странах ШОС используется более общий термин «информационная безопасность», что включает также вопросы политической и социальной стабильности, и кибербезопасность понимается как элемент информационной безопасности. В то же время, в США, ЕС и стран ОЭСР кибербезопасность понимается как общий термин, связанный, в первую очередь, с защитой инфраструктуры Интернета. Для этих стран информационная безопасность, напротив, является частью кибербезопасности в том, что касается данных и информации.

Кроме того, в отрасли нет единого понимания таких терминов, как «критически важная инфраструктура», кибероружие и кибертерроризм, и эту путаницу с терминами необходимо преодолеть. Чтобы прийти к единому знаменателю по кибербезопасности, международному сообществу нужно провести переговоры, которые займут немало времени. К сожалению, недопонимание чревато значительными рисками, которые не следует недооценивать. В первую очередь необходимо выявить расхождения в терминологии и очертить их семантическое поле. После выявления расхождений следует определить точки соприкосновения, которые и лягут в основу разработки единого глоссария по вопросам кибербезопасности.

Междисциплинарный подход к вопросам кибербезопасности

Вопросы кибербезопасности невозможно решать в отрыве от других аспектов цифровой политики, включая права человека и экономическое развитие, как это показано на рис. 12[26].

Рисунок 12. Кибербезопасность в системе общественных отношений

Таким образом, системное реагирование на риски, связанные с кибербезопасностью, подразумевает глубокое понимание междисциплинарного характера киберпространства, которое охватывает такие сферы как технологии, право, психологию, социологию, экономику, политологию и дипломатию. Эффективность такой деятельности также зависит от сотрудничества различных заинтересованных сторон, которые могут способствовать снижению рисков:

- Правительственные и надзорные ведомства, задающие нормативно-правовые условия деятельности в области кибербезопасности.
- Органы судебной власти и правоохранительные органы, занимающиеся вопросами преступности и трансграничного сотрудничества.
- Частный сектор и техническое сообщество, обладающие экспертны-

ми знаниями в этой области и де факто контролирующие большинство объектов инфраструктуры, услуг и стандартов.

- Неправительственные организации и ученые с их знаниями, связями и возможностью взаимодействовать с конечными пользователями и доносить до них информацию о рисках злоупотребления киберпространством.

Техническая архитектура Интернета и кибербезопасность

На безопасность Интернета влияют особенности его структуры. Должны ли мы продолжать придерживаться текущего подхода, пытаясь «надстроить» безопасность поверх существующего небезопасного фундамента, или стоит что-то изменить в самих основах инфраструктуры Интернета? Как скажутся такие изменения на других чертах Интернета, в частности, на его открытости и прозрачности? Большинство прежних инициатив по разработке стандартов Интернета преследовало цель улучшения производительности или внедрения новых приложений. Безопасность не была приоритетом. Нельзя предсказать, сможет ли IETF изменить стандарты электронной почты, чтобы гарантировать удостоверение подлинности (аутентификацию) и в итоге сократить ненадлежащее использование Интернета (например, спам, киберпреступность).

Учитывая противоречия, связанные с любым изменением основных стандартов Интернета, вероятнее всего, усовершенствования базового интернет-протокола в области безопасности будут постепенными и медленными.

Однако в этой сфере уже предпринимаются важные инициативы. В качестве наглядного примера таких шагов можно привести создание набора расширений протокола DNS Domain Name System Security Extensions (DNSSEC)[27]. Исследования, испытания этой системы и обсуждение ее работы техническим сообществом длились 12 лет. Сначала система DNSSEC заработала в рамках ряда национальных доменов верхнего уровня, а с 2010 г. она была внедрена на уровне корневых серверов. Однако с переходом на этот стандарт безопасности регистраторов доменных имен, интернет-провайдеров и владельцев сайта связаны определенные трудности.

Существенно повысить уровень безопасности можно за счет правильной

настройки основных интернет-узлов, в том числе DNS-серверов, по всему миру. Многие инциденты, включая кибервойну 2013 г. между двумя частными компаниями CyberBunker и Spamhaus, в ходе которой в разных странах мира была превышена пропускная способность значительных сегментов Интернета, происходят из-за существования нескольких десятков неправильно настроенных DNS-серверов, отвечающих на рекурсивные запросы любому хосту[28]. Улучшить безопасность можно за счет создания новых технологий, будь то программное, аппаратное обеспечение или протоколы, с учетом требований безопасности, в том числе, с добавлением различных защитных функций и блокировщиков.

Кибербезопасность, доверие и интернет-торговля

Кибербезопасность часто упоминают в числе предварительных условий для быстрого развития электронной коммерции. Пока Интернет не станет защищенным и надежным, клиенты будут неохотно предоставлять через него конфиденциальную информацию (к примеру, номера кредитных карт). То же относится к банковским услугам в Интернете и использованию электронных денег. На наших глазах растет количество результативных атак против корпоративных серверов, что оборачивается утечкой персональных данных и номеров банковских карт. Например, 2014 г. группировка из России похитила полмиллиарда имен пользователей и паролей пользователей электронной почты[29]. Такие инциденты подрывают доверие к интернет-службам. Если общий уровень кибербезопасности будет повышаться медленно (например, по причине отсутствия стандартов), вероятно, бизнес-структуры будут способствовать ускоренному развитию кибербезопасности. В этих условиях могут возникнуть новые угрозы принципу сетевого нейтралитета, а также предпосылки к созданию «нового Интернета», который, среди прочего, поможет сделать коммуникацию в Интернете более безопасной.

Слежка и шпионаж

Разоблачения Эдварда Сноудена в 2013 г. лишь подтвердили факт использования уязвимостей Интернета государствами, включая США, в соб-

ственных интересах. Проект PRISM Агентства национальной безопасности США заключался в слежке за населением страны посредством доступа к кабельной сети, маршрутизаторам и облачным серверам крупнейших интернет-компаний (американских телекоммуникационных компаний, поставщиков услуг и контента). Другие страны, в частности, страны ЕС и БРИКС (Бразилия, Россия, Индия, Китай и Южная Африка), занялись разработкой мер, чтобы оградить себя от такой слежки. Они начали прокладывать собственные межконтинентальные подводные кабели[30] и требовать, чтобы дата-центры интернет-компаний, хранящие персональные данные их граждан, находились в пределах юрисдикции таких стран.

Экономический кибершпионаж

В 2013 г. американская компания Mandiant, специализирующаяся на вопросах кибербезопасности, подготовила доклад об исходящих из Китая кибератаках против компаний в США[31]. Когда в США были выдвинуты обвинения против пяти китайских «военных хакеров», Китай, в свою очередь, обвинил США в кибершпионаже, что привело к приостановке работы Американо-китайской рабочей группы по киберпространству[32]. Своей кульминации это противостояние достигло накануне визита Председателя КНР Си Цзиньпина в США в сентябре 2015 г., когда американские власти пригрозили введением санкций против Китая за экономический кибершпионаж. В ходе визита Китай и США достигли договоренности о том, чтобы преднамеренно не поддерживать кибершпионаж против частного сектора[33]. Отказ от экономического кибершпионажа был также поддержан в ходе саммита G2 (15–16 ноября 2015 г.) в Анталье. Страны G2 пришли к соглашению, что «ни одна страна не должна осуществлять или поддерживать хищение интеллектуальной собственности с использованием ИКТ, включая секретную торговую информацию или другую конфиденциальную деловую информацию с целью достижения преимуществ для компаний или коммерческих секторов»[34].

Киберпространство все чаще используется государствами в военных целях за счет применения вредоносного кода и других хакерских программных средств, что приводит к росту напряженности. Это делает еще более актуальными меры на международном уровне по предотвращению распространения кибероружия.

Кибербезопасность и права человека

Вопросы кибербезопасности неразрывно связаны с правозащитной проблематикой, что необычайно важно для будущего Интернета. Пока что какая-либо связь между этими двумя областями отсутствует. Однако, судя по недавним инициативам (Закон о прекращении интернет-пиратства — SOPA, Международное соглашение по борьбе с контрафактной продукцией — ACTA, проект PRISM Агентства национальной безопасности США), защита прав человека (право на неприкосновенность частной жизни, свобода выражения мнений и доступа к информации) важна не только с точки зрения ценностей, но и в качестве практического инструмента обеспечения открытости и безопасности Интернета.

Огромная роль в обеспечении кибербезопасности принадлежит обычным интернет-пользователям. В то же время, в контексте кибератак они нередко становятся самым слабым звеном. Для организации кибератак используются компьютеры обычных пользователей, которые формируют ботнеты и участвуют в распространении вирусов и вредоносных программ. Незащищенный доступ к нашим компьютерам и мобильным устройствам становится лазейкой для доступа к данным наших компаний или организаций, что делает уязвимыми многие другие компьютеры.

Однако конечных пользователей (в силу их неосведомленности) обычно беспокоит не столько то, что их незащищенные компьютеры представляют угрозу для всей сети, сколько защита их собственных данных, то есть неприкосновенность частной жизни. В дебатах, последовавших после разоблачения проекта PRISM, подчеркивалась необходимость защиты компьютеров от слежки, в частности, путем шифрования, протоколов IPSec, установки обновлений и настройки виртуальных частных сетей VPN[35]. Такие решения одновременно могли бы решить проблему несанкционированного доступа и способствовали бы повышению уровня кибербезопасности в целом.

Ключевую роль в обеспечении глобальной кибербезопасности играют обычные интернет-пользователи, и соблюдение прав человека в этом контексте имеет особое значение. В некоторых программных документах и регламентах уже можно проследить взаимосвязь между необходимостью

обеспечения кибербезопасности и соблюдением прав человека. Так, в Стратегии кибербезопасности ЕС в описании одного из пяти основополагающих элементов стратегии говорится о необходимости сохранения открытости, свободы и безопасности киберпространства, включая продвижение и защиту основных прав человека.

Необходимость обеспечения кибербезопасности и соблюдения права на неприкосновенность частной жизни нередко рассматриваются как два уравновешивающих друг друга начала, как показано на рис. 13. Однако это не всегда так.

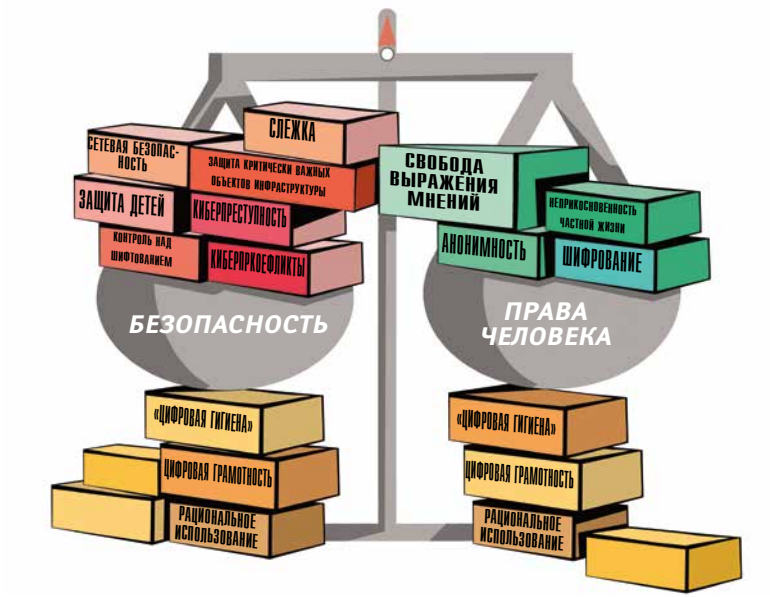


Рисунок 13. Как уравновесить необходимость обеспечения безопасности с обязанностью соблюдения прав человека?

Суть проблемы состоит в том, чтобы найти взаимовыгодное решение: повышение уровня безопасности должно сопровождаться улучшением положения в области прав человека и наоборот. Существует достаточно много областей, где возможен такой взаимовыгодный подход, при котором защита и расширение прав и возможностей физических лиц ведет к повышению

уровня кибербезопасности (доступ к информации, неприкосновенность частной жизни). Такие вопросы заслуживают приоритетного внимания. В конечном счете, следует признать, что соблюдение и продвижение прав человека является неотъемлемой частью практического осуществления политики кибербезопасности.

Киберпреступность

Противостояние между «реальным» и «виртуальным» правом существует и в этой плоскости. Сторонники «реального» права подчеркивают, что киберпреступления аналогичны преступлениям в «офлайновом» мире, только совершаются, как правило, посредством цифровых технологий. Преступления остаются теми же, отличаются только средства их совершения. В соответствии с «киберподходом», уникальные элементы киберпреступности требуют особого обращения, особенно когда речь идет о применении законов и профилактике преступности.

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

Тема киберпреступности оказалась настолько важной, что этим вопросом стали заниматься международные, региональные и местные организации, поскольку преступления в связи с электронными сетевыми системами или с их использованием происходили постоянно и становились все более разнообразными[36]. В качестве примера можно привести Инициативу Содружества по борьбе с киберпреступностью (Commonwealth Cybercrime Initiative)[37], которая была разработана в рамках Форума Содружества по управлению Интернетом (Commonwealth Internet Governance Forum — CIGF). Важность борьбы с киберпреступностью также была признана частным сектором, что привело к появлению негосударственных инициатив по повышению осведомленности в отношении этой проблемы и совершенствованию нормативно-правовой базы.

Вопросы

Определение киберпреступности

Киберпреступностью называются преступления, совершенные посредством Интернета и компьютерных систем. К отдельной категории киберпреступлений относятся нарушения, затрагивающие конфиденциальность, целостность и доступность данных и вычислительных систем. К таким преступлениям относятся несанкционированный доступ к вычислительным системам, незаконный перехват данных, неправомерные действия в отношении данных (порча, удаление, изменение или сокрытие данных) или системы (создание помех в работе компьютера или иного устройства), подделка, мошенничество и хищение персональных данных. К другому виду киберпреступлений относятся нарушения, связанные с контентом, что включает создание, предоставление, распространение, закупку и хранение интернет-контента, который считается незаконным в соответствии с нормами национального законодательства: материалы с элементами сексуального насилия в отношении несовершеннолетних, содержащие призывы к совершению действий, связанных с террористической деятельностью, материалы экстремистского характера (материалы, пропагандирующие ненависть, насилие и терроризм), интернет-травля (оскорбления, угрозы или домогательства с использованием технологий).

Киберпреступность и защита прав человека

Конвенция о киберпреступности обострила дискуссию о равновесии между безопасностью и правами человека. Некоторые представители гражданского общества опасаются, что конвенция предоставляет органам государственной власти слишком много полномочий, включая право проверять персональные компьютеры, следить за обменом информацией и т. д. Эти широкие полномочия могут поставить под угрозу некоторые права человека, в частности, право на неприкосновенность частной жизни и свободу выражения убеждений[38]. За исполнение Конвенции о киберпреступности отвечает

Совет Европы, одна из наиболее активных международных организаций, выступающих в защиту прав человека. Это обстоятельство может способствовать нахождению необходимого равновесия между борьбой с киберпреступностью и защитой прав человека. В этой связи следует отметить, что Комитет министров Совета Европы принял в 2014 г. Рекомендации Комитета министров государствам-членам Совета Европы к Руководству по правам человека для интернет-пользователей, в которых говорится, что «никто не должен подвергаться незаконному, произвольному или необоснованному вмешательству в свои права и основные свободы при использовании сети Интернет»[39].

Киберпреступность и защита прав человека

Одной из основных сложностей в борьбе с киберпреступностью является сбор данных для ведения судебных дел. Скорость современных коммуникаций требует быстрой реакции со стороны правоохранительных органов. Одним из возможных способов хранения улик является ведение провайдерами электронных протоколов («логов»), в которые заносится информация о том, кто и когда получал доступ к тем или иным интернет-ресурсам. Требование хранить данные об интернет-трафике установлено в Конвенции о киберпреступности.

Постоянно сталкиваясь с угрозами кибератак и терроризма, ЕС пошел дальше и принял Директиву о хранении данных, согласно которой интернет-провайдеры обязаны обеспечить хранение данных о трафике с привязкой к местонахождению пользователей «в целях проведения изысканий, для выявления серьезных преступлений и их расследования, в соответствии с нормами законодательства соответствующей страны»[40]. Это положение было подвергнуто жесткой критике за нарушение права на неприкосновенность частной жизни. Некоторые страны так и не приняли соответствующие законодательные меры для исполнения этой директивы, а в ряде случаев предписание и вовсе было признано неконституционным[41]. В декабре 2013 г. Суд Европейского союза объявил Директиву о хранении информации несовместимой с Хартией по правам человека[42].

Критическая инфраструктура

Согласно утвержденному Европейской комиссией определению, к критически важным объектам инфраструктуры относятся «объекты физической и информационной инфраструктуры, сети, услуги и активы», сбой в работе которых или уничтожение которых представляет угрозу для «здоровья, безопасности, сохранности и благосостояния граждан или эффективного функционирования государства»[43]. В качестве примеров таких объектов можно назвать системы энергоснабжения, транспорта, водоснабжения и связи, финансовые учреждения и услуги здравоохранения. При этом определение понятия критически важного объекта инфраструктуры зависит от ситуации в конкретной стране. В большинстве развитых стран утверждено определение этого понятия, чего нельзя сказать о многих развивающихся странах.

Цифровые технологии, например, системы оперативно-диспетчерского управления (SCADA), все чаще используются для управления критически важными объектами инфраструктуры с использованием IP-сетей (посредством замкнутых сетей или виртуальных частных сетей в Интернете). Такие решения позволяют оптимизировать использование ресурсов, при этом делая критически важные объекты инфраструктуры уязвимыми перед лицом кибератак. Это могут быть и DDoS-атаки (рис. 14), установление удаленного контроля над промышленными системами, сбор конфиденциальной информации, дестабилизация работы объектов в результате изменения параметров контроля и команд, как было в случае с вирусом Stuxnet или в ходе кибератаки против сталелитейного производства в Германии в конце 2014 г. [44]

Защита критически важных объектов (информационной) инфраструктуры

Среди критически важных объектов инфраструктуры необходимо отдельно выделить критически важные объекты информационной инфраструктуры. Согласно глоссарию IETF по вопросам безопасности, под критически важными объектами информационной инфраструктуры понимаются «системы, которые имеют такое большое значение для страны, что их выход

из строя или уничтожение будет иметь тяжелейшие последствия с точки зрения национальной безопасности, экономики, обеспечения здоровья и безопасности населения»[45].

Под защитой критически важных объектов информационной инфраструктуры понимаются правила, стратегии, планы и процедуры, связанные с предотвращением чрезвычайных ситуаций и аварий, подготовкой к ним, реагированием на них и преодолением их последствий. Как правило, для защиты критически важных объектов инфраструктуры используется ряд стратегий. Такие стратегии затрагивают широкий круг вопросов, включая правоприменение и профилактику преступности, борьбу с терроризмом, национальную безопасность и оборону, ликвидацию чрезвычайных ситуаций, обеспечение непрерывности деятельности, охрану, электронную безопасность, подготовку к природным катаклизмам, управление рисками, налаживание профессиональных связей, регулирование рынка, планирование и развитие инфраструктуры, а также обеспечение жизнестойкости в чрезвычайных ситуациях.

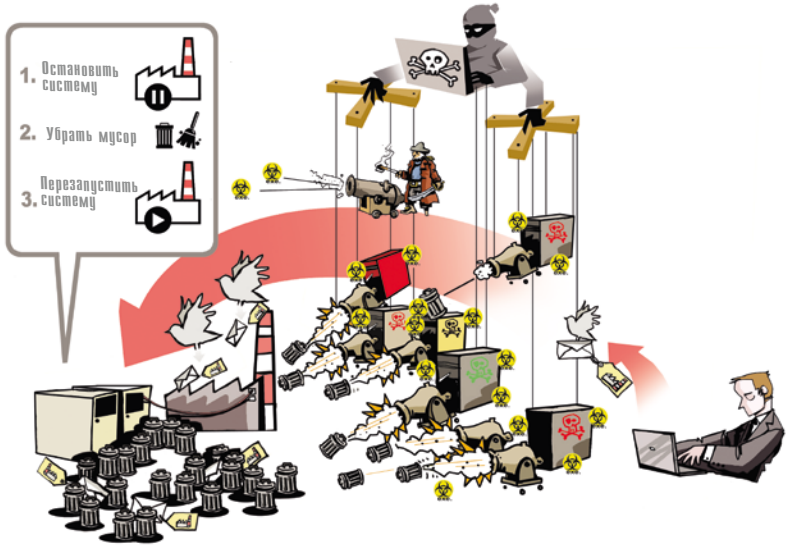


Рисунок 14. DDoS-атака против объекта критической инфраструктуры

В США в 2013 г. была принята Установочная директива Президента (PPD21) Безопасность и жизнестойкость объектов критически важной инфраструктуры[46], которая охватывает как физические, так и виртуальные системы. В ЕС действует Программа защиты критически важных объектов инфраструктуры (EPCIP)[47] и Директива по выявлению критически важных объектов инфраструктуры ЕС[48], в которых основное внимание уделяется отрасли ИКТ. Более подробные рекомендации для государств-членов ЕС по вопросам защиты ключевых объектов информационной инфраструктуры, в том числе по созданию Компьютерных групп реагирования на чрезвычайные ситуации (CERT), изложены в Директиве по сетевой и информационной безопасности и Киберстратегии ЕС. За реализацию мер по защите ключевых объектов информационной инфраструктуры, подготовку кадров в этой области и обеспечение ресурсов отвечает Европейское агентство по сетевой и информационной безопасности (ENISA).

В подготовленных ОЭСР Рекомендациях Совета по защите критически важных объектов инфраструктуры[49] описаны возможные шаги стран ОЭСР по защите ключевых объектов информационной инфраструктуры. На национальном уровне странам предлагается, в частности, разработать национальные стратегии; назначить государственные ведомства и организации, ответственные за защиту ключевых объектов информационной инфраструктуры; разработать систему предупреждения и реагирования, включая создание независимых компьютерных групп реагирования на чрезвычайные ситуации; вести консультации с частным сектором и содействовать ГЧП в этой области. Во внешнеполитической деятельности странам рекомендуется активизировать обмен информацией и укреплять сотрудничество между ведомствами, отвечающими за защиту ключевых объектов информационной инфраструктуры.

Кибертерроризм

Существует множество определений понятия «кибертерроризм». Очень часто этот вопрос решается путем экстраполяции определения понятия «терроризм» на мир виртуальных технологий. В некоторых странах, например, в Соединенном Королевстве, принято определение терроризма, но понятия «кибертерроризм» в правовом лексиконе не существует[50]. Согласно одному из определений, которое было предложено научным сообществом, под кибертерроризмом следует понимать «использование информационных технологий и средств террористическими группами и агентами»[51]. Есть более комплексное и широкое определение, согласно которому к кибертерроризму относятся «незаконные атаки и угрозы атак против компьютеров, сетей и хранящейся на них информации в целях запугивания или принуждения государства или его населения к совершению определенных политических или социальных действий»[52].

На практике, к кибертерроризму относятся также следующие действия:

- использование Интернета террористическими группировками для проведения атак (DoS-атаки, хакерские взломы);
- использование Интернета при подготовке и организации терактов;
- использование Интернета для продвижения террористических идей и набора террористов.

Противодействие распространению террористической пропаганды и идей насильственного экстремизма

Тема распространения террористической пропаганды и идей насильственного экстремизма в Интернете стала одной из основных тем современной международной политики. Большое внимание этой проблеме уделяют и интернет-компании.

По мере того как террористы продолжают совершенствовать методы работы в социальных сетях, аудитория которых постоянно расширяется, растущая угроза радикаликализации интернет-пользователей начинает привлекать внимание лиц, принимающих решения, во всех странах мира. В апреле 2016 министры иностранных дел Китая, Индии и России сделали совместное заявление, в котором подчеркивалась необходимость противодействовать распространению террористических материалов в Интернете[53]. Эта тема также обсуждалась на уровне Совета Безопасности ООН, в котором состоялись открытые слушания по вопросу о дискурсе и идеологии терроризма[54], а также на встрече лидеров стран G7[55] в мае 2016 г. в Японии.

Наряду с политиками, в дискуссиях принял участие и частный сектор, в частности, компании интернет-отрасли. В мае 2016 компания Microsoft обнародовала свои руководства по вопросу о террористических материалах в Интернете, заявив, что считает «необходимым … не содействовать, даже косвенно, совершению ужасных действий»[56]. Jigsaw, дочерняя компания Google, экспериментировала с поисковыми алгоритмами видео на YouTube, чтобы при поиске материалов террористической пропаганды система выдавала пользователю контент контртеррористической направленности[57].

При проведении кампаний по борьбе с экстремистской идеологией необходимо тщательно подходить к вопросу соблюдения прав на свободное выражение мнений. Существует тонкая грань между обеспечением безопасности и сетевой цензурой, которую легко пересечь. На это обратил внимание Специальный докладчик по вопросу о свободе выражения мнений Дэвид Кайе, который отметил, что власти могут использовать «насильственный экстремизм» в качестве «отличного предлога» для ограничения свободы выражения мнений[58]. Обеспечить максимальную свободу выражения мнений в ходе борьбы с радикализацией общества можно только посредством диалога между органами безопасности и правозащитными ведомствами и организациями.

Инициативы по борьбе с кибертерроризмом

Отсутствие согласованного определения понятия «кибертерроризм» может привести к неправильному толкованию этой проблемы и негативно сказаться на международном сотрудничестве по борьбе с этой угрозой. Несмотря на это, многие страны начинают более серьезно относиться к угрозе кибертерроризма. В 2012 г. Министерство обороны США объявило тендер на разработку программного обеспечения, которое бы позволило прогнозировать «акты кибертерроризма» путем анализа взаимодействия между преступными группировками и хакерами в Интернете[59]. Министерство безопасности и юстиции Нидерландов в период 2011–2013 гг. осуществило проект Clean IT Project, призванный «содействовать конструктивному диалогу между властями, деловыми кругами и гражданским обществом с целью снижения активности террористов в Интернете». По итогам реализации проекта были выработаны общие принципы и изучен передовой опыт в этой области[60].

Все больше внимания вопросам кибертерроризма уделяет ООН. Так, в сентябре 2006 г. Генеральная Ассамблея ООН приняла «Глобальную контртеррористическую стратегию Организации Объединенных Наций»[61], согласно которой государства-члены взяли на себя обязательство координировать усилия, предпринимаемые на международном и региональном уровнях, в целях борьбы с терроризмом во всех его формах и проявлениях в сети Интернет. В дальнейшем в рамках Целевой группы по осуществлению контртеррористических мероприятий (ЦГОКМ) была создана Рабочая группа по противодействию использованию Интернета в террористических целях, которая ставит своей задачей координацию действий по осуществлению стратегии в рамках ООН.

В 2012 г. Рабочей группой в сотрудничестве с УНП ООН был подготовлен доклад, в которой вошел обзор существовавших на тот момент нормативно-правовых режимов и подходов на национальном и международном уровнях в отношении уголовного преследования и расследования террористических действий в Интернете, а также рекомендации по активизации межгосударственного сотрудничества в этой области[62]. Контртеррористический комитет Совета Безопасности ООН также рассматривал проблему использования Интернета в террористических целях. В декабре 2015 г. комитет провел слушания с участием государств-членов, представителей интернет-компаний и правозащитных организаций по методам предотвращения использования Интернета и социальных сетей для набора террористов и подстрекательства к совершению террористических актов в контексте осуществления прав человека и основных свобод. По итогам мероприятия были приняты рекомендации государствам и частному сектору по недопущению использования киберпространства в террористических целях и мерам борьбы с злоупотреблением кибепространством в соответствии с нормами международного права в области защиты прав человека[63].

Киберконфликты и кибервойны

Действующие на настоящий момент нормы международного права регулируют порядок ведения традиционных вооруженных конфликтов и призва-

ны способствовать ограничению их негативных последствий. Эти же нормы, по мнению большинства экспертов, должны применяться к конфликтам в сети, однако как практически осуществляется такое регулирование, пока неясно.

Еще одной проблемой является отсутствие единого понимания, что считать актом войны в киберпространстве. Согласно одному из возможных определений, под кибервойной понимаются «действия государства по проникновению в компьютеры другой страны в целях нанесения ущерба или провоцирования сбоя»[64]. Однако согласия в отношении данного определения нет, в частности, между основными игроками на международной арене.

Особенность кибератаки состоит в том, что ее автора практически невозможно определить, не говоря уж о стоящем за такой атакой государстве. Дело в том, что в таких случаях используются очень сложные и технически совершенные средства, скрывающиеся за цепочкой прокси-серверов (включая ботнеты). Кроме того, в силу глобального характера Интернета, в отличие от обычных военных действий, киберконфликты не могут происходить между какими-нибудь двумя странами, не затрагивая других. Такие виды кибероружия, как ботнеты, задействуют вычислительные мощности других стран без их разрешения, что придает кибервойнам глобальный характер.

Киберконфликты и кибервойны стали частью международной политической повестки, после того как в апреле 2007 г. массивным кибератакам подверглась Эстония. DDoS-атаки были направлены против объектов инфраструктуры Интернета, министерств иностранных дел и обороны, ведущих газет и банков[65]. Хотя косвенные улики свидетельствует о наличии связи между атаками и протестами России против перемещения памятника советским воинам в Таллине, никаких явных доказательств причастности российских официальных лиц к этим атакам нет. Чаще в качестве примера кибервойны приводят атаки против грузинских СМИ и государственных ведомств в ходе конфликта между Россией и Грузией в 2008 г. Этот случай называют «кибервойной»[66], хотя причастность российского государства к этим атакам доказана не была.

СМИ также сообщали о причастности властей США и Израиля к кибератакам против компьютерных систем на иранских установках по обогащению урана, что свидетельствует о систематическом использовании кибероружия[67]. Иран, в свою очередь, обвиняли в осуществлении кибератак против

американских банков и компаний в ответ на атаки со стороны США[68]. Следующим шагом было обвинение правительством США Северной Кореи во взломе компьютерной системы компании Sony в конце 2014 г и введение экономических санкций[69].

История знает и более изощренные подходы к кибервойнам. США обвиняют Китай в систематическом кибершпионаже, мишенью которого выступают государственные ведомства и частные компании (например, Google и Microsoft), однако Китай такие обвинения отвергает[70]. Когда в 2014 г. компания Mandiant, специализирующаяся на вопросах безопасности, опубликовала доклад о причастности Китая к кибершпионажу, Китай в ответ заявил, что сам является жертвой, сославшись на проект PRISM, о существовании которого всему миру рассказал Эдвард Сноуден. Китай также отметил, что такие инциденты могут негативно сказаться на китайско-американском сотрудничестве[71].

Кибератаки и гибридные войны

В итоговых документах Мюнхенской конференции по безопасности 2015 г. важной составляющей гибридных войн названы кибератаки[72], под которыми понимаются проведенные в мирное время кибероперации с целью дестабилизации оппонента без развязывания реальной войны.

Использование ботнетов и схожих инструментов для проведения кибератак преследует те же цели, что и традиционные войны, а именно завладение экономическими ресурсами другой территории или уничтожение ресурсов противника. Кибероружие может использоваться против систем контроля критически важных объектов инфраструктуры, например, систем электроснабжения, авиадиспетчерских служб и систем безопасности атомных электростанций (рис. 15).

От других средств ведения войны кибератаки отличаются своей дешевизной. Так, по мнению исследователей, для проведения мощной DDoS-атаки в масштабах целой страны необходимо несколько тысяч евро, тогда как причиненный экономический ущерб может варьироваться от 10 млн. евро в день для такой страны в стадии переходного периода как Сербия, до 500 млн. евро в день для такой развитой страны, как Швейцария[73]. Таким обра-

зом, кибероружие дает дополнительные возможности игрокам с ограниченными ресурсами.

В основном, кибероружие используется в дополнение к традиционным методам конфронтации, а не в качестве автономного средства ведения войны.

Рисунок 15. Кибероружие

Шифрование

Шифрование (криптографическая защита) заключается в преобразовании электронных документов и сообщений в нечитаемую форму, распознать которою можно только посредством декодирования. Раньше достаточными ресурсами и потенциалом для разработки и внедрения мощных систем шифрования обладали только официальные власти, которые использовали такие технологии в военной сфере и дипломатии. Однако с появлением приложений типа Pretty Good Privacy услуги шифрования стали доступными обычным интернет-пользователям. В последнее время появился целый

ряд ресурсов по шифрованию сообщений, включая Silent Circle, Telegraph и Proton. Кроме того, интернет-компании стали использовать сложные криптографические алгоритмы для защиты своей внутренней информации и пользовательских данных.

Растущая доступность криптографических услуг для всех интернет-пользователей, включая преступников и террористов, и возможность злоупотребления такими технологиями положили начало серьезной дискуссии между властями и компаниями по вопросу о регулировании этого сегмента. Предметом спора стало соотношение между принципом неприкосновенности частной жизни интернет-пользователей и правом властей отслеживать определенные сообщения из соображений национальной безопасности (ввиду возможного использования таких технологий в преступной и террористической деятельности).

Основные сферы применения

Как правило, шифрование воспринимается как средство обеспечения конфиденциальности сообщений. Пользователям рекомендуется снабжать криптографической защитой материалы, которые они хранят на своих компьютерах или в облаке, или требовать, чтобы это сделали поставщики услуг облачного хранения. Шифрование также необходимо при передаче контента (например, в социальных сетях или при отправке письма по электронной почте). Поскольку процесс шифрования требует времени и определенных вычислительных мощностей, у многих поставщиков услуг облачного хранения или средств связи эта функция по умолчанию отключена, иначе им бы пришлось в режиме реального времени шифровать огромные объемы данных. При этом, реагируя на растущий спрос со стороны потребителей, все больше компаний предлагают услуги по криптографической защите за отдельную плату, что повышает их конкурентоспособность. В качестве примера можно привести решения компании Apple и мессенджера WhatsApp. Также пользователям доступен ряд программных продуктов, в том числе бесплатных, обеспечивающих анонимность навигации за счет шифрования трафика. Такой подход лег в основу сети Tor (программное обеспечение с открытым исходным кодом, разработанное для защиты конфиденциальности и основных свобод путем обеспечения анонимности пользователей и препятствования

анализу трафика и его отслеживанию).

Криптографическая защита стала ключевой составляющей мер по повышению безопасности основных интернет-протоколов. Так, протоколы IPSec, DNSSEC и Border Gateway Protocol Security (BGPSec) основаны на распространении цифровых сертификатов для серверов и маршрутизаторов с целью проверки IP-адресов, доменных имен и предотвращения случаев мошенничества и подмены со стороны мошеннических серверов. Аналогичным образом, криптографический протокол SSL (Secure Sockets Layer) обеспечивает зашифрованную связь между интернет-сервером и браузером, что гарантирует конфиденциальность связи и целостность данных при передаче между двумя ресурсами.

Шифрование и стандартизация

С ростом вычислительных мощностей шифрование и расшифровка криптограмм занимает все меньше времени и требует регулярной смены стандартов. Лучшие алгоритмы, которые де факто задают стандарт для коммерческих продуктов, выбирают инженеры и исследователи из таких организаций, как IETF, частных некоммерческих организаций по стандартизации, например, Американского национального института стандартов, и национальных органов по стандартизации экономически развитых стран (у которых есть ресурсы для развития криптографических технологий), включая Национальный институт стандартов и технологии США. Актуальность вопросов слежки в Интернете и массового использования решений по шифрованию данных повысили интерес к вопросам стандартизации со стороны органов безопасности. После разоблачений Сноудена журнал Der Spiegel сообщал, что «агенты АНБ посещают заседания IETF, организации, занимающейся разработкой стандартов, с целью сбора информации и, предположительно, с целью направления дискуссии в нужное русло»[74].

Международные режимы, касающиеся инструментов шифрования

Международные аспекты криптографической политики требует координации действий на уровне органов безопасности и компаний.

Так, США не смогли установить контроль над экспортом криптографического программного обеспечения, поскольку не имели возможности контролировать его оборот на международном рынке. Американские компании – разработчики программного обеспечения провели мощную лоббистскую кампанию, чтобы доказать, что экспортный контроль не способствует повышению национальной безопасности, а только подрывает конкурентоспособность США на внешних рынках.

Вопросы криптографической защиты информации до сих пор рассматривались в двух контекстах: Вассенаарского соглашения и ОЭСР (Организация экономического сотрудничества и развития). Вассенаарское соглашение — это международный режим, установленный 41 страной с целью ограничения экспорта обычных вооружений и технологий «двойного назначения» в воюющие страны и «страны-изгои»[75]. Соглашение предусматривает создание секретариата в Вене. Целью лоббистских усилий США в рамках Вассенаарского соглашения было распространение на международном уровне подхода по принципу технологии «Клиппер чип» (Clipper Approach)[76], позволяющей контролировать шифровальное ПО с помощью системы депонирования ключей. Этому воспротивились многие страны, в особенности Япония и скандинавские страны.

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

ОЭСР — еще одна площадка международного сотрудничества в области шифрования данных. Хотя документы ОЭСР не имеют обязательной юридической силы, ее указания по различным вопросам считаются весьма ав-

торитетными. Они появляются в результате работы экспертов и принятия решений на основе консенсуса. Большинство таких указаний в итоге включается в национальные законы. Деятельность ОЭСР в области криптографической защиты порождает очень много споров. Начало ей было положено в 1996 г. предложением США принять систему депонирования ключей в качестве международного стандарта. Как и в случае с Вассенаарским соглашением, переговоры по предложению США вызвали сильное противодействие со стороны Японии и скандинавских стран. В результате появилась компромиссная версия основных составляющих политики в области криптозащиты.

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.

Проблемы безопасности и права человека

Шифрование обеспечивает защиту данных пользователей. Его также используют для сокрытия своих контактов преступники, которые успешно осваивают интернет-технологии и применяют их, например, для приобретения оружия, как это было в случае с терактами 2015 г. в Париже[77]. Использование общедоступных анонимных прокси-серверов и анонимных сетевых соединений с помощью программ типа Tor для доступа к «темному интернету», а также расплата криптовалютами, например, биткойном, практически не оставляют следов, что значительно затрудняет контроль над использованием цифровых технологий и проведение расследований в этой области. Кроме того, на рынке появляется все больше мобильных устройств, обеспечивающих высокий уровень безопасности за счет использования новейших решений в области шифрования, например iPhone и Silent Circle. Наряду с этим растет число разнообразных мобильных приложений по обмену сообщениями с элементами криптозащиты, такие как Telegram и Signal. Такие программы позволяют защищать сознательных граждан, сообщающих о нарушениях, и активистов-оппозиционеров по всему миру, но, одновременно, используются как безопасный канал связи террористами, поскольку сообщения, отправленные по таким сетям, невозможно перехватить.

В ответ власти и органы безопасности многих стран, включая Соединенное Королевство, Францию и США, пытаются ограничить применение алгоритмов шифрования в товарах и услугах, доступных широкому кругу лиц, и создать механизмы, которые бы позволили государственным ведомствам при необходимости получать доступ к зашифрованным данным. В некоторых странах, включая США, Соединенное Королевство и Россию, предпринимаются попытки на законодательном уровне обязать технологические компании предоставить правоохранительным органам доступ к зашифрованным данным и/или устройствам (при определенных обстоятельствах) или оказывать содействие в получении такого доступа. Власти утверждают, что доступ к зашифрованным данным чрезвычайно важен для предотвращения преступлений, преследования виновных и обеспечения общественного порядка.

Представители гражданского общества и правозащитники серьезно обеспокоены этой ситуацией, особенно в свете разоблачений Сноудена. По их мнению, такие меры могут использоваться для введения политической цензуры и осуществления избыточной (массовой) слежки, для идентификации политических активистов, блогеров и журналистов в авторитарных государствах, что будет угрозой для их безопасности. В ряде исследований также утверждается, что шифрование не обеспечивает преступникам такой уровень защиты, как уверяют правоохранительные органы[78], и что предоставление ключей для обхода криптозащиты не достигнет своей цели[79].

С точки зрения защиты прав человека, необходимо обеспечить соблюдение права на неприкосновенность частной жизни. Технологии шифрования, включая сквозное шифрование, приобретают в этом контексте особое значение. Так, важная роль шифрования и обеспечения анонимности в сети подчеркивается в докладе Специального докладчика Совета по правам человека ООН по вопросам осуществления прав на свободу мнений и самовыражения в цифровую эпоху[80].

На международном уровне активно обсуждается вопрос соотношения требований безопасности и соблюдения прав человека применительно к шифрованию, в частности, после получившего широкую огласку спо-

ра между компанией Apple и ФБР в начале 2016 г. Дело заключалось в том, что суд попросил Apple помочь ФБР разблокировать iPhone. Мнения сторон разделились. С одной стороны, компания Apple при поддержке других интернет-компаний и правозащитников заявляла, что выполнение запроса суда создает опасный прецедент вмешательства в частную жизнь пользователей. С другой стороны, власти подчеркивали, что не требуют создания системы обхода криптозащиты или расшифровки, а просят помочь «только в одном случае», ои обвиняли Apple в том, что она ставит свои коммерческие интересы выше расследования теракта. Хотя дело, в конечном счете, было закрыто (как заявили в Министерстве юстиции, iPhone был разблокирован сторонним специалистом), проблемы, которые возникли в этой связи, так и не были решены. С одной стороны, остается неясным, при каких обстоятельствах власти вправе требовать, чтобы технологические компании взламывали встроенные в их устройства системы безопасности? Какие меры предосторожности могут или должны быть приняты в этой связи? Могут ли власти выдвигать какие-то требования относительно продуктов, над которыми работает компания? С другой стороны, в какой степени компании должны соблюдать принцип неприкосновенности частной жизни своих пользователей? Следует ли отстаивать этот принцип любой ценой?[81]

В отношениях между интернет-отраслью, которая пытается восстановить доверие, утраченное в результате разоблачений Сноудена, путем внедрения шифрования по умолчанию, и органами разведки и безопасности, которые хотят иметь возможность отслеживать электронные сообщения, а то и ограничить использование решений в области криптозащиты, напряжение постоянно возрастает. Следует ли предоставить властям право использовать существующие уязвимости в коммерческих системах? При каких обстоятельствах? Обязаны ли они информировать широкую общественность или поставщика о выявленных изъянах, чтобы устранить проблему в информационных системах?

Хотя эти вопросы остаются открытыми, многие компании, занятые в сфере Интернета и технологий, продолжают использовать шифровальное ПО в своих товарах и услугах и стремятся исключить возможность взлома криптографической защиты даже для создателя продукта или услуги (что

делает неактуальным требование властей оказать содействие в обходе систем защиты и предоставлении доступа к зашифрованным данным).

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, распространения порнографических материалов и все чаще с целью заражения компьютеров получателей вредоносным программным обеспечением. 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 таких сообщений, а также в связи с распространением вредоносного ПО в спам-рассылках (что нередко оборачивается кражей банковских реквизитов или другой важной финансовой информации)[82].

Рисунок 16. Спам

Если 10 лет назад спам был одной из основных проблем в области регулирования Интернета, сейчас эта тема привлекает к себе меньше внимания, что объясняется использованием продвинутых спам-фильтров. Согласно статистике за 2015 г., на спам приходилось 54% входящих сообщений, тогда как в 2010 г. доля спама достигала 84,9%[83]. Тем не менее исследователи обращают внимание на тот факт, что одновременно со снижением доли спама в общем потоке электронных сообщений на протяжении последних лет количество электронных писем с вредоносным содержанием значительно выросло (рис.16). Так, по наблюдению Лаборатории Касперского, в первом квартале 2016 г. объем вредоносной спам-рассылки увеличился в 3,3 раза по сравнению с аналогичным периодом 2015 г[84]. В качестве еще одного примера можно назвать выявленный в феврале 2016 г. вирус-вымогатель Locky, который распространился по всему миру за счет спам-рассылки. По данным за апрель 2016 г., попытки заразить этим трояном компьютеры были зафиксированы в 110 странах[85].

Со спамом можно бороться как техническими, так и юридическими средствами. С технической точки зрения, существует много программ, фильтрующих сообщения и удаляющих спам. В распоряжении технического сообщества имеется ряд передовых решений в этой области, включая программы, созданные группой M3AAWG (Messaging, Malware, and Mobile Anti-Abuse Working Group), в рамках проекта Spamhaus Project, а также ассоциациями GSMA и Internet Society.

Правовые аспекты

Однако технические методы имеют лишь ограниченное влияние, и их использование необходимо сопровождать конкретными правовыми мерами. Что же касается правовых аспектов вопроса, отметим, что во многих странах было принято законодательство по борьбе со спамом. В США попытка найти тонкую грань между законным использованием электронной почты для рекламы и спамом предпринята в так называемом Can-Spam Act[86]. Хотя закон предусматривает суровое наказание за распространение спама, вплоть до тюремного заключения на срок до пяти лет[87], некоторые его положения, как утверждают критики закона, вполне терпимы к спаму или даже могут способствовать его распространению. Изначальная позиция, обозначенная в законе, предполагает, что спам разрешается, пока получатель таких сообщений не скажет «стоп» (используя право отказа от рассылок).

В июле 2003 г. в Европейском союзе был принят собственный закон по борьбе со спамом, ставший частью «Директивы по конфиденциальности и электронным коммуникациям»[88]. Согласно праву ЕС, заниматься адресным маркетингом посредством рассылки писем по электронной почте можно только при условии получения предварительного согласия пользователей (явное согласие). Однако из этого правила можно сделать исключение, если между сторонами уже были коммерческие отношения. В таком случае заниматься адресным маркетингом посредством рассылки писем по электронной почте можно, если пользователи имеют возможность отказаться от таких писем при сборе данных или позднее (явный отказ). В директиве также подчеркивается важность саморегулирования и инициатив частного сектора по борьбе со спамом.

Законы о противодействии спаму, принятые как в США, так и в ЕС, имеют одно слабое место: отсутствие мер по предотвращению трансграничного спама. К сходному выводу пришли и авторы исследования законов стран ЕС о противодействии спаму, проведенного Институтом информационного права Университета Амстердама: «Уже тот факт, что источник большинства спам-сообщений находится вне ЕС, существенно ограничивает эффективность Директивы Европейского Союза»[89]. Требуется глобальное решение на основе международного договора или сходного механизма.

Меморандум о взаимопонимании, подписанный в 2013 г. Австралией, Кореей и Великобританией, является одним из первых примеров международного сотрудничества в кампании против спама. В нем говорится о важности сотрудничества по борьбе со спамом, попадающим из одной страны в другую. В июне 2016 г. власти Канады, США, Австралии, Голландии, Кореи, Новой Зеландии и Южной Африки подписали еще один меморандум о взаимопонимании по борьбе со спамом[90].

В ОЭСР создана Рабочая группа по спаму и подготовлен «набор инструментов» по борьбе со спамом. МСЭ также принимает меры в этой области. Так, в РМЭ содержатся положения о предотвращении рассылки «нежелательных массовых электронных сообщений», которые, по мнению ряда экспертов, также включают спам. Однако эти положения не носят обязательно-

го характера. Она просто рекомендуют странам «стремиться предпринимать необходимые шаги» и расширять сотрудничество.

Подробнее о РМЭ см. ***Раздел 4.***

Аналогичным образом, резолюция 2012 г. Всемирной ассамблеи МСЭ по стандартизации электросвязи (World Telecommunication Standardization Assembly – WTSA) призывает страны принимать необходимые меры по борьбе со спамом, причем исключительно на национальном уровне[91]. Что касается практической деятельности, то в рамках своего Сектора стандартизации электросвязи (МСЭ-Т) МСЭ ведет работу по изучению методов борьбы со спамом. Например, в рамках Исследовательской группы по вопросам безопасности МСЭ-Т анализируются возможные меры борьбы со спамом и разработка технических рекомендаций в отношении новых видов спама. В частности, группа занимается изучением сетевого спама в его нынешнем и будущем виде, последствий использования спама, технологий, которые позволяют создавать и распространять спам, и поиском решений по борьбе со спамом. Среди инициатив регионального уровня необходимо отметить подготовленные АТЭС Принципы борьбы со спамом[92], а Африканский союз включил положения о «рекламе электронными средствами» (включая электронную почту) в свою Конвенцию о безопасности киберпространства и защите персональных данных[93].

Среди инициатив по борьбе со спамом также необходимо отметить Лондонский план действий, который служит основой для международного сотрудничества в области внедрения мер по борьбе со спамом на законодательном уровне и решению схожих проблем, включая электронное мошенничество, фишинг, распространение вредоносных программ и вирусов. С 2004 г. в рамках этой инициативы проводятся встречи сотрудников надзорных органов более чем 25 стран, а также представителей технического и делового сообщества.

Вопросы

Системы фильтрации

Со спамом связаны многие проблемы. С технической точки зрения, одна из основных трудностей использования систем фильтрации состоит

в том, что вместе со спамом они могут удалять письма, которые спамом не являются. Например, иск против компании Verizon был связан с тем, что созданный ею спам-фильтр одновременно блокировал и нормальные сообщения, создавая неудобства для пользователей. Между тем компании, занимающиеся борьбой со спамом, продолжают расти и находят новые решения, позволяющие с все большей точностью отличить спам от обычной почты.

Различные определения спама

Разное понимание того, что представляет собой спам, влияет на эффективность борьбы с ним. В США кампанию по борьбе со спамом «тормозит» озабоченность защитой свободы слова и Первая поправка к Конституции. Американские законодатели считают спамом только «не запрашиваемые получателем коммерческие сообщения», 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[94], такое разночтение в определениях существенно ограничивает любую возможность создания эффективного международного механизма по борьбе со спамом.

Спам и удостоверение подлинности электронных сообщений

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

Необходимость действий на глобальном уровне

Большая часть спама приходит из-за рубежа. Это глобальная проблема, требующая глобального решения. Существуют различные инициативы, которые могу привести к повышению эффективности глобального сотрудничества. Некоторые из них — такие как двусторонние меморандумы о взаимопонимании — уже упоминались. Другие включают в себя, например, проекты по наращиванию потенциала и обмену информацией. Для выработки более комплексного решения потребуется разработать международный документ по борьбе со спамом. До сих пор развитые страны предпочитали укреплять национальное законодательство, параллельно проводя двусторонние или региональные кампании по борьбе со спамом. С учетом своего невыгодного положения как получателей «глобального общественного зла», исходящего преимущественно от развитых стран, большинство развивающихся стран заинтересовано в выработке глобального ответа на проблему спама.

Электронные цифровые подписи

Говоря в общем, электронные цифровые подписи[95] — это инструмент, позволяющий идентифицировать человека в Интернете. Потому они связаны со многими аспектами Интернета, включая юрисдикцию, киберпреступность и электронную коммерцию. Использование цифровых подписей должно способствовать формированию отношений доверия в Интернете. Цифровая идентификация является важным компонентом электронной коммерции. Она должна облегчать заключение электронных сделок за счет использования электронных контрактов. Например, не прост вопрос о действительности соглашения, заключенного посредством электронной почты или на веб-сайте. Ведь во многих странах закон требует, чтобы любой договор был «в письменном виде» или «подписан». Что это означает применительно к Интернету? Как удостовериться в целостности документа, снабженного электронной подписью? Столкнувшись с подобными проблемами и необходимостью создать благоприятную для электронной коммерции правовую среду, власти многих стран начали принимать законы об электронной цифровой подписи (ЭЦП).

Что касается ЭЦП, то основная сложность состоит в том, что правительства не пытаются решить существующую проблему (например, противодействовать киберпреступности или защищать авторское право), а создают новую сферу руглирования, не имея в этой области практического опыта. Это привело к появлению разнообразных решений и к общей неоднозначности документов, касающихся электронной цифровой подписи. В области регулирования цифровых подписей сложились три главных подхода[96].

Первый подход — «минималистский», согласно которому электронным подписям нельзя отказать в существовании на том лишь 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 сочетает в себе вышеупомянутые подходы. Минимализм в нем проявляется в части, касающейся признания подписей, существующих в электронном виде. Элементы максималистского подхода находят отражение в том, что «усовершенствованные» цифровые подписи имеют больший вес с точки зрения права (например, их правомерность легче доказать в суде). Именно такой подход был взят на вооружение в ЕС в 1999 г. с принятием Директивы ЕС о цифровых подписях и заменившего ее Постановления об оказании электронных услуг по идентификации и доверительных услугах в отношении электронных операций на внутреннем рынке (Постановление eIDAS)[97]. В постановлении ЕС дается новое прочтение концепции «усовершенствованных» электронных подписей, вводится понятие доверительных электронных услуг и гарантируется переход ЕС на единый правовой режим по этом вопросу.

На глобальном уровне Комиссия ООН по праву международной торговли

(United Nations Commission on International Trade Law — UNCITRAL) приняла в 2001 г. «Типовой закон об электронной цифровой подписи»[98], который придает таким подписям равный статус с обыкновенными при условии соблюдения определенных технических требований.

В непосредственной связи с электронной цифровой подписью находятся инициативы, связанные с инфраструктурой «открытого ключа» (Public key infrastructure — PKI). Созданием стандартов для этого сегмента занимаются две организации — МСЭ и IETF.

Вопросы

Идентификация пользователей

Электронные цифровые подписи являются частью более широкой проблемы поиска баланса между обеспечением конфиденциальности и необходимостью удостоверения личности в Интернет. ЭЦП — всего лишь одна из важных технологий (но не единственная), позволяющих удостоверить личность пользователя в Интернетее[99]. Например, в некоторых странах, где законодательство или стандарты и процедуры, касающиеся ЭЦП, еще не разработаны, для одобрения онлайн-транзакций банки используют подтверждение личности с помощью мобильных телефонов (по SMS).

Необходимость создания подробных стандартов правоприменения

Хотя многие развитые страны приняли законодательные акты по ЭЦП, в этих документах зачастую отсутствует подробное описание стандартов и процедур применения этих законов в Интернете. Принимая во внимание новизну проблемы, многие страны заняли выжидательную позицию, пытаясь понять, в каком направлении будут развиваться стандарты в Интернете. Инициативы по стандартизации проявляются на разных уровнях, включая международные организации (МСЭ и ISO), организации регионального уровня (Европейский комитет по стандартизации – CEN, ETSI и т. д.), национальные организации (Национальный институт стандартов и технологии США) и профессиональные ассоциации (IETF).

Технологический нейтралитет

Во многих странах идет активное внедрение новых видов электронных подписей, в том числе с использованием биометрических данных. Как и во многих других областях, где все очень быстро меняется, в сфере технологий и инноваций законодателям необходимо найти баланс между кодификацией таких механизмов и принципом технологического нейтралитета, чтобы принятые акты не утеряли своей актуальности.

Опасность несовместимости

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

Безопасность детей в Интернете

Дети и молодежь[100] все больше и чаще пользуются Интернетом, который дает им множество преимуществ, открывая новые возможности в сфере образования, личностного развития, самовыражения и взаимодействия с другими. В то же время, с Интернетом связаны риски, перед лицом которых дети и молодежь особо уязвимы.

Необходимо найти правильный баланс между выгодами, которые несут детям новые технологии, и обеспечением безопасной и защищенной среды в Интернете. С одной стороны, нужно защитить детей от неприемлемого контента и рискованных действий, а с другой – обеспечить осуществление их прав на доступ к информации, свободу слова и другие права.

Подробнее о цифровых правах детей см. Раздел 8.

Вопросы

Понимание того, как дети используют технологии и Интернет, чрезвычайно важно с точки зрения разработки политических инициатив и мер по обеспечению безопасности детей в Интернете. При этом постоянно появляются новые технологии, которые оказывают существенное воздействие на жизнь детей и их безопасность. Хотя единого, пригодного для всех стран мира подхода к вопросам защиты детей в Интернете не существует, очевидно, что все заинтересованные стороны должны действовать с учетом настроений и практики использования технологий, распространенных среди молодежи.

Риски, с которыми дети сталкиваются в Интернете

Хотя Интернет и дает массу преимуществ, все же при использовании сети и различных технологий дети и молодежь сталкиваются с определенными рисками. Хотя опасность может грозить любому пользователю вне зависимости от возраста, дети, будучи не полностью сформировавшимися личностями, оказываются наиболее уязвимыми. Существует ряд классификаций[101] таких рисков, которые можно резюмировать следующим образом:

Неподобающий контент. Дети могут столкнуться с материалами, которые не соответствуют их возрасту, включая материалы непристойного содержания или элементы насилия. Например, игры, основанные на насилии, быстро занимают место «пассивных» жестоких фильмов. В них часто фигурируют новейшие виды вооружений, напоминающие настоящее оружие, и сцены кровопролития.

Неподобающие контакты. Дети могут столкнуться с неподобающими видами поведения, включая запугивание и домогательства, и опасность таких контактов особо возрастает при использовании социальных сетей. Обычно дети становятся жертвами своих сверстников, однако в рамках неподобающих контактов они могут столкнуться и с более опасными случаями, например, с риском сексуального насилия,

Неподобающее поведение. Дети и молодежь нередко не в состоянии понять последствия, которые связаны с сохранением их «цифрового следа» в Интернете. Под неподобающим поведением понимается публикация непристойных комментариев и изображений или раскрытие деликатной информации, что чревато негативными последствиями. Обмен сообщениями сексуального содержания (sexting), преимущественно с использованием мобильных устройств, становится все более распространенным явлением. Согласно исследованиям, давление, побуждающее молодых людей заниматься такой деятельностью, возрастает.

Проблемы потребления. К проблемам потребительского или коммерческого характера относятся получение нежелательной рекламы, скрытые расходы (когда пользователям предлагают заплатить за услугу в приложении) и получение спама. Дети также сталкиваются с риском нарушения права на неприкосновенность частной жизни и незаконным сбором данных, включая данные геолокации.

Несмотря на широкий спектр рисков, исследования, проведенные в Европе[102], показывают, что не все риски, с которыми все чаще сталкиваются дети, приносят реальный вред. Конкретный исход всегда зависит от возраста, пола, способности ребенка противостоять обстоятельствам и ресурсов, позволяющих справиться с риском. Родители, опекуны, учителя, власти, деловое сообщество и другие заинтересованные стороны играют важную роль в обеспечении защиты детей и должны помогать им справляться с сетевыми рисками.

Сексуальная эксплуатация и насилие в отношении детей в Интернете

Проблема сексуального насилия в отношении детей не нова, однако с появлением Интернета ее масштабы существенно возросли. Нередко преступникам удается действовать анонимно и уходить от ответственности. Описанные в данном разделе риски могут приводить к различным формам сексуального насилия: дети могут оказаться подвергнуты влиянию преступников, обольщению и сексуальной эксплуатации; они могут сами совершать нарушения, если их убедят создать и распространять собственные изображения сексуального характера, которые впоследствии могут быть использованы для давления на них.

Общаясь в социальных сетях, которыми также пользуются и преступни-

ки, дети и молодежь зачастую не представляют, насколько опасны люди, действующие под прикрытием. Одним из наиболее распространенных подходов среди нарушителей в Интернете стало сокрытие своей истинной идентичности, что создает дополнительные риски в случае перехода от виртуального общения к реальному контакту и может привести к эксплуатации и насилию в отношении детей, педофилии, вовлечению несовершеннолетних в сексуальные отношения вплоть до торговли детьми.

Изображение сексуального насилия над детьми на юридическом языке называется «детской порнографией[103]. Как правило, речь идет об актах реального насилия. Согласно проведенным исследованиям, жертвами виртуального сексуального насилия нередко становятся дети юного возраста, которые подвергаются грубому и бесчеловечному насилию.

Объем доступных в Интернете материалов с элементами сексуального насилия над детьми оценить достаточно сложно, поскольку, в основном, такой контент хранится в так называемом «темном Интернете», то есть не индексируется поисковыми системами. «Темный Интернет» становится все более популярным среди правонарушителей, включая педофилов и сексуальных преступников, по мере того как они учатся соблюдать меры безопасности и осваивают техническую сторону сети.

Значительная часть материалов с изображением сексуального насилия над детьми была создана давно и просто загружается на различные ресурсы. Появление нового контента, как правило, свидетельствует о новой жертве. При обнаружении таких материалов необходимо принять следующие меры: сделать такие материалы недоступными и найти жертву насилия. Это даст возможность обезопасить жертву и предоставить ей необходимую помощь.

Варианты решения проблем

Для преодоления рисков, связанных с Интернетом, необходимо сочетать законодательные и нормативные меры (включая законодательные инициативы, саморегулирование и надзор, а также другие нормативно-правовые действия) с использованием технических инструментов, образовательных программ и информационно-пропагандистских мероприятий.

Законодательные меры

С нормативной точки зрения, многие страны приняли законодательство, согласно которому некоторые виды контента объявлены незаконными, хотя определение и толкование таких норм могут варьироваться в зависимости от страны. На международном уровне основными документами являетюся Конвенция ООН о правах ребенка и Факультативный Протокол к Конвенции о правах ребенка, касающийся торговли детьми, детской проституции и детской порнографии. Также необходимо отметить Конвенцию Совета Европы о киберпреступности и Конвенцию Совета Европы о защите детей от эксплуатации и посягательств сексуального характера (также известная под названием «Конвенция Лансароте»). Международный центр по делам пропавших и эксплуатируемых детей (International Centre for Missing & Exploited Children — ICMEC) разработал собственный механизм анализа и сопоставления национального законодательства в разных странах.

Совместное регулирование и саморегулирование

Эффективными подходами, особенно с точки зрения компаний, являются саморегулирование (компании берут на себя добровольные обязательства) и совместное регулирование (сочетание мер по регулированию, принятых на государственном и корпоративном уровнях). Например, интернет-провайдеры могут на добровольной основе оформлять запросы о предупреждении и удалении незаконных материалов и отфильтровывать незаконный контент, а социальные сети могли бы ввести минимальные требования для регистрации детей. Также важно наладить конструктивные отношения между компаниями и правоохранительными органами и четко определить механизмы и протоколы для совместной деятельности. Так, в 2008 г. Совет Европы опубликовал «Руководство по сотрудничеству между правоохранительными органами и интернет-провайдерами при борьбе с киберпреступностью»[104].

Технические меры

В деле борьбы с сексуальным насилием в отношении детей можно задействовать различные технические и процессуальные меры в сочетании с инициативами в других областях. Представляется целесообразным сочетать использование горячих линий для сообщений о нарушениях с подачей запросов о предупреждении и удалении. Так, Международная ассоциация горячих линий Интернета (International Association of Internet Hotlines — INHOPE) на данный момент объединяет 51 горячую линию в 45 странах, обрабатывает тысячи запросов каждый год и передает большинство из них правоохранительным органам в течение одного дня с момента поступления. К другим техническим мерам относится создание баз данных по установлению личности жертв и блокировке доступа к определенным сайтам, а также использование в расследованиях цифровых отпечатков пальцев и аналитических инструментов.

Образовательные и информационно-пропагандистские инициативы

На национальном, региональном и международном уровнях проводятся многочисленные кампании, нацеленных на детей, молодежь, их родителей, опекунов и преподавателей. В Интернете доступно множество информационных материалов по этому вопросу. МСЭ осуществляет Инициативу по защите ребенка в киберпространстве, в рамках которой предоставляются рекомендации детям, родителям, опекунам, учителям, компаниям и политикам[105]. В Европе Сеть безопасных интернет-центров (Network of Safer Internet Centers — INSAFE) объединяет 31 национальный центр и распространяет информационные материалы на различных языках. В феврале в некоторых странах отмечается День безопасного Интернета с целью пропаганды безопасного использования Интернета, в особенности среди детей и молодежи, во всех странах мира.

Координация действий

Для защиты детей и борьбы с сексуальным насилием в отношении детей в Интернете все заинтересованные стороны должны действовать сообща.

На родителей и учителей возлагается ответственность по воспитанию детей, их обучению и информированию, что создает первую линию защиты от рисков, связанных с Интернетом. Защита детей является основной обязанностью государства. Во многих странах защита детей в Интернете является одним из приоритетов государственной политики. Правоохранительные органы играют важную роль в борьбе с преступностью в Интернете и содействии региональному и международному сотрудничеству в области борьбы с сексуальным насилием. Европейское полицейское ведомство (Европол) и Международная организация уголовной полиции (Интерпол) ведут различные базы данных, которые помогают выявлять детей, пострадавших от сексуального насилия.

Компании обязаны обеспечить безопасность Интернета. Интернет-провайдеры могут сыграть ключевую роль в создании такой безопасной среды, используя различные средства, включая фильтры и механизмы уведомления о нарушениях. Существуют такие форматы сотрудничества, как Технологическая коалиция (Technology Coalition), Финансовая коалиция по борьбе с детской порнографией (США), Финансовая коалиция Азиатско-Тихоокеанского региона и Европейская финансовая коалиция, а также глобальный Альянс операторов GSMA против контента с элементами сексуального насилия в отношении детей.

Многие эксперты в этой области принимают активное участие в деятельности организаций гражданского общества и тем самым ставят свои знания на службу обществу. Неправительственные организации отдельных стран могут сотрудничать друг с другом в рамках международных сетей, таких как ECPAT International и ICMEC. Вопросами безопасности детей в Интернете занимается также ряд региональных организаций.

Значимый вклад в борьбу с сексуальной эксплуатацией и насилием в отношении детей как в Интернете, так и в реальной жизни способны внести неправительственные организации по оказанию помощи детям и горячие линии. Сотрудничество с такими организациям чрезвычайно важно, чтобы понять масштаб и природу этой проблемы. Они также могут быть задействованы в оказании психологической помощи жертвам насилия.

Примечания к разделу 3

[1] Radunović V (2013) DDoS — Available Weapon of Mass Disruption. Proceedings of the 21st Telecommunications Forum (TELFOR), 26—28 November, Belgrade, Serbia, pp. 5—9.

[2] Goodin D. Botnet that enslaved 770,000 PCs worldwide comes crashing down // Ars Technica, 13.04.2015. Адрес в Интернете: https://arstechnica.com/information-technology/2015/04/botnet-that-enslaved-770000-pcs-worldwide-comes-crashing-down/ [просмотрено 5 августа 2018 г.].

[3] United Nations General Assembly (1999) Resolution A/53/70. Developments in the Field of Information and Telecommunications in the Context of International Security. Адрес в Интернете: http://www.un.org/ga/search/view_doc.asp?symbol=A/RES/53/70 [просмотрено 5 августа 2018 г.].

[4] United Nations (2015) Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security. Адрес в Интернете: http://www.un.org/ga/search/view_doc.asp?symbol=A/70/174 [просмотрено 5 августа 2018 г.].

[5] Grigsby A. The UN GGE on cybersecurity: What is the UN's role? // Council on Foreign Relations Blog. 15.04.2015 Адрес в Интернете: http://blogs.cfr.org/cyber/2015/04/15/the-un-gge-on-cybersecurity-what-is-the-uns-role/ [просмотрено 5 августа 2018 г.].

[6] ITU (no date) Global Cybersecurity Agenda. Адрес в Интернете: http://www.itu.int/osg/csd/cybersecurity/gca/ [просмотрено 5 августа 2018 г.].

[7] ITU (no date) Global Cybersecurity Index. Адрес в Интернете: http://www.itu.int/en/ITU-D/Cybersecurity/Pages/GCI.aspx [просмотрено 5 августа 2018 г.].

[8] DiploFoundation (2015) IGF Summary. Just-in-time Reporting from the 2015 Internet Governance Forum. Адрес в Интернете: http://digitalwatch.giplatform.org/sites/default/files/IGFReportWEB.pdf [просмотрено 5 августа 2018 г.].

[9] Hague W (2011) London Conference on Cyberspace — Chairman's Summary. Адрес в Интернете: https://www.gov.uk/government/news/london-conference-on-cyberspace-chairs-statement [просмотрено 5 августа 2018 г.].

[10] Global Forum on Cyber Expertise (2015) The Hague Declaration on the GFCE. Адрес в Интернете: https://www.thegfce.com/documents/publications/2015/04/16/the-hague-declaration-on-the-gfce [просмотрено 5 августа 2018 г.].

[11] Statement by NATO Secretary General following the North Atlantic Council meeting at the level of NATO Defense Minister. Адрес в Интернете: https://www.nato.int/cps/en/natohq/opinions_132349.htm?selectedLocale=en [просмотрено 5 августа 2018 г.].

[12] NATO Cooperative Cyber Defence Centre of Excellence (2013) Tallinn Manual on the International Law Applicable to Cyber Warfare. Адрес в Интернете: https://ccdcoe.org/research.html [просмотрено 5 августа 2018 г.].

[13] Klimburg A (Ed.) (2012) National Cyber Security Framework Manual. NATO Cooperative Cyber Defence Centre of Excellence Publication. Адрес в Интернете: https://ccdcoe.org/publications/books/NationalCyberSecurityFrameworkManual.pdf [просмотрено 5 августа 2018 г.].

[14] Council of Europe (2001) Convention on Cybercrime. Адрес в Интернете: http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm [просмотрено 5 августа 2018 г.].

[15] European Union (2013) Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace. Адрес в Интернете: https://ec.europa.eu/digital-single-market/en/news/communication-cybersecurity-strategy-european-union-—-open-safe-and-secure-cyberspace [просмотрено 5 августа 2018 г.].

[16] European Union (2016) Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union. Адрес в Интернете: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2016.194.01.0001.01.ENG [просмотрено 5 августа 2018 г.].

[17] OSCE (2013) Decision No. 1106 Initial Set of OSCE Confidence-building Measures to Reduce the Risks of Conflict Stemming from the Use of Information and Communication Technologies. Адрес в Интернете: http://www.osce.org/pc/109168?download=true [просмотрено 5 августа 2018 г.].

[18] OSCE (2016) Decision No. 1202 OSCE Confidence-building Measures to Reduce the Risks of Conflict Stemming from the Use of Information and Communication Technologies. Адрес в Интернете: http://www.osce.org/pc/227281?download=true [просмотрено 5 августа 2018 г.].

[19] Organization of American States General Assembly (2003) Resolution AG/RES.1939 (XXXI-II-O/03). Development of an Inter-American Strategy to CombatThreats to Cybersecurity. Адрес в Интернете: http://www.oas.org/juridico/english/agres_1939.pdf [просмотрено 5 августа 2018 г.].

[20] Organization of American States (2011) Inter-American Cooperation Portal on Cyber-crime. Адрес в Интернете: http://www.oas.org/juridico/english/cyber.htm [просмотрено 5 августа 2018 г.].

[21] ASEAN Regional Forum (2012) Statement by the Ministers of Foreign Affairs on Cooperation in Ensuring Cyber Security. Адрес в Интернете: https://ccdcoe.org/sites/default/files/documents/ASEAN-120712-ARFStatementCS.pdf [просмотрено 5 августа 2018 г.].

[22] ASEAN (2014) ASEAN's Cyber Confidence Building Measures. Presentation by the ASEAN Secretariat. UNIDIR Cyber Stability Seminar 'Preventing Cyber Conflict', 10.02.2014, Geneva, Switzerland. Адрес в Интернете: http://www.unidir.ch/files/conferences/pdfs/the-asean-s-cyber-confidence-building-measures-en-1-958.pdf [просмотрено 5 августа 2018 г.].

[23] Grigsby A. Will China and Russia's updated code of conduct get more traction in a post-Snowden era? // Council on Foreign Relations blog, 28.01.2015. Адрес в Интернете: https://www.cfr.org/blog/will-china-and-russias-updated-code-conduct-get-more-traction-post-snowden-era [просмотрено 5 августа 2018 г.].

[24] African Union (2014) African Union Convention on Cyber Security and Personal Data Protection. Адрес в Интернете: http://www.au.int/en/treaties/african-union-convention-cyber-security-and-person-al-data-protection [просмотрено 5 августа 2018 г.].

[25] Microsoft (2015) International Cybersecurity Norms: Reducing Conflict in an Internet-dependent World. Адрес в Интернете: http://download.microsoft.com/download/7/6/0/7605D861-C57A-4E23-B823-568CFC36FD44/International_Cybersecurity_%20Norms.pdf [просмотрено 5 августа 2018 г.].

[26] Более подробную информацию о соотношении составляющих этого «треугольника» вы найдете в докладе семинара Форума по управлению Интернетом 2015 Cybersecurity, human rights and Internet business triangle. Адрес в Интернете: https://dig.watch/sessions/cybersecurity-human-rights-and-internet-business-triangle [просмотрено 5 августа 2018 г.].

[27] Domain Name System Security Extensions explained. Адрес в Интернете: https://www.icann.org/resources/pages/dnssec-qaa-2014-01-29-en [просмотрено 5 августа 2018 г.].

[28] Radunović V (2013) Waging a (private) cyber war. Адрес в Интернете: https://www.diplomacy.edu/blog/waging-private-cyberwar [просмотрено 5 августа 2018 г.].

[29] Perlroth N, Gellese D. Russian gang said to amass more than a billion stolen Internet credentials // New York Times. 05.08.2014. Адрес в Интернете: https://www.nytimes.com/2014/08/06/technology/russian-gang-said-to-amass-more-

than-a-billion-stolen-internet-credentials.html [просмотрено 5 августа 2018 г.].

[30] RT. Brazil and the EU have pushed forward their dialogue on developing a direct submarine link. 24.02.2014. Адрес в Интернете: https://www.rt.com/news/brazil-eu-cable-spying-504/ [просмотрено 5 августа 2018 г.].

[31] Keck Z. China expands cyber spying // The Diplomat. 12.04.2014. Адрес в Интернете: https://thediplomat.com/2014/04/china-expands-cyber-spying/ [просмотрено 5 августа 2018 г.].

[32] Ranger S. We're the real hacking victims, says China // ZDNet. 20.05.2014. Адрес в Интернете: https://www.zdnet.com/article/were-the-real-hacking-victims-says-china/ [просмотрено 5 августа 2018 г.].

[33] Spetalnick M, Martina M. Obama announces 'understanding' with China's Xion cyber theft but remains wary. Reuters. 26.09.2015. Адрес в Интернете: http://www.reuters.com/article/us-usa-china-idUSKCN0RO2HQ20150926 [просмотрено 5 августа 2018 г.].

[34] G20 (2015) G20 Leaders' Communiqué. Antalya Summit, 15–16 ноября 2015 г. Адрес в Интернете: https://g20.org/profiles/g20/modules/custom/g20_beverly/img/timeline/Turquia/2015-g20-final-declaration-eng.pdf [просмотрено 5 августа 2018 г.].

[35] Schneier B. NSA surveillance: A guide to staying secure // The Guardian.06.09.2013. Адрес в Интернете: https://www.theguardian.com/world/2013/sep/05/nsa-how-to-remain-secure-surveillance [просмотрено 5 августа 2018 г.].

[36] Перечень групп, организаций и инициатив по борьбе с киберпреступностью по всему миру см. на сайте Совета Европы. Адрес в Интернете: http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/networks/Networks_en.asp [просмотрено 5 августа 2018 г.].

[37] The Commonwealth (no date) Commonwealth Cybercrime Initiative. Адрес в Интернете: http://thecommonwealth.org/commonwealth-cybercrime-initiative [просмотрено 5 августа 2018 г.].

38 Bailey C (2002) The International Convention on Cybercrime. Association for Progressive Communications. Адрес в Интернете: http://rights.apc.org/privacy/treaties_icc_bailey.shtml [просмотрено 5 августа 2018 г.].

[39] Council of Europe (2014) Recommendation CM/Rec (2014)6 of the Committee of Ministers to member states on a Guide to human rights for Internet users. Адрес в Интернете: https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=090000168041d5b31 [просмотрено 5 августа 2018 г.].

[40] European Union (2006) Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC. Адрес в Интернете: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:105:0054:0063:EN:PDF [просмотрено 5 августа 2018 г.].

[41] Подробнее о вопросах хранения данных пользователей в ЕС см. European Commission (2011) Evaluation report on the Data Retention Directive (Directive 2006/24/EC). Адрес в Интернете: https://eur-lex.europa.eu/LEXUriServ/LexUriServ.do?uri=COM:2011:0681:FIN:EN:PDF [просмотрено 5 августа 2018 г.].

[42] CJEU (2014) Judgement of the Court in Joined Cases C-293/12 and C-594/12: Digital Rights Ireland v Minister for Communications, Marine and Natural Resources and Others. Адрес в Интернете: http://curia.europa.eu/juris/document/document.jsf?text=&docid=150642&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=106306 [просмотрено 5 августа 2018 г.].

[43] European Commission (2004) Critical Infrastructure Protection in the Fight Against Terrorism. Communication from the Commission to the Council and the European Parliament. Адрес в Интернете: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52004DC0702 [просмотрено 5 августа 2018 г.].

[44] Essers L. Cyberattack on German steel factory causes 'massive damage' // IT World, 19.12.2014. Адрес в Интернете: http://www.itworld.com/article/2861675/cyberattack-on-german-steel-factory-causes-massive-damage.html [просмотрено 5 августа 2018 г.].

[45] ETF (2007) Internet Security Glossary, Version 2. Адрес в Интернете: https://tools.ietf.org/html/rfc4949 [просмотрено 5 августа 2018 г.].

[46] USA White House (2013) Presidential Policy Directive — Critical Infrastructure Security and Resilience. Адрес в Интернете: https://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil [просмотрено 5 августа 2018 г.].

[47] European Commission (2006) European Programme for Critical Infrastructure Protection. Адрес в Интернете: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=URISERV%3Al33260 [просмотрено 5 августа 2018 г.].

[48] European Union (2008) Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection. Адрес в Интернете: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:345:0075:0082:EN:PDF [просмотрено 5 августа 2018 г.].

[49] OECD (2008) Recommendation of the Council on the Protection of Critical Information Infrastructures. Адрес в Интернете: https://legalinstruments.oecd.org/en/instruments/121 [просмотрено 5 августа 2018 г.].

[50] The Cyberterrorism Project (2013) What is cyberterrorism? UK Legal Definition. Адрес в Интернете: http://www.cyberterrorism-project.org/what-is-cyberterrorism [просмотрено 5 августа 2018 г.].

[51] Krasavin S (2009) What is Cyber-terrorism? Computer Crime Research Center. Адрес в Интернете: http://www.crime-research.org/library/Cyber-terrorism.htm [просмотрено 5 августа 2018 г.].

[52] Denning D (2000) Statement. Адрес в Интернете: https://fas.org/irp/congress/2000_hr/00-05-23denning.htm [просмотрено 5 августа 2018 г.].

[53] Joint Communiqué of the 14th Meeting of the Foreign Ministers of the Russian Federation, the Republic of India and the People's Republic of China, 18.04.2016. Адрес в Интернете: http://www.mea.gov.in/bilateral-documents.htm?dtl/24751/Joint_Communiqu_of_the_13th_Meeting_of_the_Foreign_Ministers_of_the_Russian_Federation_the_Republic_of_India_and_the_Peoples_Republic_of_China [просмотрено 5 августа 2018 г.].

[54] UN News Centre (2016) Security Council requests UN panel to propose global framework on countering terrorist propaganda. 11 May. Адрес в Интернете: https://news.un.org/en/story/2016/05/528972-security-council-requests-un-panel-propose-global-framework-countering#.WAszjTeZIqZ [просмотрено 5 августа 2018 г.].

[55] G7 (2016) G7 Action Plan on Countering Terrorism and Violent Extremism. Адрес в Интернете: https://www.mofa.go.jp/files/000160278.pdf [просмотрено 5 августа 2018 г.].

[56] Microsoft (2016) Microsoft's approach to terrorist content online. Адрес в Интернете: https://blogs.microsoft.com/on-the-issues/2016/05/20/microsofts-approach-terrorist-content-online/#sm.0000%201i30hhw72cdzpxr8cky3uuvbs [просмотрено 5 августа 2018 г.].

[57] Greenberg A. Google's clever plan to stop aspiring ISIS recruits. Wired, 17.09.2016. Адрес в Интернете: https://www.wired.com/2016/09/googles-clever-plan-stop-aspiring-isis-recruits/ [просмотрено 5 августа 2018 г.].

[58] UN News Centre. UN expert warns combat against violent extremism could be used as 'excuse' to curb free speech. 03.05.2016. Адрес в Интернете: http://www.un.org/apps/news/story.asp?NewsID=53841#. WAs1FjeZIqb [просмотрено

5 августа 2018 г.].

[59] GCN. DOD wants cyberterrorism-prediction software. 31.07.2012y. Адрес в Интернете: https://gcn.com/articles/2012/07/31/agg-dod-small-biz-software-support.aspx [просмотрено 5 августа 2018 г.].

[60] The Clean IT Project (2012) About the project. Адрес в Интернете: http://www.cleanitproject.eu/about-the-project/ [просмотрено 5 августа 2018 г.].

[61] United Nations General Assembly (2006) Resolution A/60/288. The United Nations Global Counter-Terrorism Strategy. Адрес в Интернете: http://www.un.org/en/ga/search/view_doc.asp?symbol=A/RES/60/288 [просмотрено 5 августа 2018 г.].

[62] UNODC (2012) The use of the Internet for terrorist purposes. Адрес в Интернете: https://www.unodc.org/documents/frontpage/Use_of_Internet_for_Terrorist_Purposes.pdf [просмотрено 5 августа 2018 г.].

[63] UN Security Council Counter-Terrorism Committee (2015) Special Meeting of the Counter-Ter-rorism Committee and technical sessions of the Counter-Terrorism Committee Executive Directorate on preventing and combating abuse of ICT for terrorist purposes. Адрес в Интернете: https://www.un.org/sc/ctc/news/2015/11/19/special-meeting-of-the-counter-terrorism-committee-and-technical-sessions-of-the-counter-terrorism-committee-executive-directorate-on-preventing-and-combating-abuse-of-ict-for-terrorist-purposes-new/ [просмотрено 5 августа 2018 г.].

[64] Berenger RD (2012) Cyber Warfare. In Yan Z [ed] Encyclopedia of Cyber Behavior. Hershey, PA: Information Science Reference, pp. 1074—1087.

[65] BBC News. Estonia hit by 'Moscow cyber war'. 17.05.2007. Адрес в Интернете: http://news.bbc.co.uk/2/hi/europe/6665145.stm [просмотрено 5 августа 2018 г.].

[66] Swaine J. Georgia: Russia 'conducting cyber war' // The Telegraph, 11.08.2008. Адрес в Интернете: http://www.telegraph.co.uk/news/worldnews/europe/georgia/2539157/Georgia-Russia-con-ducting-cyber-war.html [просмотрено 5 августа 2018 г.].

[67] Sanger D. Obama sped up wave of cyberattacks against Iran // New York Times, 01.06.2012. Адрес в Интернете: http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html [просмотрено 5 августа 2018 г.].

[68] Nakashima E. Iran blamed for cyberattacks on U.S. banks and companies // The Washington Post, 21.09.2012. Адрес в Интернете: https://www.washingtonpost.com/world/national-security/iran-blamed-for-cyberattacks/2012/09/21/afbe2be4-0412-11e2-9b24-ff730c7f6312_story.html [просмотрено 5 августа 2018 г.].

[69] Lee C and Solomon J. US targets North Korea in retaliation for Sony hack // The Wall Street Journal, 03.01.2015 Адрес в Интернете: http://www.wsj.com/articles/u-s-penalizes-north-korea-in-retaliation-for-sony-hack-1420225942 [просмотрено 5 августа 2018 г.].

[70] Foster P. China denies Pentagon cyber-attack claims // The Telegraph, 07.05.2012. Адрес в Интернете: http://www.telegraph.co.uk/news/worldnews/asia/china/10040757/China-denies-Pentagon-cyber-attack-claims.html [просмотрено 5 августа 2018 г.].

[71] Ranger S. We're the real hacking victims, says China // ZDNet, 20.05.2014. Адрес в Интернете: https://www.zdnet.com/article/were-the-real-hacking-victims-says-china/ [просмотрено 5 августа 2018 г.].

[72] Munich Security Conference (2015) Collapsing Order, Reluctant Guardians? Munich Security Report 2015. Munich Security Conference. Адрес в Интернете: https://www.securityconference.de/en/ activities/munich-security-report/ [просмотрено 5 августа 2018 г.].

[73] Radunović V (2013) DDoS — Available Weapon of Mass Disruption. Proceedings of the 21st Telecommunications Forum (TELFOR), 26—28 November, Belgrade, Serbia, pp. 5—9.

[74] Appelbaum et al. Prying Eyes: Inside the NSA's War on Internet Security // Der Spiegel, 28.12.2014. Адрес в Интернете: http://www.spiegel.de/international/germany/inside-the-nsa-s-war-on-internet-security-a-1010361.html [просмотрено 5 августа 2018 г.].

[75] The Wassenaar Arrangement. Адрес в Интернете: http://www.wassenaar.org/ [просмотрено 5 августа 2018 г.].

[76] Подход с использованием «Клиппер чипа» был предложен правительством США в 1993 г. и заключался в использовании этого чипа во всех телефонах и других устройствах голосовой связи, чтобы иметь возможность на законных основаниях заниматься слежкой. Однако эта инициатива вызвала шквал протеста со стороны правозащитников и общества в целом, что вынудило власти США отказаться от проекта в 1995 г. Denning D (1995) The case for clipper. MIT Technology Review. MIT: Cambridge, MA, USA. Адрес в Интернете: http://encryption_policies.tripod.com/us/denning_0795_clipper.htm [просмотрено 5 августа 2018 г.].

[77] Huggler J. Man arrested in Germany on suspicion of illegal arm dealing in terror crack-down // The Telegraph, 27.11.2015. Адрес в Интернете: https://www.telegraph.co.uk/news/worldnews/europe/germany/12020249/Paris-attackers-bought-weapons-from-arms-dealer-in-Germany.html [просмотрено 5 августа 2018 г.].

[78] Исследование, проведенное Центром Беркмана по изучению интернета и общества (Berkman Centre for Internet and Society) при Гарвардском университете, показало, что власти не лишатся возможности следить за деятельностью террористов и преступников. Конечно, в некоторых случаях рост доступности технологий шифрования затрудняет розыскную деятельность, однако решить эту проблему можно за счет развития технологий и рыночных механизмов, что позволит властям получать необходимую информацию. См. подробнее: The Berkman Center for Internet and Society. Harvard University (2016). Don't Panic. Making Progress on the 'Going Dark' Debate. Адрес в Интернете: https://cyber.harvard.edu/pubrelease/dont-panic/Dont_Panic_Making_Progress_on_Going_Dark_Debate.pdf [просмотрено 5 августа 2018 г.].

[79] Обзор 865 единиц аппаратного и программного обеспечения из 55 стран с точки зрения использования технологий шифрования показал, что в силу широкой доступности таких устройств и ПО, включение в них в обязательном порядке средств, которые бы позволяли властям обходить шифрование, «было бы неэффективным». Дело в том, что решения в области шифрования разрабатываются по всему миру, и преступники могут легко перейти на продукты, на которые не распространяются требования определенной юрисдикции. Вместо этого, создание обязательных лазеек скажется на «невинных пользователях таких продуктов», что сделает людей в странах с такими требованиями «уязвимыми перед лицом как преступников, так и властей». См. подробнее: Schneier B, Seidel K, Vijay-akumar S (2016) A Worldwide Survey of Encryption Products. Адрес в Интернете: https://www.schneier.com/academic/paperfiles/worldwide-survey-of-encryption-products.pdf [просмотрено 5 августа 2018 г.].

[80] Адрес в Интернете: http://ap.ohchr.org/documents/dpage_e.aspx?si=A/HRC/29/32 [просмотрено 5 августа 2018 г.].

[81] DiploFoundation. Apple vs FBI: A Socratic dialogue on privacy and security // DiploFoundation blog. 22.03.2016. Адрес в Интернете: https://www.diplomacy.edu/blog/apple-vs-fbi-socratic-dialogue-privacy-and-security [просмотрено 5 августа 2018 г.].

[82] В 2016 г. финансовый троян Dridex стал предметом особой озабоченности. Компании, специализирующиеся на вопросах кибербезопасности, называли его «одной из наиболее серьезных интернет-угроз для потребителей и компаний». Этот троян распространялся посредством массивной спам-рассылки с целью сбора данных о счетах пользователей в сотнях банков и других фи-

нансовых организаций. См. подробнее: O'Brien D (2016) Dridex: Tidal waves of spam pushing dangerous financial Trojan. Symantec. Адрес в Интернете: http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/dridex-financial-trojan.pdf [просмотрено 5 августа 2018 г.].

83 Trustwave (2016) Global Security Report. Адрес в Интернете: https://www.trustwave.com/Resources/Trustwave-Blog/Introducing-the-2016-Trustwave-Global-Security-Report/ [просмотрено 5 августа 2018 г.].

84 Gudkova D et al. (2016) Spam and phishing in Q1 2016. Kaspersky Lab. Адрес в Интернете: https://securelist.com/analysis/quarterly-spam-reports/74682/spam-and-phishing-in-q1-2016/ [просмотрено 5 августа 2018 г.].

85 Троян Locky работает весьма незамысловатым способом: пользователей обманным путем убеждают открыть файл, приложенный к спам-рассылке, в котором содержится вредоносный код. После установки на устройстве пользователя, этот троян шифрует все данные, а пользователя просят заплатить выкуп, чтобы вернуть свои файлы. Подробнее о трояне Locky см.: Sinitsyn F (2016) Locky: the encryptor taking the world by storm. Kaspersky Lab. Адрес в Интернете: https://securelist.com/locky-the-encryptor-taking-the-world-by-storm/74398/ [просмотрено 5 августа 2018 г.].

86 Подробнее о Can-Spam см.: the Bureau of Consumer Protection (2009). The CAN-SPAM Act: A Compliance Guide for Business. Адрес в Интернете: https://www.ftc.gov/tips-advice/business-center/guidance/can-spam-act-complianceguide-business [просмотрено 5 августа 2018 г.].

87 В июне 2016 г. гражданин США был приговорен к двум с половиной годам тюрьмы и штрафу в 310 628,55 долл. в качестве компенсации за отправку более 27 миллионов писем спама пользователям Facebook. По сообщению прокурора Северного округа штата Калифорния, этот человек незаконно получил, хранил и использовал данные учетных записей пользователей Facebook и зарабатывал деньги, перенаправляя пользователей на другие сайты. Эта схема проработала с ноября 2008 г. по март 2009 г. и затронула около 500 000 учетных записей. Подробнее см. в пресс-релизе прокурора Северного округа штата Калифорния. Адрес в Интернете: https://www.justice.gov/usao-ndca/pr/sanford-spam-king-wallace-sentenced-two-and-half-years-custody-spamming-facebook-users [просмотрено 5 августа 2018 г.].

88 European Union (2012) Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector. Адрес в Интернете: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32002L0058 [просмотрено 5 августа 2018 г.].

89 BBC NEWS. European anti-spam laws lack bite. 28.04.2004. Адрес в Интернете: http://news.bbc.co.uk/2/hi/technology/3666585.stm [просмотрено 5 августа 2018 г.].

90 New Zealand Law Society. NZ signatory to international anti-spam MOU.15.06.2016. Адрес в Интернете: https://www.lawsociety.org.nz/news-and-communications/latest-news/news/nz-signatory-to-international-anti-spam-mou [просмотрено 5 августа 2018 г.].

91 ITU (2012) Resolution 52 of the World Telecommunication Standardization Assembly: Countering and combating spam. Адрес в Интернете: https://ccdcoe.org/sites/default/files/documents/ITU-121129-CombSpamWTSARes52.pdf [просмотрено 5 августа 2018 г.].

92 APEC (2012) APEC Principles for Action against Spam. Адрес в Интернете: http://www.apec.org/Meeting-Papers/Sectoral-Ministerial-Meetings/Telecommunications-and-Information/2005_tel/annex_e.aspx [просмотрено 5 августа 2018 г.].

93 African Union (2014) African Union Convention on Cyber Security and Personal Data Protection. Адрес в Интернете: https://au.int/sites/default/files/treaties/29560-treaty-0048_-_african_union_convention_on_cyber_security_and_personal_data_protection_e.pdf [просмотрено 5 августа 2018 г.].

94 Сбору и обновлению статистики по странам, которые содействуют распространению спама, посвящен проект Spamhaus Project. С этими данными можно ознакомиться по адресу: https://www.spamhaus.org/statistics/countries/ [просмотрено 5 августа 2018 г.]. Благодаря проекту Spamhaus также можно ознакомиться со статистической информацией по ряду других вопросов, который касаются спама, включая деятельность интернет-провайдеров по содействию спам-рассылкам, в проекте указаны самые крупные распространители спама, страны, где зафиксировано наибольшее количество спам-ботов, домены верхнего уровня, наиболее подверженные спаму и т. д.

95 Проверка подлинности электронной записи с использованием криптографических алгоритмов; термин «электронная подпись» имеет более широкое значение, включающее широкий круг средств проверки подлинности цифровых подписей и биометрических данных.

96 Подробнее об этих трех подходах см.: ILPF (1999) Survey of Inter-national Electronic and Digital Signature Initiatives. Адрес в Интернете: http://www.ilpf.org/groups/survey.htm#IB [просмотрено 5 августа 2018 г.].

97 European Union (2014) Regulation (EU) No. 910/2014 on electronic identification and trust services for electronic transactions in the internal market. Адрес в Интернете: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2014.257.01.0073.01.ENG [просмотрено 5 августа 2018 г.].

98 UNCITRAL (2001) Model Law on Electronic Signatures. Адрес в Интернете: http://www.uncitral.org/uncitral/uncitral_texts/electronic_commerce/2001Model_signatures.html [просмотрено 5 августа 2018 г.].

99 Longmuir G (2000) Privacy and Digital Authentication. Адрес в Интернете: www.longmuir.net/papers/Research%20Paper.doc [просмотрено 5 августа 2018 г.]. В данной работе затрагивается вопрос о необходимости средств проверки подлинности в цифровом мире с точки зрения индивида, общества и государства.

100 В соответствии с правовыми инструментами и международным обиходом, под «ребенком» понимается лицо, не достигшее возраста 18 лет.

101 С примером типологии можно ознакомиться в Barbosa A et al. (2013) Risks and Safety on the Internet: Comparing Brazilian and European Results. London: LSE. Адрес в Интернете: http://eprints.lse.ac.uk/54801/ [просмотрено 5 августа 2018 г.]; OECD (2012) The Protection of Children Online; Recommendation of the OECD Council. Адрес в Интернете: http://www.oecd.org/sti/ieconomy/childrenonline_with_cover.pdf [просмотрено 5 августа 2018 г.].

102 EU Kids Online (2014) EU Kids Online: Findings, Methods, Recommendations. London: LSE. Адрес в Интернете: http://eprints.lse.ac.uk/60512/ [просмотрено 5 августа 2018 г.].

103 Термин «детская порнография» достаточно противоречив, поскольку под словом «порнография» обычно понимается изображение действий сексуального характера между взрослыми, добровольно участвующих в такой деятельности. Таким образом, такой термин не отражает присущие детской порнографии элементы насилия и эксплуатации. В этой связи вместо него такие материалы все чаще называют «материалами с изображением сексуального насилия над детьми» и «материалами с изображением сексуальной эксплуатации детей». См.: Interagency Working Group on Sexual Exploitation of Children (2016) Terminology Guidelines for the Protection of Children from Sexual Exploitation and Sexual Abuse. Адрес в Интернете: http://www.ilo.org/ipec/Informationresources/WCMS_490167/lang--en/index.htm [просмотрено 5 августа 2018 г.].

104 Council of Europe (2008) Guidelines for the cooperation between lawenforcement and Internet service providers against cybercrime. Адрес в Интернете: https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTM

Content?documentId=09000016802fa3ba [просмотрено 5 августа 2018 г.].

[105] ITU (no date) Guidelines for Child Online Protection. Адрес в Интернете: http://www.itu.int/en/cop/Pages/guidelines.aspx [просмотрено 5 августа 2018 г.].

Раздел 4

Правовые аспекты

Правовые аспекты

В эпоху Интернета право продолжает выполнять те же социальный функции, что и тысячи лет назад, когда наши предшественники только начинали организовывать человеческое общество согласно определенным правилам. Право регулирует права и обязанности физических лиц и созданных ими организаций, от компаний до государств. Огромное значение для будущего развития Интернета как средства социального взаимодействия и источника экономического роста отводится принципам верховенства права и правовой определенности.

В области правового регулирования Интернета произошел переход от концепции «киберправа» к концепции «реального» права. Когда Интернет только появился, преобладали сторонники «киберправа», которые считали, что Интернет порождает новые виды социальных взаимоотношений в киберпространстве, и для их регулирования необходимо формулировать новые «киберзаконы». В обоснование своей позиции они говорили о том, что сама скорость и объем трансграничной коммуникации в условиях Интернета будут препятствовать применению существующих правовых норм, и что традиционные виды регулирования (например, в уголовной и налоговой сферах) недостаточно эффективны[1]. При этом важно не забывать, что законодательные нормы не делают противозаконное поведение невозможным, а только устанавливают наказание за него.

С проникновением Интернета во все сферы общественной жизни большей популярностью стало пользоваться «реальное» право. Согласно этому подходу, Интернет рассматривается как явление, аналогичное предшествующим ему телекоммуникационным технологиям (от сигналов дымом до телефонии). Соответственно, существующие нормы применимы и к Интернету. Например, в 2013 г. Группа правительственных экспертов ООН обнародовала доклад, в котором утверждалось, что существующие нормы международного права применимы к использованию ИКТ государствами[2]. Впоследствии это решение было поддержано на уровне Генеральной Ассамблеи ООН в рамках обзора Всемирной встречи на высшем уровне по вопросам информационного общества WSIS+10[3]. Что касается правозащитной тематики, то в резолюциях Генеральной Ассамблеи и Совета по правам человека ООН

четко сказано, что права человека, которые гарантированы в реальном мире, также подлежат защите в виртуальном пространстве[4].

Очевидно, что существующие правовые нормы применимы в Интернете. Вопрос лишь в том, каким образом применять эти нормы. Например, достаточно проблематичным представляется обеспечение правовой помощи в международных разбирательствах. Физические и юридические лица могут исходить из норм международного частного права, а власти стран могли бы опираться на механизмы, предусмотренные международным публичным правом. Оба подхода имеют давнюю историю и были изначально разработаны в эпоху, когда трансграничных контактов было гораздо меньше. Такие механизмы необходимо проанализировать и при необходимости усовершенствовать, чтобы обеспечить доступ к правосудию в делах по Интернету для людей и организаций по всему миру.

Правовые механизмы

Существует обширный набор правовых механизмов, которые либо уже применяются, либо могут быть применены в области управления Интернетом. Они подразделяются на механизмы, применяемые на национальном уровне, и механизмы, применяемые на международном уровне.

Национальные правовые механизмы, социальные нормы и саморегулирование

Большинство правовых механизмов, регулирующих деятельность в Интернете, действуют на национальном уровне и неизбежно входят в противоречие с трансграничным характером Интернета. В некоторых случаях, например, право на забвение, решения суда имеют последствия далеко за пределами юрисдикции, в которой они принимаются. Ожидается, что граждане и компании будут все чаще обращаться в национальные суды (в случае с ЕС, речь идет о наднациональном Суде Европейского союза за защитой своих законных прав и интересов в Интернете).

Законодательные нормы

Законодательная деятельность в отношении Интернета постепенно активизируется. В особенности это касается стран, где Интернет широко распространен и оказывает огромное влияние на экономические и социальные отношения. На сегодняшний день приоритетными областями законодательной деятельности являются защита частной жизни, защита данных пользователей, защита интеллектуальной собственности, налогообложение и противодействие киберпреступности.

Постоянное развитие технологий привело к появлению принципа технологического нейтралитета в отношении разработки законодательных мер, касающихся технологий. На практике этот принцип означает, что в законе не следует упоминать конкретные технологии или отдавать предпочтение одной из них по сравнению с другими, а скорее придерживаться общих терминов, чтобы закон мог оставаться нейтральным.

Однако социальные отношения слишком многогранны, чтобы 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. Опасность правового отставания — это важный аспект, который необходимо учитывать в процессе регулирования Интернета.

Социальные нормы (обычаи)

Как и нормы закона, социальные нормы запрещают определенное поведение. В отличие от законодательства, ни одно из государственных учреждений не имеет полномочий навязывать исполнение этих норм. Их выполнение обеспечивается сообществом посредством воздействия одних его членов на других. На заре своей истории Интернет регулировался практически исключительно совокупностью социальных норм, получивших название «нетикет» (netiquette). Основной мерой наказания за их нарушение было давление со стороны других членов интернет-сообщества и исключение из сообщества.

В течение этого периода развития, когда Интернет использовался сравнительно небольшой группой людей, преимущественно исследователей, преподавателей и студентов, социальные нормы в целом соблюдались. Рост Интернета сделал предписания социального характера неэффективными. Этот вид регулирования все еще может использоваться, однако лишь внутри закрытых групп, обладающих хорошо развитыми внутренними связями. Например, сообщество Wikipedia управляется социальными нормами, на основе которых определяются подходы к написанию статей и урегулированию конфликтов в отношении их содержания. Эти нормы легли в основу кодифицированных правил саморегулирования Wikipedia.

Саморегулирование

В Белой книге по управлению Интернетом[5], которая была подготовлена правительством США в 1998 г. и, в конечном счете, привела к созданию ICANN, подчеркивалась предпочтительность саморегулирования в управлении Интернетом. Саморегулирование содержит в себе некоторые элементы, характерные также для описанных выше социальных норм. Основное различие заключается в том, что, в отличие от социальных норм, которые нередко довольно расплывчаты, саморегулирование основывается на хорошо продуманном и организованном подходе. Нормы саморегулирования обычно закрепляют нормы надлежащего поведения.

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

Хотя саморегулирование может стать полезным нормативным инструментом, опора на него сопряжена с определенными рисками при решении вопросов, вызывающих большой интерес общественности, например, в области контроля над содержанием материалов Интернета, свободы выражения мнений и защиты права на неприкосновенность частной жизни. Могут

ли интернет-провайдеры принимать решения вместо уполномоченных правовых институтов? Смогут ли они оценить, какие материалы считать приемлемыми, а какие нет?

Судебная практика

Судебная практика (решения судов) оказывает существенное влияние на регулирование Интернета. На ранних стадиях становления виртуального пространства, когда все основные события происходили в США, судебная практика, будучи краеугольным камнем правовой системы страны, играла ключевую роль в развитии Интернета. Поскольку Интернет был тогда чем-то новым, его регулирование преимущественно основывалось на судебной практике (в рамках прецедентного англо-саксонского права). Судьям приходилось выносить приговоры, несмотря на отсутствие на тот момент необходимых инструментов, то есть правовых механизмов. Таким образом, в основу формирования новой области права легли прецеденты.

В последнее время судебная практика в ЕС стала играть огромную роль в регулировании Интернета. Например, в мае 2014 г. Суд ЕС ввел «правило забвения» или, если выражаться более точным языком, право на удаление определенной информации из результатов поиска, что может распространяться на интернет-контент, исходящий как из Европы, так и других регионов мира. В октябре 2015 г. решением суда было отменено соглашение Safe Harbour (Тихая гавань) между США и ЕС, что вынудило обе стороны провести переговоры и принять новое соглашение о передаче персональных данных между юрисдикциями.

Подробнее о решениях Суда ЕС, касающихся неприкосновенности частной жизни и защиты персональных данных, см. ***Раздел 8.***

Международные правовые документы

В силу трансграничного характера деятельности в Интернете для ее регулирования требуются международные правовые инструменты. Однако когда речь заходит о международном праве, оказывается, что различное понимание терминов может приводить к очень существенным последствиям. Термин «международное право», как правило, используется как синоним международного публичного права, которое создается государствами, обычно путем заключения международных договоров и конвенций. Международное публичное право охватывает многие вопросы, связанные с Интернетом, включая телекоммуникации, права человека и киберпреступность. Однако применительно к Интернету международное частное право имеет не меньшее, а возможно, и большее значение, поскольку многие судебные дела в этой области касаются договоров, деликтов и коммерческих обязательств.

Международное частное право

Вследствие глобального характера Интернета широкое распространение получили правовые споры, в которых участвуют частные лица и институты, подпадающие под различные национальные юрисдикции. В соответствии с нормами международного частного права устанавливаются критерии для определения соответствующей юрисдикции и применимого права в отношении иностранных лиц (например, в случае с наличием двух или более организаций из разных стран), например, в рамках какой юрисдикции следует рассматривать споры между интернет-компаниями (например, Facebook или Twitter) и их пользователями по всему миру. При определении соответсвующей юрисдикции учитывается статус лица по отношению к национальной юрисдикции (например, гражданство, место проживания), а также связь между конкретной транзакцией и национальной юрисдикцией (например, где заключен договор, где произошел обмен товарами).

Однако международное частное право используется для разрешения судебных споров, связанных с Интернетом, только в редких случаях, возможно, по причине того, что его процедуры зачастую сложны, медленны и дороги. Основные механизмы международного частного права были разработаны в то время, когда трансграничное взаимодействие не было столь распространенным и интенсивным, и соответственно, судебных дел с участием частных лиц и организаций, относящихся к различным юрисдикциям, было не так много. Международное частное право должно стать более оперативным, малозатратным и гибким, чтобы обеспечивать правовую защиту при разбирательстве дел, связанных с Интернетом.

Международное публичное право

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

Международные конвенции

Международными конвенциями называют межгосударственные соглашения, обязательные для исполнения заключившими их сторонами. Некоторые считают, что большинство вопросов, связанных с Интернетом, регулируется Регламентом международной электросвязи (РМЭ) МСЭ. Однако этот регламент был принят в 1988 г., то есть на заре Интернета, и не содержал положений, которые напрямую касались Интернета. Вопрос о том, следует ли включить в РМЭ положения, посвященные непосредственно Интернету, был в повестке конференции WCIT-12. Тогда был выдвинут ряд предложений, которые могли существенно повлиять на функционирование Интернета, принципы его работы, а также на безопасность Интернета и его контент. Однако страны-участники не смогли договориться и включить в новую версию РМЭ 2012 г. прямую отсылку к Интернету. Несмотря на это ряд государств-членов МСЭ сочли, что некоторые положения пересмотренного РМЭ могут быть истолкованы, как регулирущие отдельные чувствительные вопросы Интернета, что, по их мнению, выходит за рамки деятельности МСЭ[6]. Такие страны решили не подписывать новую версию регламента и, таким образом, продолжают следовать РМЭ в редакции 1988 г.

Помимо документов МСЭ, единственной конвенцией, которая напрямую регулирует отношения в Интернете, является Конвенция о киберпреступности Совета Европы. Однако многие другие механизмы международного публичного права, от Устава ООН до более узких международных правовых документов, применимы для регулирования различных аспектов управления Интернетом, таких как права человека, торговля и права интеллектуальной собственности.

Международное обычное право

Нормообразование в международном обычном праве включает два элемента: наличие «общей практики» (consuetudo) и признание ее в качестве юридически обязательной (opinio iuris). Развитие обычного права обычно требует длительного времени для становления общей практики. Например, основные нормы морского права формировались государствами на протяжении многих столетий и были кодифицированы в 1982 г. с принятием Конвенции по морскому праву. Однако в современном мире все меняется гораздо быстрее, и разработка норм обычного права должна занимать меньше времени. Чтобы ускорить разработку таких норм, итальянский юрист Роберто Аго предложил следовать концепции «diritto spontaneo» или «мгновенного международного обычного права»[7].

«Мягкое право»

В дискуссиях об управлении Интернетом часто используется термин «мягкое право». Большинство определений «мягкого права» указывает на то, чем оно не является: это не юридически обязательный инструмент. Инструменты «мягкого права» представляют собой принципы и нормы, а не четко определенные правила. Обычно они сформулированы в таких международных документах, как декларации и резолюции. «Мягкое право» не обладает юридической силой, и поэтому его исполнение не может быть обеспечено международными судами или иными механизмами разрешения споров.

Основные итоговые документы WSIS, включая Декларацию принципов, Женевский план действий, Тунисскую программу для информационного общества и региональные декларации, могут стать базой для создания норм «мягкого права». Они не обладают юридической силой, но, как правило,

являются результатом длительных переговоров и достижения консенсуса между всеми странами. Обязательства, которые государства и иные заинтересованные стороны принимают на себя в ходе обсуждения норм «мягкого права» и достижения общего согласия, дают основание рассматривать эти документы как нечто большее, чем политические декларации о намерениях.

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

Основополагающие принципы международного права (ius cogens)

В статье 53 Венской конвенции о праве международных договоров[8] дается следующее определение ius cogens: «Норм [а], которая принимается и признается международным сообществом государств в целом как норма, отклонение от которой недопустимо и которая может быть изменена только последующей нормой общего международного права, носящей такой же характер». Британский юрист и бывший сотрудник Колледжа Всех Душ Университета Оксфорда Иэн Браунли приводит следующие примеры норм ius cogens:

- запрет на применение силы.
- недопущение геноцида.
- принцип отказа от расовой дискриминации.
- осуждение преступлений против человечности.
- нормы, запрещающие работорговлю и пиратство[9].

При управлении Интернетом нормы ius cogens могут использоваться в отношении определенных видов деятельности, которые такими нормами запрещены (например, геноцид, расовая дискриминация, рабство и т.д.).

Юрисдикция

Под юрисдикцией понимается право суда или государственных органов выносить решения в ходе разбирательств. Взаимоотношения юрисдикции и Интернета изначально противоречивы, так как юрисдикция основывается, главным образом, на географическом разделении мира на государства.

Каждое государство имеет суверенное право осуществлять юрисдикцию на своей территории. Однако Интернет делает возможным активное трансграничное взаимодействие, которое сложно (хотя и можно) отслеживать с помощью традиционных правительственных механизмов. Вопрос о юрисдикции в Интернете снова возвращает нас к одной из центральных проблем, связанных с управлением Интернетом: каким образом можно «прикрепить» Интернет к существующей правовой и политической карте?[10]

В последние годы суды все чаще сталкиваются с проблемой определения юрисдикции. В качестве наиболее ярких примеров можно привести рассмотрение дел, связанных с правом на забвение, удовлетворением запросов властей о получении данных, хранящихся в другой юрисдикции, и признанием недействительным соглашения Safe Harbour. Во всех этих случаях юрисдикция выходила за рамки страны или за пределы ЕС.

Европейские суды принимали решения по целому ряду таких дел, что имело существенные последствия:

- Европейские суды все чаще принимают решения по делам, связанным с компаниями США.
- Европейские регуляторы, в частности,а в области защиты данных, играют все более видную роль.
- Международная правовая практика по вопросам, связанным с Интернетом, все чаще определяется европейскими судами.

Принципы определения юрисдикции

Существуют три основных вопроса, имеющих отношение к юрисдикции:

- Какой суд или другой государственный орган имеет необходимые

полномочия (процессуальная юрисдикция)?

- Какие законы должны применяться (материальная юрисдикция)?
- Каким образом исполняются решения суда (исполнительная юрисдикция)?

Для определения юрисдикции в конкретных случаях используются следующие основные принципы:

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

Другим важным принципом, установленным современным международным правом, является принцип универсальной юрисдикции[11]. Принцип универсальной юрисдикции в широком смысле означает право государства преследовать в уголовном порядке определенные типы преступлений, независимо от того, где и кем они были совершены, без обязательной связи с территорией, национальностью или особым государственным интересом[12].

Под универсальную юрисдикцию подпадают такие правонарушения, как пиратство, военные преступления и геноцид. Однако с развитием Интернета число дел, в отношении которых применяется универсальная юрисдикция в соответствии с принципом доступа, стало увеличиваться. Согласно указанному принципу, доступ к Интернету с территории определенной страны является достаточным основанием для признания юрисдикции судов такой страны. Именно из этого исходил французский суд в деле компании Yahoo![13] и суд ЕС при рассмотрении дел eData[14] и Pinckney[15]. Возможность определения юрисдикции на основании такого ограниченного критерия, как доступ к Интернету, связана с определенными проблемами, включая поиск «удобного» суда. Судебное разбирательство, таким образом, может инициировать любая страна, имеющая доступ к Интернету.

Конфликт юрисдикций

Конфликт юрисдикций происходит в том случае, когда на установление юрисдикции по определенному делу претендует сразу несколько государств. Как правило, это происходит в тех случаях, когда конфликт имеет экстерриториальную составляющую (например, в нем участвуют граждане разных государств или задействованы международные транзакции). Юрисдикция устанавливается по одному из следующих принципов: территория, гражданство или действие. Размещая контент или общаясь в Интернете, не всегда можно быть уверенным, что не нарушается законодательство какой-либо страны. В этом смысле почти каждый вид деятельности в Интернете имеет международный аспект, который может приводить к множественным юрисдикциям и так называемому «эффекту переливания»[16].

Юрисдикция и доступ к контенту

Одним из наиболее наглядных и часто упоминаемых судебных разбирательств, иллюстрирующих проблему юрисдикции, является дело Yahoo! 2001 г. во Франции. Дело Yahoo! в очередной раз подчеркнуло значимость проблемы множественной юрисдикции. Причиной судебного разбирательства послужило нарушение веб-сайтом Yahoo! французского законодательства о нацистских реликвиях, запрещающего демонстрацию и продажу материалов подобного содержания. Отметим, что сам веб-сайт был размещен в США, где распространение подобных материалов было и остается законным. По данному делу было принято судебное решение, предписывающее использование технических средств (геолокационного программного обеспечения и фильтрации доступа). Yahoo! обязали распознавать пользователей из Франции и блокировать их доступ к страницам с материалами нацистского содержания[17].

Аналогичным образом, согласно решению по делу о праве на забвение (Google et al. против Mario Costeja Gonzalez et al.) на поисковые системы была возложена обязанность рассматривать запросы об удалении определенных результатов поиска в отношении пользователей из ЕС. В развитие этого решения ряд органов ЕС, отвечающих за защиту персональных данных, приня-

ли соответствующие нормативные документы. Как и в деле против Yahoo!, французские надзорные органы постановили[18], что компания Google обязана удалять результаты поиска по всему миру, а не только в европейских доменных зонах (например, .fr, .es, и .uk).

Юрисдикция и защита данных

В последние годы огромный резонанс получили споры по вопросу о защите персональных данных граждан ЕС при хранении таких данных за пределами Европейского союза. В 2013 г. гражданин Австрии Максимилиан Шремс потребовал, чтобы Комиссар по защите персональных данных Ирландии запретил компании Facebook передавать его персональные данные в США. По мнению Шремса, в США не обеспечивается защита персональных данных на должном уровне, поскольку в стране ведется массовая слежка в соответствии с американским законодательством. Этот запрос был отклонен, после чего Шремс обратился в суд. В конечном счете, дело дошло до Суда Европейского союза, который объявил недействительным соглашение Safe Harbour, которым регулируется передача персональных данных между ЕС и США[19]. В результате, вместо этого соглашения было принято Соглашение о правилах обмена конфиденциальной информацией между ЕС и США.

Подробнее о соглашении Safe Harbour и Соглашении о правилах обмена конфиденциальной информацией между ЕС и США см. ***Раздел 8.***

По итогам разбирательства в отношении защиты персональных данных были приняты следующие меры: во-первых, ряд компаний перенесли свои дата-центры и мощности по обработке данных в юрисдикции с менее жесткими требованиями, в первую очередь в Ирландию. Хотя это и не оградило компании от исков, в решении 2016 г. в отношении компании Microsoft было подтверждено, что получение ордера в США не дает американским властям право доступа к информации, хранящейся в Ирландии[20].

Во-вторых, ряд стран, включая Китай и Россию, приняли законы, согласно которым пользовательские данные должны храниться в пределах национальной территории. Требование хранить данные на серверах, расположенных в пределах страны, стало важной составляющей политики Китая по достижению «киберсуверенитета».

Юрисдикция и пользовательские соглашения

Очень часто в судебных разбирательствах, в частности, в отношении компании Facebook, в центре внимания оказывается пункт из пользовательского соглашения о применимом праве.

Так, широкий резонанс получило дело французского учителя, который опубликовал на Facebook фотографию картины из Музея Орсе с изображением обнаженной натуры, что стало причиной временной блокировки его учетной записи. Апелляционный суд Парижа постановил[21], что истец может судиться с Facebook во Франции, отвергнув довод социальной сети, которая указывала, что в пользовательском соглашении в качестве места рассмотрения спора указан штат Калифорния. После этого решения против Facebook было подано множество исков за пределами США.

В июне 2016 г. израильский суд признал недействительным положение о применимом праве в пользовательском соглашении Facebook, согласно которому все иски рассматриваются судами штата Калифорния, и позволил подавать коллективные иски против компании[22]. При рассмотрении этого дела было заявлено, что Facebook без получения предварительного согласия использовала для подбора рекламы посты, доступные только самим пользователям, нарушив право пользователей на неприкосновенность частной жизни.

Помимо технических решений (геолокация и фильтрование), решить проблему конфликта юрисдикций можно и другими способами, в том числе путем гармонизации правовых систем разных стран и использования альтернативных механизмов урегулирования споров.

Гармонизация правовых систем

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

как киберпреступность. Однако в некоторых областях, включая политику контроля над содержанием материалов Интернета, достижение глобального консенсуса маловероятно, так как культурные противоречия в виртуальном мире еще более непримиримы, чем в реальном[23].

Еще одним возможным следствием недостаточной гармонизации может стать перемещение информационных материалов в страны с низким уровнем регулирования Интернета. По аналогии с морским правом некоторые страны могут стать «удобными флагами» для «офшорных» центров в мире Интернета.

Альтернативные средства решения споров

Вместо использования традиционных судебных процедур можно задействовать альтернативные средства урегулирования споров. К таким методам относятся арбитраж (третейское разбирательство) и процедура примирения сторон. Метод урегулирования споров в Интернете предусматривает использование Интернета и технологий для урегулирования споров.

Применительно к делам, связанным с Интернетом, такие механизмы, в частности, третейский суд, широко используются для заполнения вакуума, вызванного неспособностью существующего международного частного права решать многочисленные дела, связанные с Интернетом. Частным примером такого применения арбитража является Единая политика рассмотрения споров о доменных именах (UDPR), разработанная Всемирной организацией интеллектуальной собственности (ВОИС) и принятая ICANN в качестве основной процедуры разрешения таких споров.

При использовании механизма арбитража решения принимаются одним или несколькими независимыми частными лицами, избранными участниками спора. Механизм третейского разбирательства обычно закрепляется в частном соглашении сторон, которые договариваются в будущем разрешать любые споры с помощью арбитража. Существует много вариантов соглашений об арбитраже, в которых регулируются такие вопросы, как место и процедура проведения арбитража, выбор применимого права и т. д.

В Таблице 2 приводится обзор основных различий между разрешением споров путем судебного и арбитражного разбирательства.

Таблица 2. Различия между судом и арбитражем

Элементы	Суд	Арбитраж (третейский суд)
Организация	Действует в соответствии с национальным законодательством и договорами	Постоянные и временные арбитражные комиссии (создаются сторонами и/или состав определяется сторонами)
Применимое право	Право суда (судья принимает решение о применимом праве)	Участники могут выбирать применимое право; в противном случае, используется применимое право согласно договору; если в договоре нет соответствующих указаний, используются нормы арбитражной инстанции
Процедура	Судебные процедуры определяются законами/договорами	Определяются участниками (ad hoc). Определяются арбитражным органом (постоянные)
Правоприменение	Выполнение решения суда обеспечивают национальные власти	В соответствии с арбитражным соглашением и Нью-йоркской конвенцией

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

Одно из основных преимуществ арбитража состоит в том, что он решает проблему выбора процедурной и материальной юрисдикции. 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[24]. В соответствии с этой конвенцией национальные суды обязаны выполнять арбитражные решения. На основании правового режима Нью-Йоркской конвенции обеспечить выполнение арбитражных решений проще, чем обычных судебных решений.

Основной недостаток урегулирования споров через арбитраж заключается в том, что с его помощью невозможно решать такие вопросы высокой общественной значимости, как нарушения прав человека. Для рассмотрения подобных дел все равно придется обращаться в государственные суды. Существуют и другие ограничения:

- 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, различные формы ответственности, киберпреступность).
- Многие рассматривают существующую практику включения статьи об арбитраже в обычные соглашения как невыгодную для более слабой стороны (обычно это интернет-пользователь или покупатель интернет-магазина).
- Некоторых волнует тот факт, что арбитраж выводит прецедентное право (лежащее в основе правовых систем США и Великобритании) на глобальный уровень, что постепенно приведет к подавлению национальных правовых систем. В случае с регулированием интернет-торговли это может оказаться более приемлемым, принимая во внимание уже существующий высокий уровень унификации материально-правовых норм. Что касается распространения прецедентного права на социокультурные аспекты, такие как содержание материалов Интернета, то здесь требуется более осторожный подход, поскольку национальное законодательство лучше отражает культурные особенности соответствующей страны.

Арбитраж часто используется при разрешении коммерческих споров. Сформировалась основательно проработанная система правил и институтов, направленных на урегулирование коммерческих споров. Основным международным документом является Типовой закон о международном коммерческом арбитраже, который был разработан Комиссией Организации Объединенных Наций по праву международной торговли (UNCITRAL) в 1985 г.[25] Ведущие международные арбитражные организации, как правило, создаются при торговых палатах.

Альтернативные средства урегулирования споров и Интернет

Арбитраж и другие альтернативные системы урегулирования споров широко используются при решении дел, связанных с Интернетом. В качество одного из примеров такого подхода можно привести уже упоминавшуюся Единую политику рассмотрения споров о доменных именах (UDPR). С момента запуска механизма UDPR в декабре 1999 г. Центр ВОИС по арбитражу и посредничеству рассмотрел более 35 тыс. споров в отношении доменных имен[26].

UDPR изначально создавалась как механизм урегулирования конфликтов во всех договорах, связанных с регистрацией родовых доменов верхнего уровня (.com, .edu, .org, .net) и некоторых национальных доменов верхнего уровня. Уникальным является то, что арбитражные решения применяются непосредственно путем внесения изменений в систему доменных имен (снятие доменного имени с делегирования или передача прав на доменное имя заявителю), без участия национальных судов.

В 2016 г. в рамках Европейского союза был создал новый механизм. В феврале 2016 г. начала работу платформа по урегулированию споров в режиме онлайн, цель которой состоит в том, чтобы в онлайновом режиме помогать потребителям и продавцам решать споры в связи с покупками через Интернет внутри страны и в сфере трансграничной торговли[27].

Некоторые интернет-компании, включая Google, Facebook и Twitter, разработали собственные механизмы урегулирования споров. После утверждения Судом ЕС права на забвение, компания Google создала специальный механизм, с помощью которого пользователи могут оформить запрос на удаление определенных сайтов из результатов поиска. С мая 2014 г. по октябрь 2016 г. в адрес Google поступило свыше 575 тыс. заявок такого рода[28].

Появление частных механизмов урегулирования споров породило целый ряд вопросов. Следует ли частным компаниям заниматься решением споров? Какими процедурными и материальными нормами должен регулироваться этот процесс? Как обеспечить доступ к таким механизмам для интернет-пользователей?

Право интеллектуальной собственности

Знания и идеи являются важнейшими ресурсами в глобальной экономике. Защита таких знаний и средств их выражения в форме прав интеллектуальной собственности становится одним из самых важных вопросов управления Интернетом. Право интеллектуальной собственности также находится в центре дискуссий о развитии Интернета. Развитие Интернета повлияло на право интеллектуальной собственности в основном вследствие «оцифровки» знаний и информации, а также появившихся новых возможностей их обработки. Применительно к Интернету защита прав интеллектуальной собственности распространяется на авторские права, товарные знаки и патенты, а также чертежи, модели, коммерческую тайну, географические наименования и сорта растений.

Авторское право

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

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

Интернет создает новые возможности и для обладателей авторских прав, обеспечивая более надежные технические средства защиты и мониторинга

использования материалов. В самом крайнем случае владельцы авторских прав могут вообще запретить доступ к авторским материалам, что сделает саму концепцию авторского права бессмысленной (рис. 17).

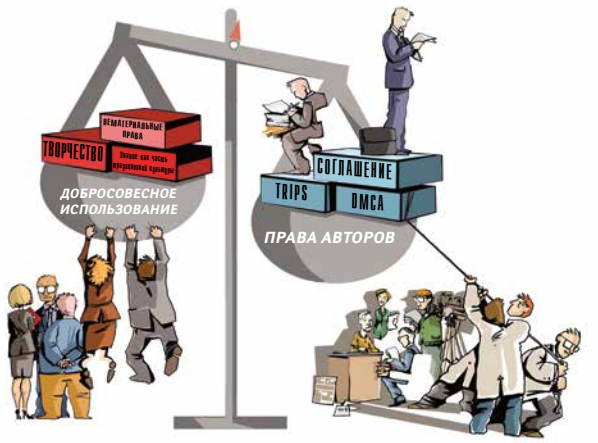


Рисунок 17. Авторские права

На сегодняшний день обладатели авторских прав, чьи интересы представляют крупные записывающие и мультимедийные компании, очень активно защищают свои права. Общественные интересы пока не формулируются достаточно четко и не защищаются в нужной степени. Однако постепенно ситуация выравнивается, в основном с помощью множества глобальных инициатив, направленных на предоставление свободного доступа к знаниям и информации (например, открытые лицензии Creative Commons).

Современное состояние

Усиление защиты авторских прав на национальном и международном уровнях

Компании индустрии звукозаписи и развлечений проводят активную лоббистскую деятельность на национальном и международном уровнях в пользу усиления защиты авторских прав. На международном уровне за-

щита цифровых материалов была включена в Договор о защите авторских прав ВОИС 1996 г.[29] 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. В качестве примера инициативы регионального уровня можно привести положения о правах на интеллектуальную собственность в соглашении о Транстихоокеанском партнерстве, которое было заключено между 12 странами Тихоокеанского региона в феврале 2016 г. Данный документ увеличивает срок авторских прав и ужесточает контроль над их соблюдением[30]. В США защита интеллектуальной собственности была усилена Законом об авторских правах в цифровую эпоху (DMCA)[31] 1998 г.

На национальном и международном уровнях был выдвинут целый ряд предложений по ужесточению контроля в сфере защиты прав интеллектуальной собственности путем предоставления сторонним организациям права осуществлять фильтрацию и мониторинг распространения материалов, защищенных авторским правом. Реакция общественности на такие инициативы была резко отрицательной, и предложения не были осуществлены. В 2011 г. в США были приняты два закона — Закон о противодействии интернет-пиратству (Stop Online Piracy Act — SOPA)[32] и Закон о защите прав на интеллектуальную собственность (PROTECT IP Act — PIPA)[33] с целью создания новых механизмов борьбы с интернет-пиратством, включая блокировку сайтов, нарушающих чьи-либо права, и запрет поисковым системам на отображение таких сайтов в результатах поиска. Однако из-за протестов вступление в силу этих двух законов было отложено на более поздний срок. На международном уровне попыткой решения проблемы защиты прав интеллектуальной собственности стала разработка Антипиратского торгового соглашения (Anti-Counterfeiting Trade Agreement — ACTA)[34], которое бы позволило частным компаниям приводить в исполнение решения в области защиты прав на интеллектуальную собственность и заниматься нормотворчеством в этой области. Но и в этот раз прокатившаяся по Европе волна протеста привела к отклонению ACTA парламентом ЕС.

Попытки ужесточить регулирование неизменно подвергаются жесткой критике со стороны научного сообщества и правозащитников, которые указывают на нарушение прав человека и основных свобод. В протестных выступлениях в виртуальном пространстве и вне сети участвовали и обычные интернет-пользователи[35].

Программное обеспечение против нарушения авторских прав

Нарушители авторских прав могут использовать различные виды программного обеспечения для незаконного распространения музыки и видео в Интернете. Аналогичным образом использовать программные решения могут и те, кто ставит своей целью защиту авторских прав. 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.

Существуют следующие варианты использования программного обеспечения звукозаписывающими и развлекательными компаниями для защиты своих прав:

- программы-«трояны», перенаправляющие пользователей на веб-сайты, где они могут законным образом купить песню, которую пытались загрузить нелегально;
- программное обеспечение, на некоторое время блокирующее компьютер и выводящее на экран предупреждение о скачивании пиратских материалов;
- сканирование жесткого диска с целью удаления обнаруженных пиратских материалов;
- «запрещающее» ПО, блокирующее доступ в Интернет при попытке загрузить пиратские файлы.

Такие меры некоторые считают противозаконными[36]. Вопрос заключается в том, нарушают ли закон компании, использующие такие меры?

Технологии «управления цифровыми правами»

В качестве долговременного и более структурного подхода к решению проблемы бизнес внедряет различные технологии управления доступом к материалам, защищенным авторским правом. Компания Microsoft соз-

дала программное обеспечение для «управления цифровыми правами» с целью регулирования загрузки звуковых файлов, фильмов и других материалов, защищенных авторским правом. Подобные системы были созданы компаниями Xerox (ContentGuard), Philips и Sony (InterTrust).

Использование технологических инструментов для защиты авторских прав получило поддержку как на международном уровне (Договор ВОИС по авторскому праву), так и в Законе об авторских правах в цифровую эпоху (DMCA), принятом в США. Последний, кроме того, придал противозаконный статус попыткам обойти технологическую защиту авторских прав.

Вопросы

Усовершенствовать существующие механизмы защиты авторских прав или создавать новые?

Каким образом следует 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»[37], необходимо произвести самые минимальные перемены, главным образом путем «дематериализации» таких базовых концепций авторского права, как фиксация, распространение, передача и публикация. Этот подход поддержан в основных международных соглашениях в области защиты авторских прав, включая Соглашение по торговым аспектам прав интеллектуальной собственности (TRIPS) и Договор ВОИС по авторскому праву.

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, нужна ли защита авторского права вообще. Необходимо понять также, как будет осуществляться защита общественных интересов — второго неизвестного в уравнении о защите авторских прав.

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

Изначально целью защиты авторского права было поощрение творчества и изобретений. По этой причине в понятие были включены два элемента: защита прав авторов и защита общественных интересов. Основная сложность заключалась в том, что нужно было предусмотреть возможность для широкой аудитории обращаться к материалам, защищенным авторским правом, в интересах поощрения творчества, получения знаний и обеспечения всеобщего благосостояния. С точки зрения функционирования этого механизма, общественные интересы защищались с помощью концепции «добросовестного использования» защищенных материалов[38].

Защита авторских прав и развитие

От ужесточения требований в области защиты авторских прав диспропорционально страдают развивающиеся страны. Интернет предоставляет исследователям, студентам и другим пользователям, особенно из развивающихся стран, мощный инструмент для участия в глобальном научном обмене. Ограничительный режим защиты авторских прав может вызвать негативные последствия для потенциала развивающихся стран. Другой аспект — рост масштабов оцифровывания предметов культуры и искусства развивающихся стран. Как ни парадоксально, развивающимся странам, в конце концов, возможно, придется платить за свое культурное и художественное наследие, когда оно будет оцифровано, помещено в новую «упаковку» и станет собственностью иностранных развлекательных и медиакомпаний.

ВОИС и ВТО

Существуют два основных международных режима защиты прав интеллектуальной собственности (ИС). Всемирная организация интеллектуальной собственности (ВОИС) координирует режим защиты ИС в соответствии с Бернской и Парижской конвенциями. Другой режим координируется Всемирной торговой организацией (ВТО) и основывается на Соглашении

по торговым аспектам прав интеллектуальной собственности (TRIPS). Координация вопросов интеллектуальной собственности на международном уровне была передана от ВОИС к ВТО с целью усиления защиты ИС, особенно с точки зрения правоприменения.

Эти изменения стали предметом обеспокоенности для ряда развивающихся стран. Строгие правоприменительные механизмы, существующие в рамках ВТО, могут ограничить пространство для маневров, имеющееся у развивающихся стран, и возможности нахождения равновесия между потребностями развития и защитой международных прав интеллектуальной собственности. До сих пор в центре внимания ВТО и TRIPS были различные толкования прав интеллектуальной собственности в отношении фармацевтических товаров. Весьма вероятно, что в будущем темой дискуссий станет интеллектуальная собственность и Интернет.

Товарные знаки

Товарным знаком называется символ или слово (-а), которые законно зарегистрированы в качестве обозначения компании или товара или признаны таковыми в силу их использования. С точки зрения защиты торговых марок, главной проблемой является регулирование регистрации доменных имен. На ранних стадиях развития Интернета доменное имя предоставлялось тому, кто первым подал на него заявку. Это привело к практике так называемого киберсквоттинга, то есть регистрации названий компаний в качестве доменных имен и их последующей перепродаже по более высокой цене.

Подобная ситуация заставила представителей бизнеса сделать вопрос о защите товарных знаков центральным в реформе управления Интернетом, что привело к созданию в 1998 г. Корпорации по присвоению имен и номеров в Интернете (ICANN). В «Белой книге об управлении названиями и адресами в Интернете» правительство США поставило перед организацией задачу разработать и применять механизм защиты торговых марок в области доменных имен[39]. Вскоре после своего создания ICANN представила Единую политику рассмотрения споров о доменных именах (UDPR), разработанную

Всемирной организацией интеллектуальной собственности[40].

Проблема защиты товарных знаков приобрела особое значение с появлением новых родовых доменов верхнего уровня, таких как .doctor, .lawyer, .berlin и так далее. В качестве примера можно привести создание домена верхнего уровня .amazon. Заявку на регистрацию такого доменного имени подала компания Amazon, будучи владельцем одноименного товарного знака. Однако страны бассейна реки Амазонки опротестовали регистрацию в рамках Правительственного консультативного комитета (GAC) ICANN, заявив, что такое название связано с географической областью, которая имеет большое значение для региона, в связи с чем компания Amazon не должна претендовать на какие-либо исключительные права в отношении данного наименования. Прислушавшись к рекомендации Правительственного консультативного комитета, Совет директоров ICANN в мае 2014 г. отклонил заявку, однако компания Amazon оспорила это решение, воспользовавшись механизмом независимой проверки (IRP). По состоянию на октябрь 2016 г. точка в этом деле поставлена не была, поскольку процесс IRP продолжался, а слушания по делу должны были состояться в феврале–марте 2017 г. [41]

Патенты

Патент обеспечивает его обладателю исключительное право лишить других возможности создавать, использовать или продавать изобретение. В традиционном понимании патент защищает новый процесс или продукт, главным образом в технической или производственной сфере. Лишь недавно стали выдавать патенты на программное обеспечение.

По мере развития интернет-технологий все больше и больше компаний стали регистрировать патенты на различные решения в области интернет-телефонии, Интернета вещей и т. п. Особо отчетливо эта тенденция прослеживается в США, где вместе с числом зарегистрированных патентов растет и количество судебных разбирательств между компаниями на огромные суммы. Например, в сентябре 2016 г. судья штата Техас вынес решение по делу, длившемуся с 2010 г., и обязал компанию Apple выплатить другой ame-

риканской компании 302,4 млн. долларов за нарушение патентов на решения в области безопасности компьютерной и мобильной связи[42].

Среди патентов, зарегистрированных для защиты бизнес-процессов, некоторые были довольно спорными; например, требование компании British Telecom о выплате ей лицензионных вознаграждений по патенту на гипертекстовые ссылки, зарегистрированному в 1980 г. В августе 2002 г. иск был отклонен[43]. Если бы British Telecom удалось выиграть это дело, то пользователям Интернета пришлось бы платить за каждый переход по ссылке.

Выдача патентов в Европе и других регионах представляет собой довольно сложный процесс. Как говорится в разъяснениях Европейского патентного ведомства, «в соответствии с Европейским патентным соглашением компьютерная программа сама по себе не может считаться изобретением, права на которое можно защитить с помощью патента [...]. Чтобы выдать патент на компьютеризованное изобретение, требуется создание инновационного и неочевидного технического решения»[44].

Трудовое законодательство

С развитием Интернета изменилось то, как мы работаем: выросла актуальность надомной работы, а также число временных и краткосрочных видов занятости. Появился термин «постоянно временный» для обозначения сотрудников, которых постоянно держат на краткосрочных, но регулярно обновляемых контрактах. Это приводит к снижению уровня социальной защищенности работников (рис. 18).

В последнее время интернет-компании, в том числе Uber и Amazon, начали применять новые модели организации трудовой деятельности, в частности «по запросу» и в качестве независимого работника. Появление новых моделей ставит перед обществом ряд вопросов. В частности, каков статус водителей Uber — являются они сотрудниками компании или независимыми подрядчиками? В зависимости от штата ответ на этот вопрос варьируется. Так, власти штатов Калифорния[45] и Орегон[46] считают водителей сотрудниками Uber, тогда как во Флориде[47] они признаются подрядчиками.

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)? Правовая практика постепенно формируется и в этой области.

Рисунок 18. Трудовое законодательство

В 2007 г. Европейский суд по правам человека (ЕСПЧ) заявил, что отслеживание того, как сотрудник пользуется электронной почтой или Интернетом на рабочем месте, является нарушением прав такого сотрудника[48]. Однако в 2016 г. тот же суд постановил, что работодатели вправе просматривать сообщения сотрудников, написанные в рабочее время. В решении по делу Барбулеску против Румынии (январь 2016 г.) суд отметил, что считает вполне естественным желание работодателя проверить, выполняют ли сотрудники в рабочее время свои профессиональные обязанности. Однако работодатель обязан уведомлять своих сотрудников об этом заранее. В судах Дании рассматривалось дело об увольнении сотрудника за отправку личных писем по электронной почте и просмотр

чатов сексуальной направленности. Суд счел увольнение незаконным, поскольку в данной организации не было правил пользования Интернетом, где был бы прописан запрет на использование Интернета в нерабочих целях. В решении ЕСПЧ по делу Барбулеску против Румынии также подчеркивается важность документа, который официально регулирует пользование Интернетом в организации: «Должны быть приняты правила, охватывающие все аспекты использования Интернета на работе, включая конкретные инструкции по использованию электронной почты, мгновенных сообщений, социальных сетей, блогов и интернет-навигации. Такие правила могут быть разработаны с учетом потребностей той или иной организации или ее подразделений, но, в любом случае, содержать права и обязательства сотрудников, изложенные предельно четко и ясно, чтобы было понятно, как можно использовать Интернет и как контролируется такая деятельность, как обеспечивается информационная безопасность, каким образом используются и удаляются данные, и кто имеет к ним доступ»[49].

С развитием социальных сетей особую актуальность приобретает проблема разграничения частной и профессиональной жизни сотрудника. Из ряда недавних дел[50] следует, что поведение сотрудника и его комментарии в социальных сетях по разным темам, от рабочих условий и характеристики коллег до стратегии и продуктов работодателя, могут считаться его личным мнением, но при этом иметь существенное влияние на имидж и репутацию компании и ее сотрудников.

Трудовое законодательство традиционно относится к внутригосударственной сфере. Однако глобализация и развитие Интернета привели к интернационализации вопросов, связанных с трудовым законодательством. Принимая во внимание рост количества людей, работающих в иностранных организациях и осуществляющих взаимодействие на международном уровне, следует признать, что назрела необходимость создания адекватных международных механизмов регулирования. Этот аспект был признан в Декларации WSIS, которая в §47 призывает к уважению соответствующих международных норм на рынке труда, связанного с информационно-коммуникационными технологиями[51].

Посредники

Посредники[52] играют ключевую роль в обеспечении работы Интернета. К ним относятся интернет-провайдеры (которые предоставляют услуги доступа к Интернету для конечных пользователей), а также поставщики услуг хостинга, поисковые системы и социальные сети.

Учитывая характер деятельности посредников, оказывающих услуги по передаче сетевого контента и доступу к нему, не удивительно, что они все чаще привлекаются к работе по обеспечению соблюдения требований закона в сфере авторских прав, борьбы со спамом и осуществления права на забвение. Соответственно, возникает вопрос, несут ли посредники ответственность (и должны ли они нести ответственность) за размещенные в сети материалы, если они содействуют доступу к такому контенту?

На национальном уровне, наиболее простой путь гарантировать соблюдение закона в сети — это сотрудничество государственных и правоохранительных органов с интернет-провайдерами.

Как правило, ресурсы, на которых размещаются материалы, поисковые системы и социальные сети выполняют функцию проводника или моста между материалами и интернет-пользователями. Такие ресурсы обычно размещаются в одной стране (иногда у таких компаний бывают представительства в различных регионах), однако имеют глобальный охват и привлекают пользователей со всего мира. Таким образом, они нередко действуют сразу в юрисдикциях нескольких стран.

Вопрос ответственности посредников постоянно обсуждается на Форуме по управлению Интернетом и других площадках. Среди 14 принципов ОЭСР по регулированию Интернета упоминаются посредники[53], а в рамках Совета Европы создан Комитет экспертов по интернет-посредникам (MSI-NET), в задачи которого входит подготовка предложений, касающихся функций и обязанностей посредников. В материалах ЮНЕСКО также поднимается вопрос о роли интернет-посредников в отношениях между авторами и интернет-пользователями, а также обеспечении свободы выражения мнений и соблюдения основных прав, включая неприкосновенность частной жизни[54].

Вопросы

Несут ли посредники ответственность за нарушения прав человека?

Как правило, в правовых нормах, которые регулируют вопрос ответственности посредников, содержится принцип, согласно которому интернет-посредник не несет ответственности за размещение материалов, содержащих нарушения авторских прав, при условии, что такому посреднику неизвестно о нарушении. Именно такой подход закреплен в DMCA и директивах ЕС[55], которые освобождают поставщика услуг от ответственности за передачу и хранение информации по указанию пользователей.

Основное различие между правовыми системами заключается в правовых действиях, которые предпринимаются после того, как посредник осознает, что размещенные на его ресурсах материалы нарушают чьи-то авторские права. Согласно требованиям законодательства США и ЕС, поставщики услуг обязаны действовать в соответствии с процедурой «Предупреждение и удаление», то есть удалить материалы после получения соответствующего уведомления[56]. Более сбалансированный подход действует в Японии, где перед удалением материала пользователь вправе обжаловать такое решение. Оба решения достаточно выгодны для посредников. В то же время, они вынуждены оценивать спорные материалы[57]. Кроме того, такие подходы не являются окончательным решением проблемы, поскольку материалы могут быть просто перенесены на другие ресурсы.

В целом, принцип ограничения ответственности посредников закрепился в правовой практике. В качестве примеров наиболее резонансных дел, в которых интернет-провайдеры были освобождены от ответственности за размещение на своих серверах материалов, содержащих нарушения авторского права, можно привести дело Церкви сайентологии (Голландия)[58], дело RIAA против Verizon (США)[59], SOCAN против CAIP (Канада)[60] и Scarlet против SABAM (Бельгия)[61]. В решении от сентября 2016 г. по делу S Media BV против Sanoma Media Netherlands BV и другие Суд ЕС избрал более утонченный подход, заявив, что операторы сайтов, на которых содержатся ссылки на материалы, содержащие нарушения авторских прав, могут быть признаны виновными в нарушении авторских прав при условии, что такие операторы знали или имели основания полагать, что в материалах содержатся нарушения. По мнению суда, может быть сочтено, что оператор осведомлен о нарушениях, если ссылки предоставляются «с целью получения финансовой выгоды»[62].

В последние годы на посредников оказывается все больше давления в вопросе нарушения авторских прав, поскольку они выполняют функцию промежуточного звена между конечными пользователями и материалами, и поэтому могут наиболее эффективно контролировать доступ. Именно такие доводы легли в основу закона Hadopi[63] во Франции, согласно которому интернет-провайдеры обязаны предпринимать превентивные меры в случае возникновения подозрений в нарушении авторских прав.

Роль посредников в регулировании содержания интернет-материалов

Под давлением властей интернет-провайдеры, поставщики услуг хостинга, операторы систем поиска и социальных сетей постепенно были вынуждены, без особого энтузиазма, приступить к работе по регулированию контента (например, клеветнического или мошеннического характера). Для таких компаний существует два пути: они могут обеспечивать исполнение закона либо осуществлять саморегулирование, то есть самостоятельно устанавливать критерии оценки материалов. В последнем случае есть риск передачи функций по контролю над содержанием материалов в частные руки, то есть от органов власти к посредникам. Но есть и преимущество: более гибкий подход в условиях быстрого развития технологий, что может сыграть важную роль в деле защиты детей в Интернете.

Суды все чаще выносят решения, которые заставляют посредников перейти в нормативно-правовое поле. В 2013 г. ЕСПЧ оставил в силе решение эстонского суда, согласно которому ответственность за размещение на портале Delfi оскорбительных комментариев была возложена на сайт[64]. В июне 2015 г. Большая палата ЕСПЧ подтвердила действительность решения 2013 г.: ЕСПЧ счел вердикт эстонского суда справедливым и соразмерным, поскольку оспариваемые комментарии носили чрезмерный характер и были размещены на сайте в ответ на статью, которая была размещена Delfi на профессиональном информационном портале, работающем на коммерческой основе[65] (при этом решение не затрагивает другие интернет-ресурсы,

на которых могут распространяться комментарии третьих лиц, включая интернет-форумы, доски объявлений и социальные сети).

Роль посредников в борьбе со спамом

Обычно считается, что интернет-провайдеры находятся на передовой борьбы со спамом. Они часто самостоятельно борются со спамом с помощью технических фильтров или различных программ по борьбе со спамом. В докладе МСЭ 2006 г. говорится, что интернет-провайдеры должны нести ответственность за спам, в связи с чем был предложен кодекс поведения по борьбе со спамом, в котором содержалось два основных положения:

- Интернет-провайдеры обязаны запретить своим пользователям заниматься рассылкой спама.
- Интернет-провайдеру запрещается сотрудничать с интернет-провайдерами, которые не следуют такому кодексу поведения[66].

Из-за проблемы спама интернет-провайдеры столкнулись с новыми трудностями. Например, использование компанией спам-фильтра привело к подаче против нее иска, поскольку наравне со спамом блокировались и обычные сообщения, что доставляло неудобства пользователям[67]. Можно сказать, что сочетание в работе интернет-провайдеров саморегулирования и исполнения требований властей, вкупе с международным сотрудничеством и использованием сложных фильтров, сделали проблему спама менее актуальной.

Примечания к разделу 4

[1] Одним из первых сторонников реального права был судья Фрэнк Истербрук, которому приписывают слова: «Успокойтесь, киберправа не существует!». В статье «Киберпространство и лошадиное право» он заявил, что лошадиного права, несмотря на значимую роль лошадей, как отдельной отрасли, никогда не существовало. Судья Истербрук утверждает, что необходимо сосредоточиться на базовых юридических инструментах, таких как контракты, обязательства и т. п. Адрес в Интернете: http://chicagounbound.uchicago.edu/cgi/viewcontent.cgi?article=2147&context=journal_articles [просмотрено 5 августа 2018 г.]. Аргументы судьи Фрэнка Истербрука имели широкий резонанс, в том числе в спор вступил Лоренс Лессиг. См.: Lawrence Lessig. The Law of the Horse: What Cyberlaw Might Teach. Адрес в Интернете: http://cyber.law.harvard.edu/works/lessig/LNC_Q_D2.PDF [просмотрено 5 августа 2018 г.]. Подробнее об использовании реального права и киберправа см. блог The Oxford Comma, Shaping Internet Governance: Tensions Between 'Real' and 'Cyber' Laws. Адрес в Интернете: http://wizardsqu1rrel.blogspot.com/2014/01/shaping-internet-governance-tensions.html [просмотрено 5 августа 2018 г.].

[2] United Nations (2013) Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security. Адрес в Интернете: http://www.unidir.org/files/medias/pdfs/developments-in-the-field-of-information-and-telecommunications-in-the-context-of-international-security-2012-2013-a-68-98-eng-0-578.pdf [просмотрено 5 августа 2018 г.].

[3] United Nations General Assembly (2015) Resolution A/70/125. Outcome document of the high-level meeting of the General Assembly on the overall review of the implementation of the outcomes of the World Summit on the Information Society. Адрес в Интернете: http://workspace.unpan.org/sites/Internet/Documents/UNPAN96078.pdf [просмотрено 5 августа 2018 г.].

[4] United Nations General Assembly (2014) Resolution A/69/166. The right to privacy in the digital age. Адрес в Интернете: http://www.un.org/en/ga/search/view_doc.asp?symbol=A/RES/69/166 [просмотрено 5 августа 2018 г.].

United Nations Human Rights Council. Resolution A/HRC/20/L.13. The promotion, protection and enjoyment of human rights on the Internet. Адрес в Интернете: http://ap.ohchr.org/documents/alldocs.aspx?doc_id=20280 [просмотрено 5 августа 2018 г.].

[5] NTIA (1988) Statement of Policy on the Management of Internet Names and Addresses. Адрес в Интернете: https://www.ntia.doc.gov/federal-register-notice/1998/statement-policy-management-internet-names-and-addresses [просмотрено 5 августа 2018 г.].

[6] Например, согласно одному из новых положений, регламент применим к «тем эксплуатационным организациям, которые уполномочены государством-членом или признаны им в качестве таковых для организации и обеспечения услуг международной электросвязи и предоставления их населению». Считается, что с введением этого положения интернет-провайдеры оказались в сфере действия РМЭ. Споры также вызвало введение положения по вопросам сетевой безопасности и нежелательных электронных сообщений. Поскольку эти вопросы связаны с более общим понятием кибербезопасности (в том числе в контексте проблемы рассылки спама по электронной почте), некоторые утверждали, что эти положения не могут распространяться только на традиционные средства электросвязи, но не на Интернет. Помимо существования разных интерпретаций таких положений, некоторые считают, что само определение электросвязи (не менялось по сравнению с РМЭ 1988 г.) охватывает Интернет, поскольку в определении сказано: «Электросвязь: Любая передача, излучение или прием знаков, сигналов, письменного текста, изображений и звуков или сообщений любого рода по проводной, радио, оптической или другим электромагнитным системам».

[7] Ago R (1956) Science juridique et droit international. Receuil des Cours Academie de Droit International (RCADI), 1956-II, 855—954, La Haye

[8] Vienna Convention on the Law of Treaties. Адрес в Интернете: http://www.ilsa.org/jessup/jessup11/basicmats/VCLT.pdf [просмотрено 5 августа 2018 г.].

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

[10] Salis RP (2001) A Summary of the American Bar Association's (ABA) Jurisdiction in Cyber-space Project: Achieving Legal and Business Order in Cyberspace: A Report on Global Jurisdiction Issues Created by the Internet. Адрес в Интернете: http://www.jstor.org/discover/10.2307/40687955?uid=3738216&uid=2&uid=4&sid=21103388060741 [просмотрено 5 августа 2018 г.].

[11] К наиболее важным ресурсам в этой области относятся «Принстонские принципы универсальной юрисдикции» (Princeton Principles on Universal

Jurisdiction) 2001 г. Адрес в Интернете: http://www1.umn.edu/humanrts/instree/princeton.html [просмотрено 5 августа 2018 г.].

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

[13] EDRI-gram (2006) French anti-hate groups win case against Yahoo! Адрес в Интернете: https://edri.org/edrigramnumber4-1yahoocase/ [просмотрено 5 августа 2018 г.].

[14] CJEU (2011) Judgement of the Court in Joined Cases Cases C-509/09 and C-161/10: eDate Advertising GmbH v X, and Olivier Martinez, Robert Martinez v MGN Limited. Адрес в Интернете: http://curia.europa.eu/juris/liste.jsf?language=en&jur=C,T,F&num=C-509/09&td=ALL [просмотрено 5 августа 2018 г.].

[15] CJEU (2013) Judgement of the Court in Case C-170/12: Peter Pinckneyv KDG Mediatech AG. Адрес в Интернете: http://curia.europa.eu/juris/liste.jsf?language=en&jur=C,T,F&num=C-170/12&td=ALL [просмотрено 5 августа 2018 г.].

[16] Обзор судебных дел с экстратерриториальной юрисдикцией, имеющих отношение к содержанию материалов Интернета, см.: Timofeeva YA (2005) Worldwide Prescriptive Jurisdiction in Internet Content Controversies: A Comparative Analysis. Connecticut Journal of International Law, 20, 199. Адрес в Интернете: http://ssrn.com/abstract=637961 [просмотрено 5 августа 2018 г.].

[17] Схожее дело рассматривалось Федеральным судом Германии в отношении бывшего гражданина Германии Фредрика Тобена, который получил гражданство Австралии. Он разместил на сайте, расположенном в Австралии, материалы, оспаривавшие реальность Холокоста. Адрес в Интернете: http://www.ihr.org/jhr/v18/v18n4p-2_Toben.html [просмотрено 5 августа 2018 г.].

[18] Commission Nationale de l'Informatique et des Libertés (2015) Right to delisting: Google infor-mal appeal rejected. Адрес в Интернете: https://www.cnil.fr/fr/node/15814 [просмотрено 5 августа 2018 г.].

[19] CJEU (2015) Judgement of the Court in Case C-362/14: Maximillian Schremsv Data Protection Commissioner. Адрес в Интернете: http://curia.europa.eu/juris/document/document.jsf?text=&docid=169195&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=2015 [просмотрено 5 августа 2018 г.].

[20] United States Court of Appeals for the Second Circuit (2016) Decision in the matter of a warrant to search a certain e-mail account controlled and maintained by Microsoft Corporation: Microsoft Corporation v USA. Адрес в Интернете: http://www.ediscoverylaw.com/wp-content/uploads/2016/07/In-re-Matter-of-a-Warrant.pdf [просмотрено 6 августа 2018 г.].

[21] С судебным решением на французском языке можно ознакомиться по адресу: https://www.cottineau.net/wp-content/uploads/2016/02/facebook-jugement-cour-appel-paris-12-fevrier-2016.pdf [просмотрено 6 августа 2018 г.].

[22] Yaron O. Israeli judge approves $400 million class action against Facebook for violating privacy// Haaretz, 17.06.2016. Адрес в Интернете: http://www.haaretz.com/israel-news/business/1.725512 [просмотрено 6 августа 2018 г.].

[23] В качестве примеров спорных вопросов можно привести расистские материалы, порнографию, азартные игры в Интернете, рекламу табачных изделий и продажу наркотиков.

[24] UNCITRAL (1958) The New York Convention. Адрес в Интернете: http://www.uncitral.org/uncitral/en/uncitral_texts/arbitration/NYConvention.html [просмотрено 6 августа 2018 г.].

[25] UNCITRAL (1985) Model Law in International Commercial Arbitration. Адрес в Интернете: http://www.uncitral.org/uncitral/en/uncitral_texts/arbitration/1985Model_arbitration.html [просмотрено 6 августа 2018 г.].

[26] WIPO (no date) Domain Name Dispute Resolution. Адрес в Интернете: http://www.wipo.int/amc/en/domains/ [просмотрено 6 августа 2018 г.].

[27] European Commission (2016) Settling consumer disputes online. Адрес в Интернете: http://ec.europa.eu/consumers/solving_consumer_disputes/docs/adrodr.factsheet_web.pdf [просмотрено 6 августа 2018 г.].

[28] Google (2016) Transparency Report. European privacy requests for search removals. Адрес в Интернете: https://transparencyreport.google.com/eu-privacy/overview [просмотрено 6 августа 2018 г.].

[29] WIPO (no date) WIPO Copyright Treaty. Адрес в Интернете: http://www.wipo.int/treaties/en/ip/wct/ [просмотрено 6 августа 2018 г.].

[30] Office of the United States Trade Representative (no date) The Trans-Pacific Partnership. Адрес в Интернете: https://ustr.gov/trade-agreements/free-trade-agreements/trans-pacific-partnership[просмотрено 6 августа 2018 г.].

[31] US Congress (1998) Digital Millennium Copyright Act. Адрес в Интернете: http://www.copyright.gov/legislation/hr2281.pdf [просмотрено 6 августа 2018 г.].

[32] US Congress (2011) Stop Online Piracy Act. Адрес в Интернете: https://www.congress.gov/bill/112th-congress/house-bill/3261 [просмотрено 6 августа 2018 г.].

[33] US Congress (2011) Protect IP Act. Адрес в Интернете: https://www.congress.gov/bill/112th-congress/senate-bill/968 [просмотрено 6 августа 2018 г.].

[34] Anti-Counterfeiting Trade Agreement (2011) Адрес в Интернете: http://trade.ec.europa.eu/doclib/docs/2011/may/tradoc_147937.pdf [просмотрено 6 августа 2018 г.].

[35] Активное участие в дебатах о законе Hadopi во Франции и выступлениях против ACTA принимала правозащитная организация La Quadrature du Net. Адрес в Интернете: http://www.laquadrature.net/en/ACTA [просмотрено 25 октября 2016 г.]. По вопросу о протестах против законодательных инициатив в США см.: Vijayan J. Protests against SOPA, PIPA go viral // Computerworld, 18.01.2012. Адрес в Интернете: http://www.computerworld.com.au/article/412655/protests_against_sopa_pipa_go_viral/ [просмотрено 6 августа 2018 г.].

[36] Sorkin AR. Software bullet is sought to kill musical piracy // New York Times, 04.05.2003. Адрес в Интернете: http://www.nytimes.com/2003/05/04/business/04MUSI.html [просмотрено 6 августа 2018 г.].

[37] US Patents and Trademark Office (no date) Intellectual Property and the National Information Infrastructure. Адрес в Интернете: http://groups.csail.mit.edu/mac/classes/6.805/articles/int-prop/nii-report-sept95.txt [просмотрено 6 августа 2018 г.].

[38] Подробнее о концепции добросовестного использования с примерами см.: The UK Copyright Service (no date) Copyright Law fact sheet P-09: Understanding Fair Use. Адрес в Интернете: https://www.copyrightservice.co.uk/copyright/p09_fair_use [просмотрено 6 августа 2018 г.].

[39] NTIA (1998) Statement of Policy on the Management of Internet Names and Addresses. Адрес в Интернете: https://www.ntia.doc.gov/federal-register-notice/1998/statement-policy-management-internet-names-and-addresses [просмотрено 6 августа 2018 г.].

[40] Комплексный обзор вопросов, связанных с UDRP, см. в WIPO (2011) WIPO Overview of WIPO Panel Views on Selected UDRP Questions, Second Edition (WIPO Overview 2.0) Адрес в Интернете: http://www.wipo.int/amc/en/domains/search/overview2.0/ [просмотрено 6 августа 2018 г.].

[41] Подробнее о деле вокруг регистрации доменного имени .amazon см.: Murphy K. Amazon files appeal on rejected .amazon domain // The Register, 03.03.2016. Адрес в Интернете: http://domainincite.com/20105-amazon-files-appeal-onrejected-amazon-domain [просмотрено 6 августа 2018 г.]. Подробнее об инициированной компанией Amazon процедуре IRP см.: ICANN (no date) Amazon EU S.à.r.l. v ICANN (.AMAZON). Адрес в Интернете: https://www.icann.org/resources/pages/irp-amazon-v-icann-2016-03-04-en [просмотрено 6 августа 2018 г.].

[42] Decker S, Robertson D. VirnetX Wins $302.4 Million Trial Against Apple in Texas // Bloomberg, 30.09.2016. Адрес в Интернете: https://www.bloomberg.com/news/articles/2016-10-01/virnetx-wins-302-4-million-trial-against-apple-in-texas [просмотрено 6 августа 2018 г.].

[43] Loney M. Hyperlink patent case fails to click // CNET, 23.08.2002. Адрес в Интернете: https://www.cnet.com/news/hyperlink-patent-case-fails-to-click/ [просмотрено 6 августа 2018 г.].

[44] European Patent Office (no date) Patents for software? European law and practice. Адрес в Интернете: https://www.epo.org/news-issues/issues/software.html [просмотрено 6 августа 2018 г.].

[45] Somerville H. Former Uber driver was an employee, rules California department // Reuters, 09.09.2015. Адрес в Интернете: http://www.reuters.com/article/ubertech-california-ruling-idUSL1N11F1KT20150910 [просмотрено 6 августа 2018 г.].

[46] Bureau of Labour and Industries of the State of Oregon (2016) Advisory opinion of the Commissioner of the Bureau of Labor and Industries regarding the employment status of Uber drivers. Адрес в Интернете: http://media.oregonlive.com/commuting/other/101415 Advisory Opinion on the Employment Status of Uber Drivers.pdf [просмотрено 6 августа 2018 г.].

[47] Ampel C. Florida: Uber drivers are contractors, not employees // Daily Business Review, 04.12.2015. Адрес в Интернете: http://www.dailybusinessreview.com/id=1202743938454/Florida-Uber-Drivers-Are-Contractors-Not-Employees?slreturn=20160929162026 [просмотрено 6 августа 2018 г.].

[48] ECHR (2007) Judgement of the Court in the Case Copland v the United Kingdom (Application no. 62617/00). Адрес в Интернете: http://hudoc.echr.coe.int/eng?i=001-79996 [просмотрено 6 августа 2018 г.].

[49] ECHR (2016) Judgement of the Court in the Case Bărbulescu v Romania (Application no. 61496/08). Адрес в Интернете: http://hudoc.echr.coe.int/eng?i=001-159906 [просмотрено 6 августа 2018 г.].

[50] См. примеры в следующих статьях: Holding R. Can You Be Fired for Bad-Mouthing Your Boss on Facebook? // Time U.S., 04.03.2011. Адрес в Интернете: http://www.time.com/time/nation/arti-cle/0,8599,2055927,00.html [просмотрено 6 августа 2018 г.]. Broughton A et al. (2009) Workplaces and Social Networking. The Implications for Employment Relations. Адрес в Интернете: http://www.acas.org.uk/media/pdf/d/6/1111_Workplaces_and_Social_Networking.pdf [просмотрено 6 августа 2018 г.].

[51] WSIS (2003) Declaration of Principles. Building the Information Society: a global challenge in the new Millennium. Адрес в Интернете: http://www.itu.int/net/wsis/docs/geneva/official/dop.html [просмотрено 6 августа 2018 г.].

[52] Принятие ОЭСР определения понятия «посредник» является попыткой обозначить категории поставщиков услуг, которые могут быть отнесены к этой категории: «Интернет-посредники проводят или содействуют проведению транзакций между третьими лицами в Интернете. Они обеспечивают доступ к материалам, товарам и услугам третьих лиц в Интернете, осуществляют их хостинг, передачу и индексирование и оказывают интернет-услуги третьим лицам». См.: OECD (2011) The Role of Internet Interme¬diaries in Advancing Public Policy Objectives. Адрес в Интернете: http://www.oecd.org/sti/ieconomy/theroleofinternetintermediariesinadvancingpublicpolicyobjectives.htm [просмотрено 6 августа 2018 г.].

[53] OECD (2011) OECD Council Recommendation on Principles for Internet Policy Making. Адрес в Интернете: http://www.oecd.org/internet/ieconomy/49258588.pdf [просмотрено 6 августа 2018 г.].

[54] MacKinnon R et al. (2014) Fostering Freedom Online. The Role of Internet Intermediaries. UN-ESCO/Internet Society. Адрес в Интернете: http://unesdoc.unesco.org/images/0023/002311/231162e.pdf [просмотрено 6 августа 2018 г.].

[55] European Union (2000) Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce). Адрес в Интернете: http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=celex:32000L0031 [просмотрено 6 августа 2018 г.]. European Union (2001) Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society. Адрес в Интернете: http://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1477400249287&uri=CELEX:32001L0029 [просмотрено 6 августа 2018 г.].

[56] Под процедурой «Предупреждение и удаление» понимается обязательство поставщиков услуг удалять материалы с сайтов, которыми они управляют, в случае получения уведомления или претензии в отношении законности определенных материалов.

[57] Опасаясь судебного преследования, некоторые интернет-провайдеры предпочитают ограничивать доступ к определенным материалам, даже если нарушений не было. Подробнее см. разборы таких дел в Европе (Голландия): Nas S (2004) The Multatuli Project ISP Notice & Take Down, Bits of Freedom. Адрес в Интернете: https://www-old.bof.nl/docs/researchpaperSANE.pdf [просмотрено 6 августа 2018 г.]. США: Urban J and Quilter L (2006) Efficient Process or 'Chilling Effects'? Takedown Notices Under Section 512 of the Digital Millennium Copyright Act. Адрес в Интернете: https://scholarship.law.berkeley.edu/cgi/viewcontent.cgi?referer=&httpsredir=1&article=1500&context=facpubs [просмотрено 6 августа 2018 г.].

[58] Апелляционный суд не поддержал иск о нарушении авторских прав, поданный Церковью сайентологии против голландского писателя и ее интернет-провайдера XS4ALL. Писатель, которая некогда была членом церкви сайентологии, разместила на одном сайте конфиденциальные документы церкви, что привело к подаче церковью иска в соответствии с Законом о защите авторских прав 1912 г. В 1999 г. Окружной суд поддержал ответчика, заявив о необходимости соблюдения свободы слова. Однако в том же решении говорилось, что интернет-провайдер должен нести ответственность за размещенные материалы, если в них нарушаются авторские права. Апелляционный суд поддержал первое решение, но отменил второе, заявив, что интернет-провайдеры не несут ответственности за размещенные при их участии материалы. Подробнее см.: Gelman L (2003) Church of Scientology Loses Copyright Infringement Case in Dutch Court. Адрес в Интернете: http://cyberlaw.stanford.edu/packets001638.shtml [просмотрено 6 августа 2018 г.].

[59] Подробнее об этом деле см.: Electronic Privacy Information Center (2004) RIAA v Verizon. Адрес в Интернете: http://epic.org/privacy/copyright/verizon/ [просмотрено 6 августа 2018 г.].

[60] Верховный суд Канады отверг доводы Общества композиторов, сочинителей и звукозаписывающих компаний Канады, которые утверждали, что интернет-провайдеры должны выплачивать авторские отчисления, поскольку некоторые из их клиентов скачивают материалы, защищенные авторским правом (SOCAN против CAIP). Адрес в Интернете: http://www.canlii.org/en/ca/scc/doc/2004/2004scc45/2004scc45.html [просмотрено 6 августа 2018 г.].

[61] Бельгийское общество сочинителей, композиторов и издателей (SABAM) требовало, чтобы интернет-провайдер Scarlet установил систему для фильтрации всех входящих и исходящих электронных сообщений и блокировал потенциально незаконные сообщения. При рассмотрении дела в суде первой инстанции, суд заявил, что интернет-провайдер не несет ответственности, но при этом признал легитимность требований SABAM, обязав провайдера создать систему фильтрации. Компания Scarlet оспорила решение, и дело было передано на рассмотрение в Суд Европейского союза. В своем решении Суд ЕС постановил, что создание систем фильтрации и блокировки для всех пользователей и на неограниченный срок, исходя из абстрактных соображений превентивного плана, является нарушением основных прав, а именно права

на неприкосновенность частной жизни, свободы связи и информации. Кроме того, такой подход был признан нарушающим право интернет-провайдера свободно заниматься коммерческой деятельностью. См. подробнее: CJEU (2011) Judgement of the Court in Case C-70/10: Scarlet Extended SA v Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM). Адрес в Интернете: http://curia.europa.eu/juris/liste.jsf?language=en&jur=C,T,F&num=C-70/10&td=ALL [просмотрено 6 августа 2018 г.].

[62] CJEU (2016) Judgement of the Court in Case C-160/15: GS Media BV v Sanoma Media Netherlands BV, Playboy Enterprises International Inc., Britt Geertruida Dekker. Адрес в Интернете: http://curia.europa.eu/juris/liste.jsf?language=en&jur=C,T,F&num=C-160/15&td=ALL [просмотрено 6 августа 2018 г.].

[63] В 2013 г. закон Hadopi был частично отменен, поскольку наказание в форме блокировки доступа нарушителя к Интернету было сочтено несоразмерным проступку.

[64] ECHR (2013) Judgement of the Court (First Section) in the Case Delfi AS v Estonia (Application no. 64569/09). Адрес в Интернете: http://hudoc.echr.coe.int/eng?i=001-126635 [просмотрено 6 августа 2018 г.].

[65] ECHR (2015) Judgement of the Court (Grand Chamber) in the Case Delfi AS v Estonia (Application no. 64569/09). Адрес в Интернете: http://hudoc.echr.coe.int/eng?i=001-155105 [просмотрено 6 августа 2018 г.].

[66] Palfrey J (2006) Stemming the International Tide of Spam. In: ITU (2006) Trends in Telecommunication reforms 2006. Адрес в Интернете: http://www.itu.int/ITU-D/treg/publications/Chap%207_Trends_2006_E.pdf [просмотрено 6 августа 2018 г.].

[67] Shannon V. The end user: Junk payout in spam case — Technology // International Herald Tribune. The New York Times, 26.04.2006. Адрес в Интернете: http://www.nytimes.com/2006/04/12/technology/12iht-PTEND13.1523942.html [просмотрено 6 августа 2018 г.].

Раздел 5

Экономические аспекты

Экономические аспекты

Мы знаем, как регулировать передачу пакетов, но совершено не знаем, как регулировать передачу долларов.

Дэвид Кларк, главный архитектор протоколов сети Интернет

Эти слова Дэвида Кларка отражают тот дух, который царил в интернет-сообществе на ранних этапах его развития, когда Интернет был некоммерческим проектом и преимущественно финансировался за счет американских исследовательских грантов. Однако в 1990-х и начале 2000-х годов в Кремниевой долине стали появляться новые бизнес-модели, позволявшие зарабатывать за счет интернет-рекламы.

Экономические аспекты управления Интернетом во многом связаны с превращением Интернета из некоммерческого проекта в важнейшее направление хозяйственной деятельности и источник экономического роста в современном мире. С первых дней своего существования Интернет способствовал распространению творческих идей и начинаний. Постепенно в дополнение и отчасти в противовес этой функции началось его использование в коммерческих целях. С притоком денег повысился интерес к Интернету со стороны делового сообщества и регуляторов. На смену царившему на заре творческому подходу, открывавшему безграничные возможности и горизонты, пришла свойственная деловому сообществу коммерческая хватка. Высокий творческий потенциал и финансовые ресурсы позволили совершить настоящую экономическую революцию, географическим центром которой стал город Сан-Франциско в американском штате Калифорния.

Политика в области цифровых технологий влияет на экономические процессы и денежные потоки и в то же время испытывает на себе их влияние[1]. Создание нормативно-правовой базы, которая бы способствовала развитию цифровых технологий, чрезвычайно важно для экономического роста. Так, одной из причин стремительного развития этого сектора в Кремниевой долине стало эффективное регулирование, позволившее защитить интеллектуальную собственность интернет-компаний, способствовать привлечению инвестиций и т. д. Важность «аналоговой» надстройки (благоприятной нормативно-правовой среды) для цифровой экономики отмечена в «Докладе о мировом развитии 2016: Цифровые дивиденды» Всемирного банка[2].

На регулирование в сфере цифровых технологий также влияют Интернет-компании. Они приобрели мощные лоббистские ресурсы, что особенно заметно в центрах принятия решений по вопросам цифровых технологий, включая Вашингтон, Брюссель и Женеву.

В ходе анализа экономических аспектов Интернета мы сконцентрируем внимание на четырех областях хозяйственной деятельности денежного и неденежного характера:

- Электронная коммерция: традиционная торговля с использованием Интернета.
- Экономика Интернета ДАННЫХ: новая модель коммерческой деятельности и реклама как ее основа.
- Экономика Интернета ДОСТУПА: телекоммуникационная отрасль в эпоху Интернета.
- Интернет-банкинг, электронные деньги и виртуальные валюты.

В добавление к этому мы рассмотрим еще два важных вопроса: защиту прав потребителей и налогообложение.

Электронная коммерция

На протяжении последних 15 лет электронная коммерция была одной из основных движущих сил развития Интернета. Важность экономического аспекта управления Интернетом может проиллюстрировать название документа, который положил начало реформе системы управления Интернетом и привел к учреждению ICANN — «Основы глобальной электронной коммерции» (1997)[3]. В этом документе указано, что «частный сектор должен играть главную роль» в управлении Интернетом, и основная функция такого управления заключается в обеспечении «предсказуемой, минималистичной, непротиворечивой и простой правовой среды для электронной коммерции».

В современном мире электронная коммерция оказывает огромное воздействие на деятельность людей и компаний. Она дает множество преимуществ потребителям: это удобство совершения покупок в Интернете, гибкость доступа к различным рынкам и возможность сэкономить время, пользуясь интернет-банками и услугами электронных платежей. Кроме того, электронная коммерция влияет на бизнес, меняет подходы к управлению цепочками поставок и упрощает выход к покупателям путем интернет-рекламы, маркетинга и других решений. Однако и работать на интернет-рынке становится сложнее из-за возросшей конкуренции.

Определение

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 интернете, 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. ВТО дает еще более точное определение, согласно которому электронной торговлей является «производство, распространение, реклама, продажа или доставка товаров и услуг электронным способом»[4]. В своем подходе к электронной коммерции ЕС оперирует понятием «услуги информационного общества», к которому относятся «любые услуги, которые обычно предоставляются за вознаграждение, удаленно, с использованием электронного оборудования для обработки (включая цифровой сжатие) и хранения данных, а также по индивидуальному запросу получателя услуги»[5].

Электронная коммерция существует в различных формах:

- business-to-consumer (B2C) — самая известная форма электронной торговли (например, Amazon.com);
- business-to-business (B2B) — экономически важный вид электронной торговли, более чем в два раза превышающий объем сегмента B2C[6];
- business-to-government (B2G) — имеет огромное значение с точки зрения политики госзакупок;
- consumer-to-consumer (C2C) — например, электронные аукционы (типа eBay).

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

ВТО и электронная коммерция

Играя ключевую роль в регулировании международной торговли, ВТО способствовала принятию системы соглашений в этой области. К ним относятся Генеральное соглашение по тарифам и торговле (General Agreement on Tariffs and Trade — GATT)[7], в котором речь идет о торговле товарами, Генеральное соглашение по торговле услугами (General Agreement on Trade in Services — GATS)[8] и TRIPS[9]. В рамках этих соглашений, ВТО регулирует многие важные для электронной коммерции вопросы, в том числе либерализацию телекоммуникаций, защиту прав интеллектуальной собственности и некоторые аспекты развития ИКТ. Следующие виды деятельности и инициативы ВТО имеют непосредственное отношение к электронной коммерции.

- Временный мораторий на обложение электронных транзакций таможенными пошлинами, введенный в 1998 г. В соответствии с ним все сделки, совершаемые в Интернете, были освобождены от уплаты таможенных пошлин в странах-членах ВТО[10].
- Подготовленная в 1998 г. Рабочая программа ВТО по электронной коммерции, которая включает обязательства органов ВТО в вопросах, связанных с электронной торговлей[11].
- Механизм разрешения споров, предназначенный, в частности, для электронных сделок. Ярким примером, имеющим непосредственное от-

ношение к электронной коммерции, является дело «США против Антигуа», связанное с азартными играми в Интернете[12].

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

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

Многие сделки в сфере электронной коммерции имеют двойственную природу. На заре цифровых технологий основная проблема заключалась в том, считать ли аудиопродукцию товаром или услугой в зависимости от того, как она доставляется покупателю — на компакт-дисках (материальная форма) или через Интернет (нематериальная форма)? В конечном счете, одна и та же песня может иметь различный торговый статус (и подлежать обложению разными налогами и таможенными пошлинами) в зависимости от способа ее доставки потребителю. Вопрос отнесения сделки к той или иной категории также актуален в случае со сделками смешанного типа, когда имеется как нематериальная сторона (заключение договора в Интернете, распространение программного обеспечения), так и материальная сторона (доставка принтера или другого цифрового устройства). С развитием сегмента Интернета вещей количество подобных сделок будет только увеличиваться. Проблема такой классификации очень важна, поскольку к торговле товарами и услугами применяются разные механизмы регулирования.

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

Поскольку Соглашение по торговым аспектам прав интеллектуальной собственности (TRIPS), заключенное в рамках ВТО, предоставляет гораздо более мощные правоприменительные механизмы в области прав интеллектуальной собственности, чем конвенции ВОИС, развитые страны пытались распространить сферу применения TRIPS на электронную коммерцию

и Интернет в целом, используя при этом два подхода. Во-первых, апеллируя к принципу «технологического нейтралитета», они указывали, что TRIPS, как и другие нормы ВТО, необходимо распространить на любые средства телекоммуникации, включая Интернет. Во-вторых, некоторые развитые страны потребовали более тесной интеграции так называемых цифровых договоров ВТО в систему TRIPS. Оба вопроса остаются открытыми, их важность для переговоров в рамках ВТО в будущем возрастет. 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.

Какую роль будет играть ВТО в сфере электронной коммерции в будущем?

В настоящее время идут споры о том, следует ли ВТО играть более активную роль в регулировании электронной коммерции. В ходе Общественного форума ВТО в сентябре 2016 г. участники отмечали, что организации следовало бы уделять больше внимания электронной коммерции и в целом цифровой экономике[13]. Однако среди стран – членов ВТО согласия по этому вопросу нет. Одни полагают, что необходимо сконцентрироваться на вопросах электронной коммерции и принять соответствующее многостороннее соглашение, другие считают, что у ВТО есть более важные задачи (например, обеспечение доступа к инфраструктуре и цифровая грамотность), которые необходимо решить, прежде чем заниматься созданием нормативно-правовой базы[14].

Электронная коммерция и другие вопросы цифровых технологий

Провести грань между вопросами регулирования электронной коммерции и другими проблемами, связанными с управлением Интернетом, становится все сложнее. Например, торговля, будучи составной частью экономики данных, не может не касаться правозащитной тематики, включая право на неприкосновенность частной жизни и свободу информации (этим занима-

ется Совет по правам человека ООН), а также вопросов кибербезопасности, поскольку роль данных в борьбе против терроризма и преступности возрастает (Группа правительственных экспертов ООН, УНП ООН). Хотя у ВТО нет возможности (и необходимости) заниматься всеми вопросами цифровых технологий за пределами торговли, она должна разработать механизм для координации своих действий по регулированию электронной коммерции с другими международными организациями, от которых зависит соблюдение правил в этой области.

Другие международные инициативы в области электронной торговли

Вопросами, связанными с электронной коммерцией, занимается несколько международных организаций. Значительная работа в этой области проделана Комиссией ООН по праву международной торговли (UNCITRAL). В 1992 г. в рамках UNCITRAL была создана Рабочая группа по электронному обмену данными (позже переименована в Рабочую группу по электронной торговле), которая, в частности, способствовала принятию Типового закона об электронной торговле[15] и Конвенции Организации Объединенных Наций об использовании электронных сообщений в международных договорах[16]. Этот типовой закон стал одной из наиболее успешных и популярных международных инициатив в этой области. Закон регулирует вопросы, связанные с интеграцией электронной коммерции и традиционного торгового законодательства (например, признание действительности электронных документов). Этот документ стал основой законодательства об электронной коммерции во многих странах.

Еще одной инициативой в области электронной коммерции стала разработка стандартов Electronic Business XML (ebXML) в рамках Центра ООН по упрощению торговых процедур и электронному бизнесу (CEFACT) и Организации по развитию стандартов структурированной информации (OASIS). Основная задача этой инициативы – внедрение открытых технических стандартов для внутренних и международных электронных сделок[17]. Одновременно с разработкой новых стандартов, продолжают активно использоваться старые стандарты EDI (Electronic Data Interchange). Пока неясно, будут ли они

подлежать корректировке в свете новейших тенденций в развитии технологий.

Конференция ООН по торговле и развитию (UNCTAD) наиболее активна в области исследований и развития потенциала; в основном она занята вопросами связи между электронной коммерцией и развитием. Каждый год UNCTAD публикует «Доклад об информационной экономике», который содержит обзор новых технологий в области торговли и развития. В 2016 г. UNCTAD приступила к реализации инициативы Электронная торговля для всех (eTrade for All Initiative), которая представляет собой многосторонний проект, призванный расширить доступ развивающихся стран к электронной коммерции и ее преимуществам[18].

Деятельность ОЭСР охватывает различные аспекты электронной коммерции, включая вопросы защиты прав потребителей и цифровые подписи. Первым документом этой организации по вопросам электронной торговли был План действий по электронной коммерции 1998 г., в котором можно выделить четыре момента: повышение уровня доверия со стороны пользователей и потребителей, установление основных правил работы цифрового рынка, развитие информационной инфраструктуры в сегменте электронной коммерции и извлечение из него максимальной пользы[19]. В дальнейшем ОЭСР выпускала рекомендации и руководства по этим вопросам.

В последние годы растет внимание к вопросам электронной коммерции и со стороны G20. В ходе саммита G20 в г. Ханчжоу (Китай) в сентябре 2016 г. электронная коммерция была названа одной из приоритетных областей сотрудничества между участвующими странами[20]. Лидеры стран ознакомились с инициативой по созданию Международной платформы электронной торговли (Electronic World Trade Platform) с целью содействия малым и средним предприятиям при выходе на международный рынок электронной торговли.

В секторе бизнеса одной из самых активных организаций является Международная торговая палата, которая выпускает большое количество рекомендаций и аналитических докладов по вопросам электронной коммерции.

Также следует упомянуть Глобальный договор ООН (UN Global Compact). Не затрагивая напрямую вопросы электронной коммерции, этот документ увязывает коммерческую деятельность и правозащитную проблематику и призывает компании действовать ответственно с учетом всеобщих прин-

ципов в области прав человека. Учитывая, что интернет-компании уделяют все больше внимания вопросам соблюдения прав человека в цифровой среде, эта инициатива может оказать существенное влияние на интернет-отрасль, включая электронную коммерцию.

Региональные инициативы

ЕС принял стратегию развития электронной торговли на так называемом Саммите Dot.Com лидеров стран ЕС в Лиссабоне (март 2000 г.). Несмотря на то, что в отношении электронной торговли акцент был сделан на частные и ориентированные на рынок инициативы, в рамках ЕС были также приняты некоторые коррекционные меры, направленные на защиту государственных и общественных интересов (содействие предоставлению универсального доступа к Интернету, регулирование конкуренции с учетом общественных интересов, ограничение распространения вредоносных материалов). В 2015 г. была принята Единая стратегия развития рынка цифровых технологий (Digital Single Market Strategy). В этом документе уделяется большое внимание электронной коммерции с акцентом на повышение доступности цифровых товаров и услуг и развитие цифровой экономики как источника роста.

ЕС принял Директиву по электронной коммерции (для перехода на единую и комплексную нормативно-правовую базу в области электронной коммерции для всех стран-членов ЕС), а также ряд других документов по использованию электронной цифровой подписи, защите данных и электронным финансовым транзакциям.

В Азиатско-Тихоокеанском регионе центральную и направляющую роль в вопросах электронной коммерции играет АТЭС. Одной из первых программ АТЭС по развитию электронной торговли стал План действий АТЭС в области электронной коммерции (APEC Blueprint for Action on Electronic Commerce), принятый с целью реализации различных инициатив АТЭС в этой области. Задача по реализации этого плана возложена на Руководящую группу по электронной коммерции, которая была создана для решения различных вопросов, связанных с электронной коммерцией, включая защиту прав потребителей, защиту данных, противодействие спаму и обеспечение кибербезопасности. Наиболее значимой инициативой стал

Индивидуальный план действий АТЭС по развитию безбумажной торговли (Paperless Trading Individual Action Plan)[21], нацеленный на обеспечение перехода на систему трансграничной торговли с безбумажным документооборотом.

В рамках АСЕАН была создана Рабочая группа по электронной коммерции и содействию развитию ИКТ в области торговли. Инициатива направлена на создание нормативно-правовой базы в области электронной коммерции и повышение уровня доверия со стороны потребителей. В этой связи реализуется Проект по созданию правовой инфраструктуры в сфере электронной коммерции, цель которого состоит в выработке рекомендаций по развитию правовой инфраструктуры и оказании помощи в предпринимательской деятельности компаний стран АСЕАН в этом сегменте.

В рамках Общего рынка Восточной и Южной Африки (COMESA) также ведется работа по развитию электронной коммерции. Была принята стратегия, в которой говорится о готовности организации активно содействовать развитию электронной коммерции с целью создания общего цифрового рынка в регионе. В 2010 г. Советом COMESA принят Типовой закон по электронным транзакциям, который содержит положения об электронных подписях, электронной коммерции, защите прав потребителей, нежелательных коммерческих сообщениях и разрешении споров в Интернете[22].

Коллективные инициативы

Коллективной (многосторонней) инициативой называется объединение усилий стран из разных регионов по какому-то определенному вопросу. Такой подход все чаще используется в рамках ВТО. В последнее время ведутся переговоры по ряду трансрегиональных торговых соглашений, которые могут оказать существенное влияние на регулирование сферы цифровых технологий. Наибольшую известность среди этих соглашений получили подписанное в феврале 2016 г. Транстихоокеанское партнерство (TPP) и Трансатлантическое и инвестиционное партнерство (TTIP), переговоры по которому по состоянию на октябрь 2016 г. еще не завершились. Указанные соглашения затрагивают не только сферу электронной коммерции, но и вопросы регулирования Интернета и разрешения споров.

Экономика Интернет-данных

Формирование новой коммерческой модели интернет-отрасли (рис. 19), преимущественно силами компаний из Кремниевой долины, началось в конце 1990-х годов и завершилось в конце первого десятилетия XXI века. Уже в 1990-е гг. стало понятно, что финансировать развитие Интернета за счет государственных средств, как это было в прошлом, не получится. Нужна была более устойчивая модель развития. Были предприняты единичные попытки взимать плату за доступ к интернет-услугам и материалам, но они не увенчались успехом. Новая модель не предусматривает предоставление интернет-услуг на возмездной основе; доход генерируется за счет сложных решений в области рекламы.

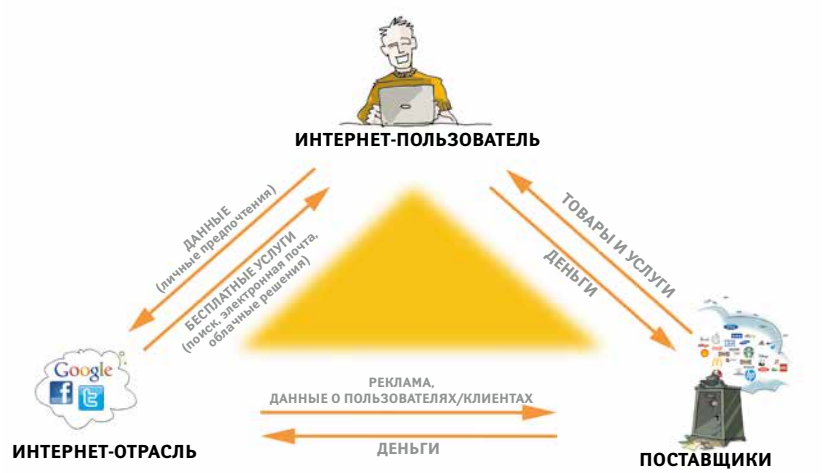


Рисунок 19. Коммерческая модель Интернета

Главным экономическим ресурсом в такой коммерческой модели стали данные пользователей. Осуществляя поиск информации и общаясь в сети, пользователи оставляют за собой «электронный след», то есть огромный объем информации, в том числе их персональные данные и созданную ими информацию. Интернет-компании собирают и анализируют такие данные с целью выявления предпочтений, вкусов и привычек пользователей. Кроме

того, компании стремятся получить информацию о конкретных группах, например, данные о поведенческих моделях подростков в конкретном городе или регионе. Интернет-компании могут предсказать с высокой долей вероятности, что может пожелать купить или сделать человек, относящийся к определенной категории. Эти данные об интернет-пользователях представляют огромную ценность, поскольку их можно использовать в различных целях. Как правило, ими пользуются поставщики товаров и услуг в своей маркетинговой деятельности.

ВОПРОСЫ

Защита пользователей и прозрачность

С формальной точки зрения, нажимая клавишу «Принимаю» под длинным договором или пользовательским соглашением, отпечатанным мелким шрифтом, пользователи соглашаются с условиями поставщика услуги. Это, однако, не дает ответа на вопрос, делают ли они осознанный выбор, учитывая возможность использования их данных в коммерческих целях. Велика вероятность, что пользователи обменивают свои данные на возможность пользоваться интернет-услугами, не задумываясь о последствиях таких действий. Чем прозрачнее и проще для понимания будут интернет-соглашения, тем лучше не только для пользователей, но и для интернет-компаний, которые смогут разработать устойчивую бизнес-модель, основанную на осознанном выборе потребителей.

Риск злоупотребления доминирующим положением на рынке

Интернет-отрасль склонна к монополизации рынка. Так, по состоянию на август 2016 г. на компанию Google приходилось 70% всех поисковых запросов, сделанных с помощью настольных ПК, и более 90% всех запросов на мобильных устройствах/планшетах[23].

Обладая монополией или доминирующим положением на рынке, компании зачастую используют свое преимущество, чтобы не допустить или затруднить выход на рынок новых участников. Для решения этой проблемы

соответствующим ведомствам национального и/или регионального уровня следует создать эффективные механизмы анализа конкурентной среды, поддерживать здоровую конкуренцию и вести борьбу с монополиями путем надзора и законодательных мер. Хотя такие нормативные и законодательные меры варьируются в зависимости от страны или региона, они помогают противостоять попыткам международных интернет-компаний подавить конкурентов на локальном и региональном уровнях. Например, опираясь на развитую законодательную базу в этой области, ЕС предпринял ряд инициатив по предотвращению и искоренению незаконных действий интернет-компаний и вынудил их соблюдать соответствующие требования. В последние годы Европейская комиссия активно занимается мониторингом конкурентной среды на рынке цифровых технологий ЕС. В результате, несколько исков были выдвинуты против интернет-компаний, злоупотреблявших своим доминирующим положением на рынке, в том числе в отношении рекламной деятельности компании Google.

Экономика Интернет-доступа

Интернет-пользователи и компании платят интернет-компаниям за услугу доступа к Интернету. Как правило, полученная интернет-провайдерами плата используется для покрытия следующих расходов:

- Стоимость связи и интернет-соединения со следующим крупным узлом.
- Стоимость IP-адресов, полученных от региональных интернет-регистратур (RIR) или местных интернет-регистратур (LIR). Каждому устройству с доступом в Интернет присваивается свой IP-адрес.
- Стоимость приобретения, установки и обслуживания оборудования и программного обеспечения (рис. 20).

Кроме того, власти постоянно вводят новые требования в области доступа к Интернету, например, в отношении хранения данных, что еще больше осложняет ситуацию. Появление новых нормативно-правовых требований ведет к новым расходам, которые либо перекладываются на плечи

интернет-пользователей, у которых повышается абонентская плата, либо приводят к снижению прибыли интернет-провайдеров.

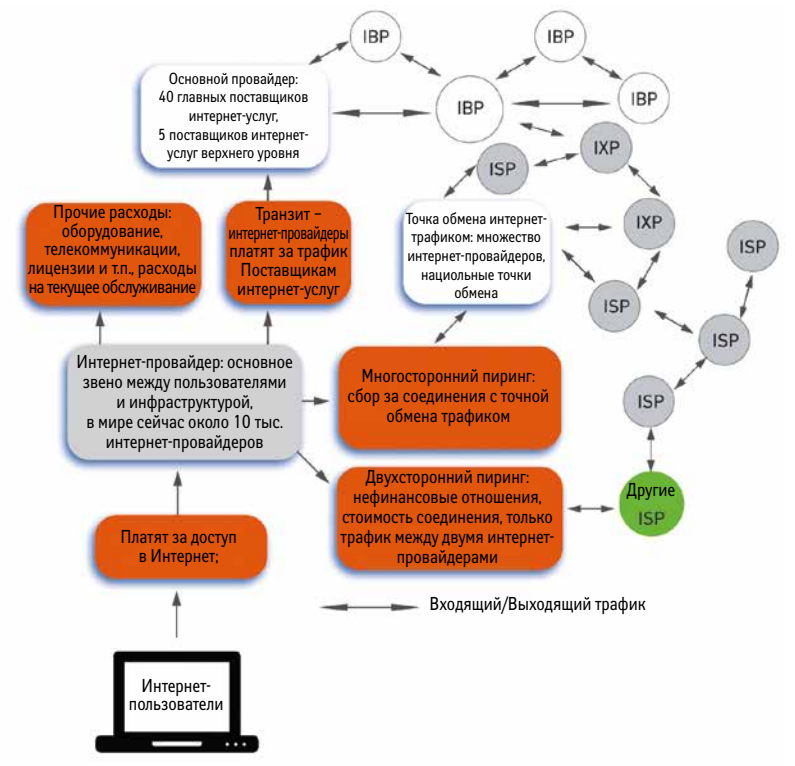


Рисунок 20. Организация трафика в экономике интернет-доступа

Вопросы

Перераспределение доходов между телекоммуникационными компаниями и интернет-компаниями

Вопрос о перераспределении доходов от Интернета поднимают телекоммуникационные компании, пытаясь увеличить свою долю доходов на фоне стремительного роста доходности в интернет-отрасли. Пока наибольшую выгоду извлекают компании, создающие интернет-контент. Они смогли освоить

инновационную модель ведения бизнеса, в основе которой лежит реклама. Однако телекоммуникационные компании утверждают, что тоже имеют право на эти доходы, поскольку именно они обеспечивают доступ к материалам с использованием собственной телекоммуникационной инфраструктуры.

Как правило, для обоснования своих претензий на долю в доходе интернет-компаний телекоммуникационные компании ссылаются на необходимость инвестировать средства в развитие телекоммуникационной инфраструктуры. В свою очередь, компании, распространяющие свои материалы в Интернете, заявляют, что телекоммуникационные компании и так взимают с интернет-пользователей плату за доступ в Интернет, а их более низкую доходность они объясняют устаревшей коммерческой моделью (предоставление безлимитного доступа за фиксированную плату). В ходе подготовки к WCIT-12 в Дубае в интернет-сообществе широко обсуждалось противоречивое предложение европейского оператора ETNO, который предложил взимать плату с поставщиков материалов (например, Facebook и Google) за доступ к их услугам. Тогда это предложение не было поддержано, однако оно остается актуальным в дальнейших переговорах по вопросам управления Интернетом.

Вопрос о перераспределении доходов от Интернета тесно связан с дебатами о сетевом нейтралитете. Должен ли весь трафик обрабатываться на равных основаниях или его следует поделить на несколько уровней в зависимости от качества услуг, оплаты и надежности (например, можно представить себе широкий спектр услуг от предоставления VIP доступа в Интернет до создания Интернета для бедных).

Фиксированная плата и продажа услуг пакетами

Обсуждение вопроса о фиксированной плате за доступ в Интернет часто сводится к поиску оптимального баланса между тремя составляющими: технической целесообразностью, экономической эффективностью и социальными эффектами[24]. Некоторые авторы отметили проблемы, которые могут быть связаны с заменой нынешней простой системы с фиксированными тарифами более сложной системой тарификации на основании пакетов услуг[25]. С точки зрения практических изменений, некоторые считают, что изменение подходов к тарификации интернет-услуг принесет больше проблем, чем решений.

Нужно ли делиться доходом от коммуникационных услуг с развивающимися странами?

Многие развивающиеся страны поднимали вопрос о справедливости сложившейся экономической модели Интернета. В отличие от обычной телефонии, где стоимость каждого международного звонка делится между двумя странами, в Интернете все издержки ложатся на одну из сторон. Пользователям из развивающихся стран приходится самим находить средства для подсоединения к магистральным кабелям, которые преимущественно расположены в развитых странах. В итоге, как это ни парадоксально, выходит, что малые и бедные государства субсидируют Интернет в развитых странах.

Этот вопрос наиболее актуален для самых бедных стран, в которых доход от услуг международной электросвязи является важным источником бюджетных поступлений. Ситуацию еще больше осложнило появление IP-телефонии, что привело к перемещению значительного объема телефонного траффика от национальных операторов электросвязи в Интернет.

Развивающие страны выступали с требованиями перехода на более справедливую модель доступа к Интернету, в том числе в рамках WSIS, рабочих групп МСЭ и WCIT-12.

Новые тенденции: Интернет вещей, искусственный интеллект, экономика совместного потребления

Интернет вещей появился недавно и уже оказывает огромное воздействие на экономику Интернета. Интеграция Интернета вещей позволяет снизить издержки и повысить эффективность коммерческой деятельности. Многие новые компании пользуются так называемыми «умными зданиями», стремясь оптимизировать расход электроэнергии и защитить окружающую

среду. ИКТ позволяют повысить конкурентоспособность компаний, давая им возможность развиваться быстрее по сравнению с предприятиями, придерживающимися традиционных подходов. Это привело к формированию со стороны делового сообщества запроса на новые, индивидуальные и инновационные решения в области информационных технологий, что способствует общему росту благосостояния.

Применение искусственного интеллекта также может оказать существенное воздействие на развитие экономики. С одной стороны, ожидается, что производительность труда за счет внедрения искусственного интеллекта существенно возрастет, с другой стороны, существуют опасения, что его повсеместное внедрение отрицательно скажется на рынке труда и уровне занятости.

Последним новшеством стала экономика совместного потребления, появление которой ознаменовалось выходом на международных рынок таких компаний, как Uber и Airbnb. Они смогли извлечь максимальную выгоду из экономики Интернета, сделав цифровые решения неотъемлемой частью своих бизнес-процессов. Это позволило снизить издержки и наладить взаимодействие с потребителями без каких-либо посредников. Против такой модели выступили предприятия, придерживавшиеся традиционных подходов к организации коммерческой деятельности в сегментах такси и гостиничного обслуживания. В настоящее время продолжаются споры о том, нужно ли вводить специальный нормативно-правовой режим для предприятий экономики совместного потребления (в частности, решения вопросов ответственности, защиты прав потребителей, налогообложения и т. п.). Можно даже услышать предложения запретить предоставление таких услуг. На данный момент ЕС занял выжидательную позицию по этому вопросу. В июне 2016 г. Европейская комиссия опубликовала «Европейскую повестку по экономике совместного потребления», которая содержит разъяснения относительно применения существующих норм ЕС в этой сфере. По мнению Комиссии, полный запрет на предоставление услуг в соответствии с моделью экономики совместного потребления может вводиться только как крайняя мера[26].

С развитием электронной коммерции все больше людей стали работать в качестве внештатных, вольнонаемных сотрудников. С одной стороны, такое изменение рынка труда способствовало формированию динамичного и прогрессивного сообщества внештатных сотрудников, развитию малых

и средних предприятий и снижению уровня безработицы. С другой стороны, это требует пересмотра подходов к регулированию рынка труда, в частности в том, что касается классификации полученных доходов.

Развитию экономики Интернета также способствовал такой противоречивый фактор, как рост популярности сетевых азартных игр. В силу специфики данной области, к ее регулированию применялись различные подходы. Например, в ЕС государства-члены могут регулировать азартные игры в Интернете по своему усмотрению. Поскольку эта сфера тесно связана с вопросами государственной политики, нравственности, защиты малолетних, кибербезопасности и борьбы с преступностью, было решено передать полномочия по регулированию этого сегмента на национальный уровень с учетом политической и социальной специфики каждой страны.

Интернет-банкинг, электронные деньги, виртуальные валюты

Цифровые деньги представляют угрозу для всех стран, желающих контролировать свою валюту.

Дэвид Сакстон, один из основателей Net1[27]

Интернет-банкинг

Интернет-банкинг предполагает использование Интернета 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. Например, транзакция, которая обходится банку в 4 доллара при ее проведении традиционным способом, будет стоить лишь 0,17 доллара при использовании интернет-банкинга[28].

Электронные деньги

Электронными деньгами называют остаток, зафиксированный электронными средствами на карте предоплаты или на сервере. Согласно определению Банка международных расчетом (БМР), электронные деньги представляют собой «баланс или механизмы предоплаты для осуществления платежей посредством терминалов торговой точки, прямых переводов между двумя устройствами или по таким открытым компьютерным сетям, как Интернет»[29]. Электронные деньги являются частью существующей банковской и валютно-кредитной системы (официальное платежное средство, регулируемое центральными банками). Как правило, их использование связано с использование карт, выпущенных такими компаниями, как Mondex и Visa Cash.

Цифровые деньги, виртуальная валюта и криптовалюта

В отличие от обычных электронных денег, которые являются выражением официальной валюты (например, евро или долларов США), не меняя их стоимости, цифровая валюта не связана с официальной валютой и не вписывается в какую-либо национальную финансовую систему. Таким образом, цифровая валюта не регулируется государственными властями.

Цифровая валюта может быть централизованной и децентрализованной. В централизованной модели такие операции как выпуск денег и правоприменение в области использования и оборота денежных средств регулируются центральным органом, тогда как в децентрализованной модели такие операции осуществляются в сети различными лицами.

К цифровым валютам относятся как виртуальная валюта, так и криптовалюта. Виртуальные валюты основаны на централизованной модели, тогда как криптовалюты (для обеспечения их безопасности и предотвращения подделок используется криптозащита) могут быть как централизованными, так и децентрализованными. Одним из примеров криптовалюты является биткойн[30].

Согласно опубликованному в 2012 г. определению Европейского центрального банка (ЕЦБ), виртуальными деньгами (виртуальной валютой) называются «нерегулируемые цифровые деньги, которые выпускаются и, как правило, контролируются их разработчиками, используются и принимаются в качестве платежного средства членам определенного виртуального сообщества»[31]. В 2014 г. Европейская служба банковского надзора дала следующее определение: «Виртуальная валюта — цифровое воплощение денег, выпущенных без участия центрального банка или государственных властей, которые могут не иметь привязки к официальной валюте, но принимаются в качестве расчетного средства физическими и юридическими лицами и могут быть переданы, храниться или торговаться в электронном виде»[32].

Криптовалюты завоевывают мир, а их популярность и использование растут. Такие крупные компании, как Apple, Dell и PayPal, уже заявили о планах по включению криптовалют в свои платежные системы. Их примеру могут последовать и другие компании.

Последние годы наибольшей популярностью среди криптовалют пользовались биткойны. Соответственно, росло и число услуг с оплатой в биткойнах.

Биткойн

В основе биткойна лежит технология распределенного реестра (блокчейн), которая выполняет функцию центрального хранилища. По сути, это база данных, «распределенная» в сети (сети P2P). Использование такого программного обеспечения с открытым исходным кодом позволяет участникам сети проверять любую сделку с биткойнами на достоверность и, таким образом, выступать в качестве хранителей центрального реестра. Участники сети называются узлами, которые работают сообща, но при этом практически не взаимодействуют друг с другом, используя в качестве подтверждения хронологии транзакций взаимную проверку подлинности. Подделать такой распределенный реестр невозможно, при условии, что добросовестных узлов больше, чем узлов-нарушителей.

Общее количество биткойнов, которые могут быть выпущены, ограничено 21 миллионом, соответственно, стоимость этой цифровой валюты со временем будет расти (что дает ранним участникам системы существенное преимущество). Создавать («добывать») биткойны может любой. Для этого достаточно включиться в цепочку передачи нерешенных вычислительных задач (с использованием системы «доказательство выполнения работы»). Над решением задачи трудятся все узлы, и как толь-

ко решение найдено, блок закрывается, и все узлы переходят к решению другой задачи (следующий блок в цепочке). За предоставление в этих целях своих компьютерных мощностей узлы, то есть «добытчики», получают вознаграждение в форме биткойнов и комиссий за проведенные другими пользователями транзакции.

Основное преимущество криптовлюты — гораздо более низкая стоимость транзакций по сравнению с традиционными банковскими услугами, высокая скорость и прозрачность платежей, а также возможность мобильного доступа. Такие преимущества могут помочь стартапам достичь новых высот и поставить развивающиеся страны на одну ступеньку с развитыми экономиками на глобальном рынке.

Сейчас многие международные системы принимают к оплате биткойны. При этом такие транзакции не облагаются НДС в ряде стране. В июле 2015 г. Суд Европейского союза постановил, что обмен официальной валюты на биткойны не должен облагаться потребительскими налогами, тем самым приравняв такие транзакции к операциям с обычными банкнотами и монетами.

По всей видимости, виртуальные валюты привлекают все большее внимание со стороны центральных банков. Например, в начале 2016 г. Народный банк Китая заявил о возможном создании собственной виртуальной валюты, что могло бы способствовать повышению прозрачности экономической деятельности, а также борьбе с отмыванием денег и уклонением от налогообложения[33].

В 2016 г. Международный валютный фонд (МВФ) выпустил доклад «Виртуальные валюты и их аналоги: первоначальные соображения» (Virtual Currencies and Beyond: Initial Considerations). В документе отмечены проблемы, связанные с регулированием виртуальных валют, включая защиту прав потребителей, вопросы налогообложения и финансовой стабильности. По мнению авторов доклада, «необходимо, чтобы регулирование позволяло бороться с рисками, не препятствуя инновациям». На международном уровне необходимо вводить нормы и обеспечивать гармонизацию режимов различных юрисдикций с учетом передового опыта и международных стандартов[34].

Вопросы

Трансформация международной банковской системы

Дальнейшее распространение электронных денег и банковских услуг в режиме онлайн может изменить всемирную банковскую систему, предоставив потребителям дополнительные возможности и снизив стоимость банковских операций. Экономически эффективные электронные банковские услуги бросают серьезный вызов традиционным банковским методам. Следует отметить, что многие традиционные банки активно используют интернет-банкинг. В 2002 г. в США было всего 30 банков, предлагающих услуги в Интернете. Сегодня сложно найти банк, не предоставляющий услуги в электронной форме.

Мобильная коммерция

Сегмент электронных платежей и денег быстро меняется в условиях развития технологий и появления новых устройств. Мобильные платежи больше не сводятся к заказам SMS. Мобильные телефоны стали гораздо сложнее и «умнее» (например, смартфоны и iPhone), что позволяет запускать на них различные приложения, в том числе в сфере мобильной коммерции.

Кибербезопасность

Кибербезопасность является одной из основных проблем на пути более широкого распространения электронных платежей. Как можно гарантировать безопасность финансовых транзакций в Интернете? Стоит отметить ответственность банков и других финансовых институтов за безопасность интернет-транзакций. Важным событием с этой точки зрения является принятие Конгрессом США в ответ на финансовые скандалы с участием компаний Enron, Arthur Andersen и WorldCom так называемого Акта Сарбанеса-Оксли[35]. Этот закон усиливает финансовый контроль и повышает ответственность финансовых институтов за безопасность интернет-транзакций. Он также делит ответственность за безопасность между клиентами, которые должны проявлять определенное благоразумие, и финансовыми институтами.

Невозможность воспользоваться средствами электронного платежа

Одним из основных препятствий, замедляющих развитие электронной коммерции, считается невозможность использовать электронные средства оплаты. В настоящее время основным платежным средством в области электронной торговли является кредитная карта. Это создает серьезные трудности для развивающихся стран, где сегмент банковских карт недостаточно развит. Властям этих стран необходимо внести изменения в законодательство для скорейшего внедрения кредитных карт в качестве платежного средства.

Инициативы национального и регионального уровня

Чтобы способствовать развитию электронной торговли, правительствам всех стран необходимо поощрять все формы безналичных платежей, включая кредитные карты и электронные деньги. Быстрое внедрение электронных денег потребует дополнительных мер государственного регулирования.

После того, как Гонконг первым принял комплексное законодательство в области электронной коммерции, в ЕС в 2000 г. была принята Директива об электронных деньгах (новая версия принята в 2009 г.)[36]. В отличие от электронных денег, в ЕС сегмент цифровой и/или виртуальной валюты пока никак не регулируется. На данный момент странам-членам предоставлена возможность самостоятельно регулировать использование таких валют, как биткойн. В Германии биткойн считается «частной валютой», которая может использоваться в отношениях между двумя лицами или организациями. Большинство стран заняло выжидательную позицию по этому вопросу, тогда как Россия и Таиланд пошли на более радикальные меры, запретив на своей территории транзакции с биткойнами.

Международные инициативы

Учитывая саму природу Интернета, весьма вероятно, что электронные деньги и виртуальная валюта станут глобальным явлением — и это даст повод рассматривать вопрос на международном уровне. Одним из действующих лиц в сфере предоставления банковских услуг в Интернете является Группа по электронным банковским услугам Базельского комитета. Она уже начала заниматься проблемами авторизации сделок, стандартов проверки благонадежности, прозрачности, конфиденциальности, отмывания денег и трансграничного надзора над банковской деятельностью — ключевыми вопросами с точки зрения внедрения электронных денег[37].

Центральную роль в регулировании виртуальной валюты на международном уровне играет Целевая группа по финансовым мероприятиям (FATF), которая занимается вопросами отмывания денег и финансирования терроризма. В рамках этой структуры США инициировали обсуждение вопроса о применении к виртуальным валютам норм, касающихся отмывания денег и финансирования терроризма.

Связь с правоприменительной деятельностью

В качестве примера того, как правоохранительные органы могут использовать системы электронных платежей в своей деятельности, можно привести запрос, направленный генеральным прокурором штата Нью-Йорк в адрес системы Paypal и банка Citibank с требованием не осуществлять платежи в пользу интернет-казино[38]. То, чего правоохранительные органы не могут достигнуть с помощью правовых механизмов, они могут добиться с помощью контроля над электронными платежами.

Неприкосновенность частной жизни

Каждый электронный платеж оставляет след, который фиксируется эмитентом средства электронного платежа (компании, выпускающие кредитные карты, банки). Хотя хранение таких данных представляется оправданной необходимостью в целях проведения взаиморасчетов, а также в качестве подтверждения факта платежа, накопление таких данных может представлять серьезную угрозу для соблюдения принципа неприкосновенности частной жизни пользователей, если такая информация используется для отслеживания потребительского поведения или оценки состоятельности клиентов при оказании будущих финансовых услуг.

Риски и злоупотребления, связанные с виртуальной валютой

Связанные с виртуальными валютами риски стали очевидны после закрытия в феврале 2014 г. Mt Gox, одной из крупнейших бирж по продаже биткойнов[39]. Пользовавшиеся ей инвесторы потеряли около 500 млн. долларов в результате кражи данных учетных записей.

Нередко звучат предупреждения о возможности злоупотребления виртуальными валютами для торговли запрещенными товарами и услугами, их использования в мошеннических операциях и при отмывании денег. Тот факт, что сделки с использованием биткойнов полностью анонимны, повышает вероятность злоупотреблений. Кроме того, кошельки биткойнов (оффлайн-хранилища биткойнов) также могут снабжаться криптозащитой.

В 2014 г. ФБР закрыло сайт Silk Road, который использовался для торговли украденными данными банковских карт, наркотиками и другими незаконными товарами. В качестве средства оплаты на сайте использовались биткойны[40].

В конце 2015 г. при поддержке американских властей был подготовлен доклад «Последствия виртуальной валюты с точки зрения национальной безопасности» (National Security Implications of Virtual Currencies). В нем говорилось, что «негосударственные субъекты», включая террористов и повстанцев, могут использовать виртуальную валюту в своих сделках[41].

В ЕС предпринимаются попытки решать такие проблемы законодательным путем. В июле 2016 г. Европейская комиссия опубликовала предложение о внесении изменений в Директиву о предотвращении использования финансовой системы в целях отмывания денег и финансирования терроризма, которое предусматривает включение площадок по торговле виртуальной валютой в сферу действия директивы с целью выявления подозрительных сделок, а также включение в законодательство определения термина «виртуальная валюта» и целей ее использования на основе определения, разработанного в 2014 г. Европейской службой банковского надзора[42].

Защита прав потребителей

Доверие потребителей является одним из основных условий успешного развития электронной коммерции. Этот вид деятельности является относительно новым, поэтому потребители еще не доверяют электронной коммерции так, как традиционной торговле. Защита прав потребителей является важным правовым инструментом укрепления доверия к электронной торговле. Регулирование электронной коммерции должно защищать потребителей в различных сферах:

- от кражи или незаконной передачи личных финансовых данных (например, информации о платежных картах);
- от недобросовестной рекламы,
- от некачественных товаров и услуг.

Новой характерной особенностью электронной коммерции становится необходимость защиты прав потребителей на международном уровне, что не является приоритетом для традиционной торговли. В прошлом потребители редко нуждались в международной защите, так как в основном приобретали товары и услуги в своей стране, и нуждались в защите только со стороны национальных органов по защите прав потребителей. С развитием электронной коммерции все больше сделок выходит за пределы государственных границ.

Важным вопросом с точки зрения защиты прав потребителей является проблема юрисдикции, к которой существует два основных подхода. Первый подход более выгоден для продавцов (преимущественно компаний, осуществляющих электронную торговлю) и основывается на принципе «страны происхождения», или принципе «предписано продавцом». При таком сценарии компании, занимающиеся электронной коммерцией, имеют преимущество, поскольку всегда действуют в рамках предсказуемой и хорошо знакомой им правовой среды. Другой подход, защищающий, в первую очередь, покупателя, основывается на принципе «страны назначения».

Здесь главной проблемой для компаний становится возможность столкновения с множеством разнообразных правовых систем. Одним из предлагаемых механизмов разрешения этой проблемы является гармонизация

законодательства различных стран в сфере защиты прав потребителей, что делает менее актуальным сам вопрос о юрисдикции. В области защиты прав потребителей, как и в других вопросах, связанных с электронной коммерцией, ведущую роль на международной арене играет ОЭСР. В рамках этой организации были приняты Руководство по защите прав потребителей в контексте электронной коммерции[43] (1999) и Директива по защите потребителей от мошеннических и обманных действий на трансграничном уровне (2003)[44]. Установленные ОЭСР основные принципы сохраняют свою актуальность и были взяты на вооружение другими деловыми объединениями, включая Международную торговую палату.

Высокая степень защиты прав потребителей обеспечивается в ЕС, где также проводятся информационные кампании по вопросам интернет-торговли. Вопросы юрисдикции разрешаются в рамках Брюссельского регламента[45], который требует, чтобы потребители всегда могли обратиться к местному законодательству и местным судам для защиты своих прав. В январе 2015 г. вступила в силу новая версия Брюссельского регламента[46], цель которой состоит в том, чтобы гармонизировать правовые режимы и расширить права потребителей на рассмотрение в судах ЕС исков против лиц, зарегистрированных за пределами ЕС.

Ряд частных ассоциаций и неправительственных организаций также работает в сфере защиты прав потребителей при электронных сделках, к ним относятся такие организации, как Consumers International, Consumer Protection and Enforcement Network и Международная торговая палата.

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

Налогообложение

Когда Фарадей открыл электромагнитную индукцию, один скептически настроенный политик спросил его, какая может быть польза от такого изобретения. Фарадей ответил: «Сэр, не знаю, какая от него польза. В одном я уверен: когда-нибудь вы будете брать с него налог»[47]. Эта история в полной мере отражает суть дискуссий по вопросу о налогообложении Интернета.

По мере роста роли Интернета в современной экономической жизни, растет интерес и к вопросу налогообложения отрасли. После финансового кризиса 2008 г. этот вопрос приобрел особую актуальность на фоне попыток многих стран повысить налоговые поступления и снизить уровень государственного долга. Одним из наиболее очевидных источников фискального дохода стало налогообложение экономической деятельности в Интернете.

Один из первых развернутых докладов по вопросу налогообложения Интернета был подготовлен Министерством экономики и финансов Франции в январе 2013 г[48]. Впоследствии появились и другие доклады по вопросам налогообложения в цифровой экономике[49].

Возникший в управлении Интернетом спор о том, должны ли вопросы киберпространства рассматриваться как отличные от явлений реального мира, находит свое отражение и в вопросе о налогообложении. США с самого начала пытались объявить Интернет зоной, свободной от налогов. В 1998 г. Конгресс США принял Закон о свободе Интернета от налогообложения, срок действия которого продлевался несколько раз. В 2016 г. Конгресс принял закон, который окончательно запретил региональным и местным властям облагать налогом доступ в Интернет. Наряду с введением в действие бессрочного Закона о свободе от налогообложения, были отменены налоги на ряд цифровых товаров и услуг[50].

ОЭСР и ЕС отстаивают противоположную позицию: с точки зрения налогообложения для Интернета не должно делаться каких-либо исключений. В Оттавских принципах ОЭСР отмечается, что электронная коммерция должна подлежать налогообложению на тех же принципах, что и обычная торговля, а именно принципах нейтральности, эффективности, четкости, простоты, действенности, справедливости и гибкости[51]. В своем докладе, опубликованном в 2014 г., Европейская комиссия вновь подчеркнула, что «к цифровым компаниям не должен применяться какой-либо специальный налоговый режим. Скорее, цифровые компании должны регулироваться по общим правилам, чтобы условия их деятельности не отличались от условий других участников рынка»[52].

Поскольку Интернет не требует особого режима налогообложения, ЕС ввел в 2003 г. правила, которые обязывают компании, занимающиеся электронной торговлей и не являющиеся резидентами ЕС, уплачивать НДС при реализации товаров в странах ЕС. Обоснованием для принятия такого решения послужил тот факт, что внешние компании (в основном, из США) имели преимущество по сравнению с европейскими компаниями, которые обязаны уплачивать НДС со всех транзакций, включая электронные. В настоящее время примеру ЕС последовали и другие страны. В условиях стремительного роста числа интернет-пользователей и повышения роли интернет-компаний (в основном, американских) в экономической жизни, многие страны ввели налог на услуги, предоставляемые в Интернете компаниями-нерезидентами. В качестве примера можно привести Россию[53], Индию[54], Израиль[55] и Индонезию[56].

Еще одной нерешенной проблемой в области налогообложения интернет-торговли является вопрос, в казну какого государства должны уплачиваться соответствующие налоги. Согласно Оттавским принципам налоги уплачиваются не в «стране происхождения», а в «стране назначения». США крайне заинтересованы в том, чтобы налоги уплачивались в соответствии с «принципом происхождения» товара, поскольку большинство компаний, занимающихся интернет-торговлей, зарегистрированы в США. В свою очередь, ЕС больше заинтересован в том, чтобы взимать налоги в «стране назначения», поскольку, с точки зрения электронной коммерции, там больше покупателей, чем продавцов.

В контексте Интернета обсуждаются вопросы налообложения, касающиеся не только внесения законодательных изменений, но и проблемы уклонения от уплаты налогов крупных интернет-компаний. В январе 2016 г. Европейская комиссия представила Пакет мер по борьбе с уклонением от налогов, призванный помешать компаниям ЕС выводить прибыль в страны с низкими ставками налогов. Появление этого документа было связано с обсуждением налоговой практики компании Google. По данным итальянских властей, в период 2009–2013 гг. компания Google вывела из-под налогообложения 227 млн. евро[57]. Кроме того, предметом острых дискуссий стала информация о сделке между Google и налоговыми органами Соединенного Королевства[58]. В мае 2016 г. власти Франции даже провели обыски в парижском офисе Google в рамках расследования дела о налоговом мошенничестве. Во Франции компанию обвиняют в неуплате налогов на сумму 1,6 млрд. евро[59]. Согласно опубликованному недавно исследованию американского фонда Public Interest Research Group Education Fund и организации Citizens for Tax Justice, из 30 крупнейших компаний, пользующихся льготными режимами налогообложения, 10 представляют технологическую отрасль, а рекорд в этом отношении принадлежит компании Apple[60].

В некоторых странах действуют льготные режимы налогообложения для операторов интернет-инфраструктуры и/или поставщиков интернет-услуг. Эти меры призваны способствовать инвестициям в развитие инфраструктуры и интернет-торговли. Например, в Индии Министерство связи предложило ввести налоговые каникулы для крупных проектов в сфере информационных технологий для привлечения инвестиций[61]. В Китае Государственный совет предлагает китайским компаниям в сфере высоких технологий ставку налога не 25%, а 15%[62]. Правительство Соединенного Королевства включило в бюджет 2016 г. положение о введении налоговых послаблений для микропредприятий, предлагающих интернет-услуги или сдающих недвижимость в аренду с помощью Интернета[63].

Примечания к разделу 5

[1] Математик Эндрю Одлыжко (Andrew Odlyzko) рассматривает вопрос ценообразования и архитектуры Интернета в исторической перспективе. Исходя из сравнения с развитием системы транспорта с древних времен до наших дней, он делает определённые выводы в отношении ценообразования в Интернете. См. подробнее: Odlyzko A (2004) Pricing and Architecture of the Internet: Historical Perspectives from Telecommunications and Transportation. Адрес в Интернете: http://www.dtc.umn.edu/~odlyzko/doc/pricing.architecture.pdf [просмотрено 7 августа 2018 г.].

[2] World Bank (2016) World Development Report 2016: Digital Dividends. Адрес в Интернете: http://www.worldbank.org/en/publication/wdr2016 [просмотрено 7 августа 2018 г.].

[3] The White House (1997) Framework for Global Electronic Commerce. Адрес в Интернете: http://clinton4.nara.gov/WH/New/Commerce/ [просмотрено 7 августа 2018 г.].

[4] WTO (1998) Work programme on electronic commerce. Адрес в Интернете: http://www.wto.org/english/tratop_e/ecom_e/wkprog_e.htm [просмотрено 7 августа 2018 г.].

[5] European Union (2000) Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce). Адрес в Интернете: https://eur-lex.europa.eu/legal-cotent/

EN/ALL/?uri=celex:32000L0031 [просмотрено 7 августа 2018 г.].

[6] PFSweb (2015) B2B eCommerce. Адрес в Интернете: http://alrickbrown.com/wp-content/uploads/PFSweb-B2B-eCommerce-Whitepaper.pdf [просмотрено 7 августа 2018 г.].

[7] WTO (no date) GATT and the Goods Council. Адрес в Интернете: http://www.wto.org/english/tratop_e/gatt_e/gatt_e.htm [просмотрено 7 августа 2018 г.].

[8] WTO (no date) Services trade. Адрес в Интернете: https://www.wto.org/english/tratop_e/serv_e/serv_e.htm [просмотрено 7 августа 2018 г.].

[9] WTO (1994) Agreement on Trade-related Aspects of Intellectual Property Rights. Адрес в Интернете: https://www.wto.org/english/docs_e/legal_e/27-trips_01_e.htm [просмотрено 7 августа 2018 г.].

[10] Хотя мораторий изначально носил «временный» характер, впоследствии он был продлен решением Министерской конференции ВТО. Последний раз такое решение было принято на Министерской конференции в Найроби в декабре 2015 г. с перспективой его очередного рассмотрения на конференции 2017 г. WTO Ministerial Conference (2015) Ministerial Decision of 19 December 2015: WT/MIN(15)42 — WT/l/977. Адрес в Интернете: https://www.wto.org/english/thewto_e/minist_e/mc10_e/l977_e.htm [просмотрено 7 августа 2018 г.].

[11] Подробнее о деятельности ВТО в области электронной коммерции см.: WTO (no date) Electronic commerce. Адрес в Интернете: http://www.wto.org/english/tratop_e/ecom_e/ecom_e.htm [просмотрено 7 августа 2018 г.].

[12] Подробнее о деле между США и Антигуа по вопросу об азартных играх в Интернете см.: http://www.wto.org/english/tratop_e/dispu_e/cases_e/ds285_e.htm [просмотрено 7 августа 2018 г.].

[13] Geneva Internet Platform (2016) Report from WTO Public Forum 2016. Адрес в Интернете: http://digitalwatch.giplatform.org/events/wto-public-forum [просмотрено 7 августа 2018 г.].

[14] Более подробный обзор дискуссий по вопросу электронной коммерции в рамках ВТО см.: Maciel M (2016) E-commerce in the WTO: the next arena of Internet policy discussions. Адрес в Интернете: https://www.diplomacy.edu/blog/e-commerce-wto-next-arena-internet-policy-discussions [просмотрено 7 августа 2018 г.].

[15] UNCITRAL (1996) Model Law on Electronic Commerce. Адрес в Интернете: http://www.uncitral.org/uncitral/en/uncitral_texts/electronic_commerce/1996Model.html [просмотрено 7 августа 2018 г.].

[16] United Nations General Assembly (2005) Resolution A/60/20. United Nations Convention on the Use of Electronic Communications in International Contracts. Адрес в Интернете: http://www.uncitral.org/uncitral/en/uncitral_texts/electronic_commerce/2005Convention.html [просмотрено 7 августа 2018 г.].

[17] ebXML website. Адрес в Интернете: http://www.ebxml.org/ [просмотрено 7 августа 2018 г.].

[18] UNCTAD (no date) Information Economy Report (series). Адрес в Интернете: http://unctad.org/en/Pages/Publications/InformationEconomyReportSeries.aspx [просмотрено 7 августа 2018 г.].

[19] UNCTAD (no date) eTrade for All: Unlocking the Potential of E-Commerce in Developing Countries. Адрес в Интернете: http://unctad.org/en/Pages/DTL/STI_and_ICTs/eTrade-for-All.aspx [просмотрено 7 августа 2018 г.].

[20] OECD (1998) Action Plan for Electronic Commerce. Адрес в Интернете: http://www.oecd.org/officialdocuments/publicdisplaydocumentpdf/?cote=SG/EC(98)9/FINAL&docLanguage=En [просмотрено 7 августа 2018 г.].

[21] Teleanu S (2016) Digital policy issues emphasised at the G20 Leaders' Summit. Адрес в Интернете: https://www.diplomacy.edu/blog/digital-policy-issues-emphasised-g20-leaders'-summit [просмотрено 7 августа 2018 г.].

[22] APEC (no date) Paperless Trading Individual Action Plan. Адрес в Интернете: https://www.apec.org/ Groups/Committee-on-Trade-and-Investment/Electronic-Commerce-Steering-Group/Paperless-Trading-Individual-Action-Plan.aspx [просмотрено 7 августа 2018 г.].

[23] COMESA (2010) Model Law on Electronic Transactions and Guide to enactment. Адрес в Интернете: http://programmes.comesa.int/attachments/article/166/COMESA%20Model%20Law%20and%20%20Guide%20to%20Enactment%20(fin).pdf [просмотрено 7 августа 2018 г.].

[24] Net Market Share (2016) Market Share Statistics for Internet Technologies. Адрес в Интернете: https://www.netmarketshare.com/search-engine-market-share.aspx?qprid=4&qpcustomd=0 [просмотрено 7 августа 2018 г.].

[25] Thuy T, Nguyen T and Armitage GJ. Evaluating Internet Pricing Schemes: A Three-Dimensional Visual Model // ETRI Journal. 2005. 27(1) pp. 64—74. Адрес в Интернете: https://onlinelibrary.wiley.com/doi/epdf/10.4218/etrij.05.0104.0061 [просмотрено 7 августа 2018 г.].

[26] Hayel Y, Maille P and Tuffin B (2005) Modelling and analysis of Internet pricing: introduction and challenges. In Proceedings of the International Symposium on Applied Stochastic Models and Data Analysis (ASMDA), Brest, France. Адрес в Интернете: http://conferences.telecom-bretagne.eu/asmda2005/IMG/pdf/proceedings/1389.pdf [просмотрено 7 августа 2018 г.].

[27] European Commission (2016) A European agenda for the collaborative economy. Адрес в Интернете: http://ec.europa.eu/DocsRoom/documents/16881 [просмотрено 7 августа 2018 г.].

[28] Цит. по Holland K, Cortese A. The future of money: e-cash could transform the world's financial life // Business Week, 12.06.1995. p. 66.

[29] См.: Olson T. Higher costs, new laws mean no more free rides on some bank services, accounts // Pittsburgh Tribune-Review, 01.04.2012. Адрес в Интернете: http://triblive.com/x/pitts-burghtrib/business/s_789300.html [просмотрено 7 августа 2018 г.].

[30] Basel Committee on Banking Supervision (1998) Risk Management for Electronic Banking and Electronic Money Activities. Basel March 1998. Адрес в Интернете: http://www.bis.org/publ/bcbs35.pdf [просмотрено 7 августа 2018 г.]. Окончательная версия опубликована в 2003 г. Адрес в Интернете: http://www.bis.org/publ/bcbs98.htm [просмотрено 7 августа 2018 г.].

[31] Kamberi A (2014) Cryptocurrencies and Bitcoin. Адрес в Интернете: https://www.diplomacy.edu/blog/cryptocurrencies-and-bitcoin [просмотрено 7 августа 2018 г.].

[32] European Central Bank (2012) Virtual currency schemes. Адрес в Интернете: https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes201210en.pdf [просмотрено 7 августа 2018 г.].

[33] European Banking Authority (2014) EBA Opinion on 'virtual currencies'. Адрес в Интернете: https://www.eba.europa.eu/documents/10180/657547/EBA-Op-2014-08+Opinion+on+Virtual+Currencies.pdf [просмотрено 7 августа 2018 г.].

[34] The Register. China to set up its own virtual currency. 22.01.2016. Адрес в Интернете: https://www.theregister.co.uk/2016/01/22/china-virtual-currency-risks/ [просмотрено 7 августа 2018 г.].

[35] He D et al. (2016) Virtual Currencies and Beyond: Initial Considerations. International Monetary Fund Staff Discussion Note 16/03. Адрес в Интернете: https://www.imf.org/external/pubs/ft/sdn/2016/sdn1603.pdf [просмотрено 7 августа 2018 г.].

[36] Soxlaw (no date) A guide to the Sarbanes Oxley Act. Адрес в Интернете: http://www.soxlaw.com/ [просмотрено 7 августа 2018 г.].

[37] European Union (2009) Directive 2009/110/EC of the European Parliament

and of the Council of 16 September 2009 on the taking up, pursuit and prudential supervision of the business of electronic money institutions amending Directives 2005/60/EC and 2006/48/EC and repealing Directive 2000/46/EC. Адрес в Интернете: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:267:0007:0017:EN:PDF [просмотрено 7 августа 2018 г.].

[38] Базельский комитет по банковскому надзору расположен в Банке международных расчетов (БМР). Комитет выпускает «Обзор развития сегмента электронных денег, платежей в Интернете и мобильных платежей» (Survey of Developments in Electronic Money and Internet and Mobile Payments). Адрес в Интернете: http://www.bis. org/publ/cpss62.pdf [просмотрено 7 августа 2018 г.].

[39] Richtel M. PayPal and New York in Accord on Gambling // The New York Times, 22.08.2002. Адрес в Интернете: http://www.nytimes.com/2002/08/22/business/technology-paypal-and-new-york-in-accord-on-gambling.html?src=pm [просмотрено 7 августа 2018 г.].

[40] Takemoto Y, Knight S. Mt. Gox file for bankruptcy, hit with lawsuit // Reuters, 28.02.2014. Адрес в Интернете: https://www.reuters.com/article/us-bitcoin-mtgox-bankruptcy/mt-gox-files-for-bankruptcy-hit-with-lawsuit-idUSBREA1R0FX20140228 [просмотрено 7 августа 2018 г.].

[41] Federal Bureau of Investigation (2014) Press Release: Operator of Silk Road 2.0 Website Charged in Manhattan Federal Court. Адрес в Интернете: https://www.fbi.gov/contact-us/field-offices/newyork/news/press-releases/operator-of-silk-road-2.0-website-charged-in-manhattan-federal-court [просмотрено 7 августа 2018 г.].

[42] Baron J et al. (2015) National Security Implications of Virtual Currency. Examining the Potential for Non-state Actor Deployment. Rand Corporation. Адрес в Интернете: http://www.rand.org/content/dam/rand/pubs/research_reports/RR1200/RR1231/RAND_RR1231.pdf [просмотрено 7 августа 2018 г.].

[43] European Commission (2016) Proposal for a Directive of the European Parliament and of the Council amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing and amending Directive 2009/101/ EC. Адрес в Интернете: http://ec.europa.eu/justice/criminal/document/files/aml-directive_en.pdf [просмотрено 7 августа 2018 г.].

[44] OECD (1999) Guidelines for Consumer Protection in the Context of Economic Commerce. Адрес в Интернете: http://www.oecd.org/internet/consumer/oecdguidelinesforconsumerprotectioninthecontextofelectroniccommerce1999.htm [просмотрено 7 августа 2018 г.].

[45] OECD (2003) Guidelines for Protecting Consumers from Fraudulent and Deceptive Commercial Practices. Адрес в Интернете: http://www.oecd-ilibrary.org/industry-and-services/oecd-guidelines-for-protecting-consumers-from-fraudulent-and-deceptive-commercial-practices-across-borders_9789264103573-en-fr [просмотрено 7 августа 2018 г.].

[46] European Union (2001) Regulation (EC) No 44/2001 (Brussels I Regulation). Адрес в Интернете: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32001R0044:en:HTML [просмотрено 7 августа 2018 г.].

[47] European Union (2012) Regulation (EU) No 1215/2012 (Recast Brussels I Regulation). Адрес в Интернете: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2012:351:0001:0032:en:PDF [просмотрено 7 августа 2018 г.].

[48] Soete L, Weel B (1999) Cybertax. Maastricht Economic Research Institute on Innovation and Technology (MERIT), Maastricht University. Адрес в Интернете: http://www.merit.unu.edu/publications/rmpdf/1998/rm1998-020.pdf [просмотрено 7 августа 2018 г.].

[49] Collin P, Colin N (2013) Mission d'expertise sur la fiscalité de l'économie numérique. Адрес в Интернете: http://www.economie.gouv.fr/files/rapport-fiscalite-du-numerique_2013.pdf [просмотрено 7 августа 2018 г.].

[50] В качестве примеров публикаций, в которых рассматривается вопрос налогообложения применительно в Интернету можно привести : EY (2015) The dawning of digital economy taxation. Адрес в Интернете: http://www.ey.com/Publication/vwLUAs-sets/ey-the-dawning-of-digital-economy-taxation/$FILE/ey-the-dawning-of-digital-economy-taxation.pdf [просмотрено 7 августа 2018 г.]; Andes S, Atkinson R (2013) A Policymakers' Guide to Internet Tax. Адрес в Интернете: http://www2.itif.org/2013-policymakers-guide-internet-tax.pdf [просмотрено 7 августа 2018 г.]; OECD (2015) Addressing the Tax Challenges of the Digital Economy. Адрес в Интернете: http://www.oecd-ilibrary.org/taxation/addressing-the-tax-challenges-of-the-digital-economy_9789264218789-en [просмотрено 7 августа 2018 г.]. С другими ресурсами по этому вопросу можно ознакомиться в GIP Digital Watch observatory (no date). Taxation. Адрес в Интернете: https://dig.watch/issues/taxation [просмотрено 7 августа 2018 г.].

[51] Phillips Erb K. Congress Makes Internet Access Tax Ban Permanent // Forbes, 11.02.2016. Адрес в Интернете: http://www.forbes.com/sites/kellyphillipserb/2016/02/11/congress-makes-internet-access-tax-ban-permanent/#a403c12380a3 [просмотрено 7 августа 2018 г.].

[52] К Оттавским принципам относятся нейтральность, эффективность и справедливость. OECD (2003) Implementation of the Ottawa Taxation Framework Conditions. The 2003 Report. Адрес в Интернете: http://www.oecd.org/tax/administration/20499630.pdf [просмотрено 7 августа 2018 г.].

[53] European Commission (2014) Commission Expert Group on Taxation of the Digital Economy. Brussels: European Commission, p. 5. Адрес в Интернете: https://ec.europa.eu/taxation_customs/sites/taxation/files/resources/documents/taxation/gen_info/good_governance_matters/digital/report_digital_economy.pdf [просмотрено 7 августа 2018 г.].

[54] Russia State Duma passes Google Tax Law // The Moscow Times, 15.06.2016. Адрес в Интернете: https://themoscowtimes.com/articles/russia-state-duma-passes-google-tax-law-53310 [просмотрено 7 августа 2018 г.].

[55] Revanna H. Govt notifies 6% equalization tax on online advertisements // IBT, 31.05.2016. Адрес в Интернете: http://www.ibtimes.co.in/govt-notifies-6-equalisation-tax-digital-ads-take-effect-june-1-680785 [просмотрено 7 августа 2018 г.].

[56] Google, Facebook, eBay and other tech firms targeted by new Israeli tax rules // The Guardian. 12.04.2016. Адрес в Интернете: https://www.theguardian.com/technology/2016/apr/11/google-facebook-ebay-tech-firms-israel-tax [просмотрено 7 августа 2018 г.].

[57] Indonesia says Internet giants need to pay tax or face blockages // Reuters, 29.02.2016. Адрес в Интернете: http://www.reuters.com/article/us-indonesia-tax-internet-idUSKCN0W20QM [просмотрено 7 августа 2018 г.].

[58] Italian tax police believe Google evaded 227 million euros in taxes: sources // Reuters, 28.01.2016. Адрес в Интернете: http://www.reuters.com/article/us-google-italy-tax-idUSKCN0V614L [просмотрено 7 августа 2018 г.].

[59] Robertson J. Google tax row: what's behind the deal // BBC News, 28.01.2016. Адрес в Интернете: http://www.bbc.com/news/business-35428966 [просмотрено 7 августа 2018 г.].

[60] Google's Paris HQ raided in tax probe // BBC, 24.05.2016. Адрес в Интернете: http://www.bbc.com/news/business-36370628 [просмотрено 7 августа 2018 г.].

[61] McIntyre RS et al. (2015) Offshore Shell Games 2015. Адрес в Интернете: http://www.uspirg.org/sites/pirg/files/reports/USP%20ShellGames%20Oct15%201.3.pdf [просмотрено 7 августа 2018 г.].

[62] Aulakh G. Budget 2016: Telecom Ministry seeks 10-year tax holiday for Make in India drive // Economic Times, 15.02.2016. Адрес в Интернете: http://economictimes.indiatimes.com/industry/telecom/budget2016-telecom-ministry-seeks-10-year- tax-holiday-for-make- in-in-dia-drive/articleshow/50988028.cms

[просмотрено 7 августа 2018 г.].

[63] Ren. Beijing offers tax concessions to hi-tech companies // South China Morning Post, 14.02.2016. Адрес в Интернете: https://www.scmp.com/news/china/policies-politics/article/1913172/beijing-offers-tax-concessions-high-tech-companies [просмотрено 7 августа 2018 г.].

[64] Rampen J. Airbnb hosts get first £1,000 tax free after Budget 2016 shake up // Mirror, 16.03.2016. Адрес в Интернете: https://www.mirror.co.uk/money/airbnb-hosts-first-1000-tax-7568083 [просмотрено 7 августа 2018 г.].

Раздел 6

Вопросы развития

Вопросы развития

На протяжении всей истории технологии играли роль основного двигателя социального прогресса (колесо, сельскохозяйственный инструмент, типографический станок, телеграф и т. д.). Совершенствование технологий способствует развитию общества. Современная идея о взаимосвязанности общественного и технического прогресса уходит корнями в эпоху Просвещения, в период развития науки и техники XVI—XX веков. Именно тогда зародилась мысль о роли технологий в деле общественного развития и решении социальных проблем, проще говоря, техническом прогрессе как инструменте развития.

Технологии также лежат в основе повестки ООН в области развития, которая начала формироваться после Второй мировой войны в целях содействия развитию новых независимых государств из числа бывших колоний. И хотя технический прогресс позволил сократить масштабы бедности и повысить благосостояние, он имел определенные ограничения. Социально-экономическое развитие представляет собой гораздо более сложный процесс по сравнению с техническим прогрессом. Например, чтобы использовать новые технологии, требуются образование и подготовка людских ресурсов, а также регламенты и общественные институты, которые должны помочь обществу адаптироваться к изменениям без ущерба для его культурной идентичности. Кроме того, социальные изменения являются более длительным процессом по сравнению с разработкой новых технологий.

> Коммунизм и провал модели развития на основе технического прогресса
>
> Крах коммунистической системы в конце XX века нанес сокрушительный удар по модели развития, основанной на техническом прогрессе. Для Советского Союза и стран Восточного блока наука и техника были важнейшими приоритетами. Несмотря на первоначальное отставание и ограниченность ресурсов, Советский Союз догнал западные страны по многим направлениям науки и техники. Особых успехов советские ученые достигли в сфере спутниковых и военных технологий. Однако научно-технический прогресс не смог решить все проблемы социально-экономического развития, что привело к распаду системы. В числе целого ряда причин, способствовавших краху, в том числе идеологического и структурного характера, многие из которых пока не изучены, одну можно назвать уже сейчас — это излишняя зависимость от технических решений и технологий.

Наступление цифрового века в очередной раз подтвердило правильность тезиса о том, что технологии являются движущей силой развития. С появлением Интернета существенно расширились возможности отдельного человека, открылись перспективы для реализации проектов глобального уровня. Однако, как отмечалось в целом ряде исследований и обзоров[1], прямой зависимости между техническим прогрессом и развитием общества не существует. В настоящем разделе мы рассмотрим сложное взаимодействие между технологиями и обществом, включая следующие вопросы:

- Способствует ли Интернет углублению или преодолению разрыва между развитыми и развивающимися странами?
- Как и когда развивающиеся страны смогут достичь уровня информационных технологий промышленноразвитых стран?
- Каким образом Интернет и цифровые технологии могут содействовать устойчивому развитию?

В данном разделе речь пойдет собственно о вопросах развития, которые также присущи многим спорам о регулировании цифровых технологий. Почти каждый аспект управления Интернетом тем или иным образом связан с развитием. Например:

- наличие телекоммуникационной инфраструктуры является основой для предоставления доступа в Интернет, первой предпосылкой для преодоления разрыва в цифровых технологиях;
- текущая экономическая модель доступа к Интернету возлагает несоразмерно тяжелое бремя на развивающиеся страны, которым приходится оплачивать доступ к интернет-магистралям, расположенным в развитых странах;
- электронная торговля дает компаниям из развивающихся стран возможность выйти на международные рынки, но для этого они должны иметь доступ к Интернету.

Каким образом ИКТ влияют на развитие общества?

В международную повестку вопросы развития цифровых технологий появились в начале 2000-х гг. в рамках процесса WSIS. В первой резолюции Генеральной Ассамблеи ООН по тематике WSIS подчеркивался вклад Всемирной встречи на высшем уровне по вопросам информационного общества в «содействие развитию, в особенности в том, что касается доступа к технологиям и их передаче»[2]. Саммит ставил целью преодоление разрыва в цифровых технологиях между развитыми и развивающимися странами и реализацию программы Цели развития тысячелетия (ЦРТ). В Женевской декларации и плане действий WSIS подчеркивался приоритет развития в свете Декларации тысячелетия ООН[3], отмечалась важность обеспечения доступа всех стран к информации, знаниям и технологиям связи в целях содействия развитию. В контексте ЦРТ[4] важная роль отводилась форуму WSIS. В Тунисской программе для информационного общества также рассматривались вопросы развития ИКТ, при этом особое внимание уделялось разработке финансовых механизмов для решения существующих проблем. Десятилетие спустя в статье 5 итогового документа совещания высокого уровня Генеральной Ассамблеи, посвященного общему обзору хода осуществления решений Всемирной встречи на высшем уровне по вопросам информационного общества, была установлена взаимосвязь между деятельностью WSIS и Целями устойчивого развития (ЦУР)[5]:

> *Мы признаем, что расширение возможностей сетевого подключения, масштабов инновационной деятельности и доступа сыграли исключительно важную роль в достижении прогресса в реализации целей в области развития, сформулированных в Декларации тысячелетия, и призываем обеспечить тесную увязку деятельности по выполнению решений Всемирной встречи на высшем уровне по вопросам информационного общества с деятельностью по осуществлению Повестки дня в области устойчивого развития на период до 2030 года, обращая особое внимание на роль информационно-коммуникационных технологий в достижении целей в области устойчивого развития и ликвидации нищеты и отмечая, что доступ к таким технологиям сам становится одним из показателей развития и одной из его целей[6].*

Интернет напрямую упоминается в Цели 9 (c) ЦУР, которая предусматривает: «Существенно расширить доступ к информационно-коммуникационным технологиям и стремиться к обеспечению всеобщего и недорогого доступа к Интернету в наименее развитых странах к 2020 году». Кроме того, в рамках ЦУР был создан Механизм содействия развитию технологий, в задачи которого входит рассмотрение возможностей применения достижений научно-технической мысли и инноваций для осуществления ЦУР[7].

Вопросы развития также затрагивались в рамках форумов по управлению Интернетом, начиная с первой встречи в Афинах (2006 г.) до последнего форума 2015 г., темой которого стала «Эволюция управления Интернетом: содействие устойчивому развитию».

Каким образом ИКТ влияют на развитие общества?

После принятия ЦУР было разработано большое количества программ, в которых анализировались соответствующая тематика и методы использования ИКТ в целях развития.

В качестве примера можно привести программу ЮНКТАД «Информационно-коммуникационные технологии на службе развития» (ICT for Development)[8], матрицу WSIS по ЦУР, в которой рассматриваются пути использования ИКТ для достижения целей устойчивого развития[9], а также материалы Форума WSIS 2015 и 2016 гг., посвященные вопросам взаимосвязи между ЦУР и ИКТ[10]. Наконец, Комиссия по науке и технике в целях развития (КНТР/CSTD) в межсессионный период 2015–2016 гг. в рамках темы «Цифровое развитие» рассмотрела возможные последствия, которые может иметь внедрение новейших цифровых технологий (включая Интернет вещей, интернет-образование, 3D-печать, цифровую автоматизацию и т. п.) для

экономики, общества и окружающей среды в долгосрочной перспективе.

Комиссия разработала ряд рекомендаций, в которых правительствам предлагалось принять необходимые меры для поддержки новых технологий и использования открывающихся возможностей, создания благоприятной среды для развития цифровых технологий с упором на наращивание человеческого капитала, ИКТ и связанной с ними инфраструктуры и разработку нормативно-правовой базы.

В «Докладе о мировом развитии 2016: Цифровые дивиденды» (World Development Report 2016: Digital Dividends)[11] Всемирный банк призывает участников дискуссии воздерживаться от упрощенного подхода к взаимосвязи ИКТ и развития в смысле обязательной увязки роста с техническим прогрессом. Авторы обращают внимание на то, что Интернет (и цифровые технологии в целом) обладают потенциалом для стимулирования роста и развития, однако неравенство и отставание продолжают сохраняться и углубляться как на глобальном, так и внутреннем уровнях.

Цифровые технологии выгодны людям (доступ к информации, трудоустройство и другие возможности), компаниям (рост производительности и товарооборота, развитие конкуренции и инноваций), а также властям (повышение качества государственных услуг и налаживание более эффективных каналов связи с населением). Однако для обеспечения глобального экономического роста скорость распространения и равномерность распределения этих преимуществ оказались недостаточны. Чтобы преодолеть эту проблему, Всемирный банк в своем докладе дает две основные рекомендации: преодолеть цифровой разрыв и принять серию взаимодополняющих мер, которые бы позволили физическим лицам, компаниям и государственным органам воспользоваться всеми преимуществами цифровых технологий. Такие меры, так называемые «аналоговые надстройки», предусматривают развитие конкуренции и содействие инновациям в частном секторе, а также образовательные программы и подготовку кадров в области компьютерной грамотности, повышение потенциала и обеспечение подотчетности государственных органов в части применения технологий, принятия решений и предоставления государственных услуг. Кроме того, даже при наличии всех указанных составляющих основная проблема состоит

в том, как и когда их следует использовать и в каком соотношении.

Доклад подтверждает старую истину о том, что технологии не могут быть нейтральными. История человечества изобилует примерами того, как технологии открывали новые возможности перед одними людьми, оставляя в стороне другие группы и страны. Интернет в этом отношении не исключение. На всех уровнях, от отдельных пользователей до межгосударственных отношений, все используют потенциал цифровых технологий по-разному. Ситуация с распределением богатства и власти изменилась кардинальным образом.

В целом, ИКТ оказывают неоднозначное воздействие на различные сферы социально-экономического развития. С ростом интереса к социально-экономическим аспектам информационно-коммуникационных технологийпоявляется возможность лучше понять механизм воздействия различных ИКТ на общество и определить методы использования ИКТ в целях социально-экономического развития.

Разрыв в цифровых технологиях

Разрыв в цифровых технологиях («цифровой разрыв») можно определить как водораздел между теми, кто в силу технических, политических, социальных или экономических причин может использовать Интернет/ ИКТ, и теми, кто такой возможности не имеет. Согласно определению ОЭСР, под разрывом в цифровых технологиях понимается «разрыв между физическими лицами, домохозяйствами, компаниями и географическими областями с разным уровнем социально-экономического развития с точки зрения доступа к информационно-телекоммуникационным технологиям (ИКТ) и использования ими Интернета в различных видах деятельности»[12].

Разрыв в цифровых технологиях является отражением социально-экономического неравенства в области образования, здравоохранения, материального положения, условий проживания, трудоустройства, санитарии и питания. Соответственно, цифровой разрыв не следует считать обособленной проблемой.

Для объяснения соотношения возможностей, которые открываются с появлением новых технологий, с их восприятием и освоением, можно обратиться к разработанной Эвереттом Роджерсом схеме диффузии инноваций (рис. 21). Такой подход позволяет выделить несколько категорий людей — от инноваторов до отстающих — с точки зрения скорости освоения ими новых технологий.

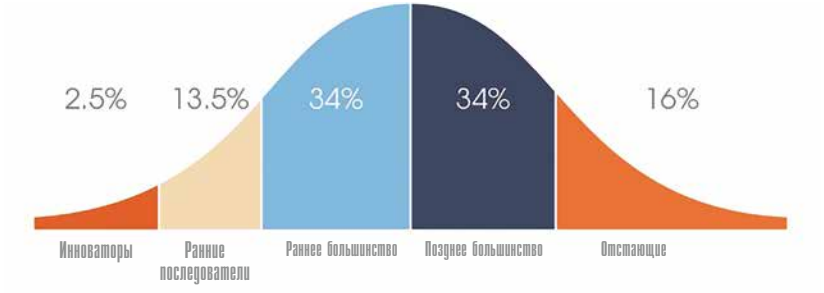


Рисунок 21. Диффузия инноваций Эверетта Роджерса.

Диффузия Роджерса позволяет объяснить существование разрыва в цифровых технологиях на различных уровнях: внутри стран и между странами, между городским и сельским населением, между молодыми и старыми, мужчинами и женщинами, в зависимости от уровня образования и так далее.

Увеличивается ли цифровой разрыв?

Интернет/ИКТ развиваются намного быстрее, чем другие области (например, сельское хозяйство или медицина), и в силу того, что в развитых странах, в отличие от развивающихся, созданы все условия для эффективного использования достижений ИКТ. Поэтому создается впечатление, что «цифровой разрыв» увеличивается постоянно и с довольно внушительной скоростью. Данная точка зрения представлена во многих авторитетных источниках, например в Докладах о развитии человека (Human Development Reports) Программы развития ООН и в докладах Международной организации труда об уровне занятости.

Существует противоположная точка зрения, согласно которой статистика, оценивающая разрыв в цифровых технологиях, часто обманчива, и «цифровой разрыв» на деле отнюдь не увеличивается, а наоборот постепенно сходит на нет[13]. В соответствии с этой позицией традиционное внимание к количеству компьютеров, веб-сайтов и пропускной способности нужно заменить оценкой воздействия, которое оказывают Интернет/ИКТ на общество в развивающихся странах. Примером могут послужить успехи Бразилии, Китая и Индии в области цифровых технологий.

В действительности, поскольку окружающая нас реальность постоянно меняется, критерии оценки разрыва в цифровых технологиях находятся в постоянном движении и становятся все более сложными. В используемых сегодня оценках учитываются такие аспекты, как готовность ИКТ и общее влияние ИКТ на общество. Всемирный экономический форум разработал Индекс сетевой готовности (Networked Readiness Index — NRI) для измерения уровня развития Интернета в странах мира[14]. Этот инструмент позволяет по-новому взглянуть на то, как решить проблему разрыва в цифровых технологиях.

Всеобщий доступ

Помимо «цифрового разрыва», другой часто упоминаемой концепцией в дискуссиях о развитии является всеобщий доступ, то есть доступ для всех. Хотя этот аспект должен быть краеугольным камнем любой политики в отношении информационных технологий, существуют различные мнения и различное понимание сущности и масштаба политики всеобщего доступа. Вопрос обеспечения всеобщего доступа к Интернету по всему миру остается открытым. Во многом его решение зависит от того, готовы ли развитые страны обеспечить достижение этой цели за свой счет, а также от нормативной среды в развивающихся странах. Тем не менее во многих международных документах, включая итоговые документы WSIS+10, подчеркивается важность обеспечения всеобщего доступа к Интернету.

В отличие от международного уровня, в некоторых странах концепция всеобщего доступа подробно разработана с экономической и правовой точек зрения. Предоставление всем гражданам доступа к услугам связи было положено в основу политики США в области телекоммуникаций. В результате появилась хорошо развитая система различных политических и фи-

нансовых механизмов, целью которых является финансирование доступа в отдаленных регионах и областях, где связь дорога. Субсидии предоставляются регионами с низкой стоимостью подключения услуг связи — главным образом, большими городами. ЕС также принял ряд конкретных мер, направленных на обеспечение всеобщего доступа путем проведения политики по предоставлению всем гражданам доступа к основным услугам связи, включая доступ к Интернету, и введение в действие соответствующих нормативно-правовых актов[15]. В сентябре 2016 г. Европейская комиссия выступила с предложением разработать Европейский кодекс электросвязи, в рамках которого на уровне ЕС пересмотреть понятие универсальной услуги путем отказа от устаревших видов обслуживания (общественных таксофонов) и концентрации внимания на широкополосной связи[16].

В последнее время многие интернет-компании занимаются вопросами расширения доступа в Интернет. Они стремятся использовать огромный коммерческий потенциал регионов, где еще нет широкополосного доступа. Такие инициативы предусматривают либо создание традиционной кабельной инфраструктуры, либо более современные методы, например использование для распространения интернет-сигнала беспилотных летающих устройств (Facebook) and аэростатов (Google).

Подробнее об инфраструктуре Интернета, включая инновационные решения, см. ***Раздел 2.***

Стратегии преодоления «цифрового разрыва»

Как отмечается в докладе Совета по правам человека ООН[17], учитывая многогранность проблемы доступа, которая может охватывать широкий спектр вопросов от подключения до контента, преодоление разрыва в цифровых технологиях на глобальном, региональном и национальном уровнях представляется сложным и долгосрочным процессом, который предусматривает разработку соответствующих мер и участие множества заинтересованных сторон (органов власти, межправительственных организаций, частного сектора и т. п.).

Развитие телекоммуникаций и инфраструктуры Интернета

Одним из основных препятствий с точки зрения преодоления разрыва в цифровых технологиях является доступ к инфраструктуре Интернета. Говоря о доступе к Интернету в развивающихся странах, следует обратить внимание на два важных момента: во-первых, доступ к международным опорным сетям Интернета, и, во-вторых, каналы связи между развивающимися странами.

Возможность получения доступа к опорным сетям Интернета зависит от наличия подводных оптоволоконных кабелей, которые соединяют континенты. В силу географических факторов и сравнительно невысокой стоимости их прокладки, основные межконтинентальные кабели проложены по дну океана. В настоящий момент на эти кабели приходится более 90% глобального интернет-трафика.

Подробнее о магистральных кабелях см. ***Раздел 2.***

Наряду с подводными кабелями планируется прокладка дополнительных наземных межконтинентальных магистралей. Например, в рамках инициативы «Один пояс, один путь» рассматривается возможность соединения Азии и Европы посредством наземного межконтинентального кабеля. Существуют и другие проекты по прокладке таких кабелей.

В долгосрочной перспективе переход на наземные интернет-коммуникации может оказать существенное воздействие на развитие евразийских стран, лишенных выхода к морю. Доступ в Интернет станет для них проще и дешевле по сравнению с нынешней ситуацией, когда подключение к подводным кабелям обходится очень дорого.

Еще одним вариантом решения проблемы доступа считается создание точек обмена интернет-трафиком, благодаря которым обмен локальным интернет-трафиком может осуществляться внутри страны. Например, без таких точек переписка по электронной почте между пользователями двух разных операторов в одной стране будет пересылаться через серверы, расположенные за рубежом. Точки обмена интернет-трафиком представляют собой технические комплексы для осуществления межоператорского обмена IP-трафиком на основе пиринга (бесплатно). Как правило,

такие точки создаются для обмена трафиком в пределах небольших территорий (города, региона или страны).

Однако во многих развивающихся странах точек обмена интернет-трафиком пока нет, и значительные объемы внутреннего межпользовательского трафика передаются с использованием зарубежных серверов. Это приводит к увеличению объема международного интернет-трафика из развивающихся стран, и, соответственно, стоимости интернет-услуг. Разработан ряд программ по созданию точек обмена интернет-трафиком в развивающихся странах[18]. Так, существенные успехи достигнуты в рамках проекта Африканского союза African Internet eXchange System (AXIS) по созданию точек обмена интернет-трафиком в Африке.

Еще одной важной проблемой является развитость коммуникационной сети в развивающихся странах. Когда-то большинство интернет-пользователей жили в крупных городах, тогда как в сельской местности Интернета не было. С развитием мобильной телефонии и беспроводной связи ситуация стала меняться.

Беспроводные коммуникации могут помочь решить проблему развития традиционной инфраструктуры наземных коммуникаций (избавить от необходимости прокладки кабелей через огромные расстояния многих азиатских и африканских стран). В данном контексте огромное значение имеет политика по распределению радиочастотного спектра, которая должна быть направлена на обеспечение доступности частот и их эффективного использования. Таким способом можно преодолеть проблему «последней мили» (местной линии связи) — одну из основных преград на пути развития Интернета. Однако существует мнение, что мобильные технологии следует рассматривать в качестве не универсального, а временного решения, когда речь идет о подключении к Интернету больших территорий, лишенных других средств доступа. Сторонники такой позиции утверждают, что радиочастотный спектр имеет физические ограничения, например по количеству устройств, подключенных к беспроводной сети[19].

Традиционно инфраструктурные аспекты цифрового разрыва находятся в центре внимания Международного союза электросвязи (МСЭ) и его Сектора развития электросвязи (ITU-D).

Кто должен платить за трафик между развивающимися и развитыми странами?

При отправке письма по электронной почте конечным пользователем из Африки кому-нибудь в Европе, США или Китае, затраты по оплате международного соединения с магистральными линиями связи через основные сетевые центры в Европе, Северной Америке или Азии возлагаются на африканского интернет-провайдера. Однако при отправке письма по электронной почте конечным пользователем из Европы в Африку, африканский интернет-провайдер все равно платит за международный трафик, то есть, в конечном счете, эти затраты перекладываются на конечных пользователей в Африке, которым приходится мириться с более высокой абонентской платой за входящий и исходящий трафик. Дело в том, что интернет-провайдеры развивающихся стран сталкиваются с трудностями при заключении соглашений о долевом распределении расходов на пиринг с крупными иностранными провайдерами из-за небольшой абонентской базы. В конечном счете, такие интернет-провайдеры действуют в качестве дистрибьюторов, приобретающих право доступа у иностранных провайдеров для его дальнейшей продажи потребителям на внутреннем рынке, что ведет к росту цен[20].

Основной довод в спорах об изменении существующей системы оплаты услуг Интернета основан на аналогии с оплатой услуг телефонии, где стоимость делится поровну между конечными точками коммуникации. Однако ведущий научный сотрудник APNIC Джефф Хастон указывает, что эта аналогия не имеет под собой оснований[21]. В системе традиционной телефонии существует лишь одна оплачиваемая услуга, а именно телефонный звонок, делающий возможным общение между людьми, находящимися возле своих телефонных аппаратов. В Интернете нельзя выделить единственную оплачиваемую услугу; в нем есть только пакеты данных, передаваемые по различным маршрутам внутри сети. Это фундаментальное различие делает вышеуказанную аналогию неприменимой и является основным источником проблем при попытках применить модель оплаты телефонных услуг к Интернету.

По инициативе МСЭ были начаты переговоры о возможном усовер-

шенствовании существующей системы покрытия затрат на Интернет, цель которых — более сбалансированное распределение стоимости доступа в Интернет. В 2008 г. МСЭ приняло Рекомендацию D.50, в которой изложены предложения, касающиеся заключения коммерческих соглашений по международным интернет-соединениям с учетом необходимости компенсации стоимости трафика, маршрутизации, стоимости передачи данных и так далее. Однако эти предложения не имели практического эффекта из-за противодействия со стороны развитых стран и телекоммуникационных операторов. Переговоры по этому вопросу на межгосударственном уровне малоэффективны, поскольку такие соглашения обычно заключаются между частными телекоммуникационными операторами и носят конфиденциальный характер. В этой связи в 2013 г. МСЭ принял Приложение к Рекомендации D.50, в котором приведены альтернативные способы снижения стоимости международного трафика, включая использование точек обмена интернет-трафиком, прокладку подводных кабелей и развитие местного контента[22].

Финансовая поддержка

В рамках процесса WSIS стала очевидной важность финансовой поддержки для преодоления разрыва в цифровых технологиях. Так, поступило предложение создать под эгидой ООН Фонд цифровой солидарности для оказания технически отсталым странам помощи в создании телекоммуникационной инфраструктуры. Хотя Глобальный фонд цифровой солидарности официально действует с марта 2005 г., развитые страны не проявляют интереса к сотрудничеству и отдают предпочтение прямым инвестициям вместо финансирования централизованного фонда развития.

Развивающиеся страны получают финансовую поддержку по различным каналам, включая двусторонние и многосторонние агентства содействия развитию (например, Программу развития ООН или Всемирный банк), а также через региональные инициативы по развитию и региональные банки. В рамках МСЭ был создан Фонд развития ИКТ – фонд посевных инвестиций, который должен содействовать развитию путем реализации проектов в области ИКТ на национальном, региональном и глобальном уровнях. На третьей Международной конференции по финансированию развития была принята Аддис-Абебская программа действий, которая была поддержана Генеральной Ассамблеей ООН в июле 2015 г. В этом документе изложен глобальный подход к финансированию устойчивого развития по всем целям устойчивого развития, включая привлечение финансовых средств для устранения цифрового разрыва[23].

По мере либерализации рынка телекоммуникаций соответствующая инфраструктура все больше создается за счет прямых иностранных инвестиций. Перенасыщенный рынок телекоммуникационных услуг в развитых странах побуждает многие международные телекоммуникационные компании связывать свои будущие планы с рынками развивающихся стран.

Навыки и компетенции для обеспечения эффективного доступа

Подключение к Интернету является неотъемлемым условием доступа в сеть. При этом многие полагают, что определение понятия «доступ» должно быть расширено и учитывать качество доступа. В итоговом документе WSIS+10 отмечается, что «суть понятия «доступ» меняется с ростом внимания к таким показателям качества доступа, как скорость, стоимость, язык, местный контент и доступность для людей с ограниченными возможностями».

Наличие инфраструктуры не имеет значения, если люди не обладают средствами (устройства) и знаниями (компьютерная грамотность) для получения доступа и использования Интернета в своих интересах. Вклад развивающихся стран, особенно африканских, в копилку знаний об интернет-технологиях пока остается весьма скромным. Этот разрыв между развитыми и развивающимися странами отражает проблему даже более наглядно, чем ситуация с интернет-доступом. Например, по созданию информационного наполнения для Wikipedia один Гонконг опережает весь африканский континент, хотя в Африке в 50 раз больше интернет-пользователей[24].

Социокультурными аспектами и методикой преодоления разрыва в цифровых технологиях занимаются ряд организаций и инициатив. На-

пример, такие международные программы и организации как One Laptop per Child, Close the Gap и Computer Aid International поставляют в бедные общины развивающихся стран недорогие отремонтированные компьютеры. Инициативы по обеспечению населения недорогими устройствами реализуются и на локальном уровне. Так, в Сингапуре действует программа, в рамках которой студентам и людям с ограниченными возможностями из малоимущих семей предоставляется возможность приобрести компьютер по доступной цене[25].

Одна из основных проблем развивающихся стран состоит в «утечке мозгов», то есть в переезде высококвалифицированных сотрудников из развивающихся в развитые страны. Это приводит к потере квалифицированной рабочей силы, а также средств, затраченных на обучение и подготовку таких специалистов.

Утечка мозгов, скорее всего, будет продолжаться, учитывая разнообразные схемы по трудоустройству или эмиграции, которые были разработаны в США и других развитых странах для привлечения квалифицированных специалистов в области ИКТ.

С другой стороны, развитие аутсорсинга в области ИКТ и передача некоторых функций развивающимся странам может обратить этот процесс вспять. В качестве наиболее успешного примера можно привести центры разработки программного обеспечения в Индии, включая Бангалор и Хайдарабад.

Политика и регулирование

Политика в области телекоммуникаций тесно связана с проблемой разрыва в цифровых технологиях:

- Ни частные инвесторы, ни государственные фонды не готовы инвестировать в страны, где не создана соответствующая институциональная и правовая база для развития Интернета.
- Развитие национальных секторов ИКТ зависит от создания необходимых правовых рамок.
- Политика в области телекоммуникаций должна способствовать созданию эффективного рынка телекоммуникационных услуг с целью развития конкуренции, снижения затрат и расширения сферы услуг.

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

Одним из первых шагов должно стать создание независимого и профессионального надзорного органа в области телекоммуникаций. Опыт развитых стран показывает, что продуманная система надзора является необходимой предпосылкой для быстрого развития телекоммуникационной инфраструктуры. Развивающиеся страны пытаются следовать этому подходу, однако многим из них пока не удалось решить проблему надзорных органов, которые остаются слабыми и зависимыми, либо являются частью системы, в которой надзорную политику определяют государственные телекоммуникационные операторы.

Либерализация телекоммуникационного рынка — еще одна важная проблема. Как правило, в качестве примера стран, где либерализация рынка способствовала стремительному развитию Интернета и ИКТ, что, в свою очередь, способствовало развитию экономики в целом, приводятся Индия и Бразилия. Однако для других стран, включая наименее развитые государства, либерализация телекоммуникационного рынка стала огромной проблемой. С утратой монополии в сфере телекоммуникаций власти этих стран лишились важного источника бюджетных поступлений, что не могло не сказаться на всех сферах социальной и экономической жизни.

В ряде случаев, когда приватизация телекоммуникационных компаний не сопровождалась формированием эффективного рынка и развитием конкуренции, страны теряли не только доход от телекоммуникационной монополии, но и выгоды от либерализации, которая, по идее, должна снижать стоимость и повышать качество услуг. В этой связи Всемирный банк подчеркнул, что странам следует вводить конкуренцию в основных сегментах рынка до приватизации государственных операторов либо одновременно с этим. Это позволит снизить стоимость услуг и издержки быстрее, чем в странах, которые сначала проводят приватизацию, а меры по повышению конкуренции осуществляют позже.

Развитие потенциала

Залогом эффективности и легитимности системы управления Интернетом является способность стран, организаций и физических лиц принимать полноценное участие в управлении соответствующими процессами. Речь идет о возможности «выявлять и решать проблемы, принимать осознанные решения, определять приоритеты, планировать дальнейшие действия и претворять в жизнь программы и проекты, направленные на достижение поставленных целей».

О развитии потенциала

Хотя важность развития потенциала никто не ставит под сомнение, содержание этого понятия остается предметом споров. Словосочетание «развитие потенциала» стало частью профессионального жаргона. Так, в ходе дипломатических переговоров при отсутствии согласия по всем другим вопросам этот термин нередко используется в качестве наименьшего общего знаменателя.

Как правило, под развитием или наращиванием потенциала понимается подготовка кадров и повышение квалификации. Такое толкование термина уходит корнями в период 1950 — 1960 гг., когда центральную роль в программах технической помощи развитых стран развивающимся странам играло образование. В 1970-х гг. понятие технического сотрудничества уже не сводилось к передаче навыков и знаний. В зависимости от специфики конкретной страны, в рамках национальной политики и программ развития понятию «наращивание потенциала» придавалось разное значение. В последнее время (с 1990-х гг.), под этим термином все чаще понимается расширение возможностей и укрепление национальных потенциалов в развивающихся странах.

> Развитие или создание потенциала
>
> При обсуждении вопросов развития часто можно услышать два термина: развитие потенциала и создание потенциала. Первый относится к развитию существующего национального потенциала и навыков, имеющихся во всех странах, тогда как под созданием потенциала понимается создание с нуля не существовавших ранее возможностей. В современном дискурсе о развитии преимущественно используется понятие развития потенциала.

Рисунок 22. Схема развития потенциала

Суть понятия «развитие потенциала» можно объяснить, выделив виды потенциала и уровни, на которых они развиваются.

Виды потенциала:

- Реальный (твердый) потенциал: технические и специализированные знания и ноу-хау (например, в области инженерного дела).
- «Мягкий» потенциал, который обычно делится на две подгруппы:
- Операционный потенциал: межкультурное общение, лидерство, организационная культура и ценности, способность к решению проблем.

- Адаптационный потенциал: способность анализировать и адаптироваться, корректировать состояние готовности и управление, уверенность.

Наличие реального потенциала, носящего технический характер, очевидно, тогда как мягкий потенциал невидим и лежит в плоскости рационального.

Уровни, на которых происходит развитие и использование различных возможностей, отображены на схеме (рис. 22), напоминающей по своей форме бабочку (в соответствии с методологией Швейцарского агентства по развитию и сотрудничеству)[27].

Развитие потенциала применительно к управлению Интернетом и политике в области цифровых технологий

Важность наращивания потенциала применительно к проблематике управления Интернетом была отмечена еще в итоговых документах WSIS 2003—2005 гг., в которых говорилось о приоритете развития потенциала для развивающихся стран. В итоговом документе WSIS+10 2015 г. содержится призыв продолжать инвестировать в развитие потенциала.

Учитывая новизну темы управления Интернетом, основное внимание уделяется подготовке кадров и изучению нормативного и надзорного опыта.

Ряд организаций, включая МСЭ, DiploFoundation, Geneva Internet Platform (GIP)[28], APC, Internet Society и ICANN, разработали специальные программы по развитию потенциала. Управление Интернетом изучается в рамках региональных летних школ, организованных, в частности для развивающихся стран. Многие из существующих программ затрагивают такие темы, как телекоммуникационная инфраструктура, технические стандарты, кибербезопасность, спам, регулирование ИКТ, свобода выражения мнений, интернет-торговля, трудовое законодательство, вопросы доступа и преодоление цифрового разрыва.

Подготовку по вопросам управления Интернетом и политики в области цифровых технологий прошли сотни специалистов. На следующем этапе необходимо сосредоточить внимание на организационных аспектах путем проведения мероприятий по развитию организационных навыков представителей органов власти, гражданского общества, деловых ассоциаций

и научного сообщества развивающихся стран. Совершенствование организационной деятельности и системный подход к наращиванию потенциала приобретают особое значение в таких областях, как кибербезопасность.

Ниже приводятся основные тезисы исследований в области развития потенциала и управления Интернетом:

- Интернет представляет собой феномен глобального масштаба, однако его регулирование нередко осуществляется на локальном уровне, исходя из специфики конкретной культуры и общества (например, с точки зрения восприятия контента представителями разных культур, важности защиты персональных данных). Таким образом, при развитии потенциала в области управления Интернетом и реализации соответствующих программ и инициатив следует учитывать местную специфику, особенности политической, социальной и культурной жизни и другие характеристики.
- Развитие потенциала обеспечивается путем своевременной реализации образовательных программ в рамках развития системы управления Интернетом. Таким подходом отчасти руководствуются DiploFoundation и GIP при подготовке дипломатов, организация ICANN при осуществлении Fellowship Programme[29], а также Internet Society в своей программе IGF Ambassadors Programme[30].
- Необходимо разработать системный подход к вопросу развития потенциала в области регулирования цифровых технологий. Тема управления Интернетом и связанные с ней вопросы должны войти в программы послевузовского образования.
- Расширить возможности в этой области можно путем применения целостного подхода к развитию потенциала на уровне индивида, организации, системы и сети, как это показано на рис. 22.

Примечания к разделу 6

[1] Речь идет о двух исследованиях: World Bank (2016) World Development Report 2016: Digital Dividends. Адрес в Интернете: http://www.worldbank.org/en/publication/wdr2016 [просмотрено 7 августа 2018 г.].

[2] United Nations General Assembly (2002) Resolution A/56/183. World

Summit on the Information Society. Адрес в Интернете: http://www.itu.int/net/wsis/docs/background/resolutions/56_183_unga_2002.pdf [просмотрено 7 августа 2018 г.].

[3] United Nations General Assembly (2000) Resolution A/55/L.2. United Nations Millennium Declaration. Адрес в Интернете: http://www.un.org/millennium/declaration/ares552e.htm [просмотрено 7 августа 2018 г.].

[4] United Nations (no date) Millennium Development Goals. Адрес в Интернете: http://www.un.org/millenniumgoals/ [просмотрено 7 августа 2018 г.].

[5] United Nations General Assembly (2015) Resolution A/70/1. Transforming our world: the 2030 Agenda for Sustainable Development. Адрес в Интернете: http://www.un.org/ga/search/view_doc.asp?symbol=A/RES/70/1&Lang=E [просмотрено 7 августа 2018 г.].

[6] United Nations General Assembly (2015) Resolution A/70/125. Outcome document of the high-level meeting of the General Assembly on the overall review of the implementation of the outcomes of the World Summit on the Information Society. Адрес в Интернете: http://workspace.unpan.org/sites/Internet/Documents/UNPAN96078.pdf [просмотрено 7 августа 2018 г.].

[7] Подробнее о связи между целями устойчивого развития и Интернетом см. GIP Digital Watch observatory (no date) Sustainable Development Goals and the Internet. Адрес в Интернете: http://digitalwatch.giplatform.org/processes/sustainable-development-goals [просмотрено 7 августа 2018 г.].

[8] UNCTAD (no date) Information and Communication Technology for Development. Адрес в Интернете: http://unctad.org/en/Pages/DTL/STI_and_ICTs/ICT4D.aspx [просмотрено 7 августа 2018 г.].

[9] WSIS Forum (2015) WSIS-SDG Matrix: Linking WSIS Action Lines with Sustainable Development Goals. Geneva: International Telecommunications Union. Адрес в Интернете: https://www.itu.int/net4/wsis/sdg/Content/Documents/wsis-sdg_matrix_document.pdf [просмотрено 7 августа 2018 г.].

[10] Подробнее о дискуссиях в рамках WSIS 2015 и 2016 гг. см.: GIP Digital Watch observatory (no date) WSIS Forum 2015. Адрес в Интернете: https://dig.watch/events/wsis-forum-2015 [просмотрено 7 августа 2018 г.]; and GIP Digital Watch observatory (no date) WSIS Forum 2016. Адрес в Интернете: https://dig.watch/events/wsis-forum-2016 [просмотрено 7 августа 2018 г.].

[11] World Bank (2016) World Development Report 2016: Digital Dividends. Адрес в Интернете: http://www.worldbank.org/en/publication/wdr2016 [просмотрено 7 августа 2018 г.].

[12] OECD (2001) Understanding the Digital Divide. p. 5. Адрес в Интернете: http://www.oecd.org/internet/ieconomy/1888451.pdf [просмотрено 7 августа 2018 г.].

[13] Internet World Stats (2016) Digital Divide Gap is Getting Smaller. Адрес в Интернете: http://internetworldstats.com/wp/digital-divide-gap-is-getting-smaller/ [просмотрено 7 августа 2018 г.].

[14] WEF (2016) Global Information Technology Report. Адрес в Интернете: https://www.weforum.org/reports/the-global-information-technology-report-2016 [просмотрено 7 августа 2018 г.].

[15] European Union (2014) Universal Service. Адрес в Интернете: https://ec.europa.eu/digital-single-market/universal-service [просмотрено 7 августа 2018 г.].

[16] European Commission (2016) Proposal for a Directive of the European Parliament and of the Council establishing the European Electronic Communications Code. Адрес в Интернете: https://ec.europa.eu/digital-single-market/en/news/proposed-directive-establishing-european-electronic-communications-code [просмотрено 7 августа 2018 г.].

[17] United Nations (2011) Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue. Адрес в Интернете: http://www2.ohchr.org/english/bodies/hrcouncil/docs/17session/A.HRC.17.27_en.pdf [просмотрено 7 августа 2018 г.]. О дебатах в связи с докладом ООН см.: Wagner A. Is Internet access a human right? // The Guardian, 11.01.2012. Адрес в Интернете: https://www.theguardian.com/law/2012/jan/11/is-internet-access-a-human-right [просмотрено 7 августа 2018 г.].

[18] Internet Society (2012) Promoting the Use of Internet Exchange Points (IXPs): A Guide to Policy, Management and Technical Issues. Адрес в Интернете: https://www.isoc.org/educpillar/resources/docs/promote-ixp-guide.pdf [просмотрено 7 августа 2018 г.].

[19] South Eastern European Dialogue on Internet Governance (2016) SEEDIG's contribution to the IGF 2016 Inter-sessional Programme on Policy Options for Connecting and Enabling the Next Billion — Phase II. Адрес в Интернете: http://www.seedig.net/wp-content/uploads/2016/09/SEEDIG-contribution-to-IGFCENB-II.pdf [просмотрено 7 августа 2018 г.].

[20] Berkman Center for Internet & Society, Harvard Law School (2003) BOLD 2003: Development and the Internet, Part 4: Solutions in the Architecture. Адрес в Интернете: http://cyber.law.harvard.edu/bold/devel03/modules/modIC.html [просмотрено 7 августа 2018 г.].

[21] Huston G (2005) Where's the Money? Internet Interconnection and Financial Settlement // The ISP Column, January 2005, Internet Society, pp. 7/9. Адрес в Интернете: http://www.potaroo.net/ispcol/2005-01/interconn.pdf [просмотрено 7 августа 2018 г.].

[22] Рекомендация D.50 МСЭ а также приложения к этому документу см.: http://www.itu.int/rec/T-REC-D.50/e [просмотрено 7 августа 2018 г.].

[23] United Nations (2015) Addis Ababa Action Agenda of the Third International Conference on Financing for Development. Адрес в Интернете: http://www.un.org/esa/ffd/publications/aaaa-outcome.html [просмотрено 7 августа 2018 г.].

[24] World Bank (2016) World Development Report 2016: Digital Dividends. Адрес в Интернете: http://www.worldbank.org/en/publication/wdr2016 [просмотрено 7 августа 2018 г.].

[25] Infocomm Development Authority of Singapore (no date) NEU PC Plus Programme. Адрес в Интернете: https://www.imda.gov.sg/community/consumer-education/digital-inclusion/neu-pc-plus-programme [просмотрено 7 августа 2018 г.].

[26] Swiss Agency for Development and Cooperation (2006) Glossary Knowledge Management and Capacity Development. Адрес в Интернете: https://www.eda.admin.ch/dam/deza/en/documents/publikationen/glossar/157990-glossar-wissensmanagement_EN.pdf [просмотрено 7 августа 2018 г.].

[27] Swiss Agency for Development and Cooperation (2006) Capacity Development in SDC. Адрес в Интернете: https://www.eda.admin.ch/content/dam/deza/en/documents/die-deza/strategie/202114-capacity-development-

sdc_EN.pdf [просмотрено 7 августа 2018 г.].

[28] В рамках деятельности по развитию потенциала фонд Diplo проводит программу Internet Governance Capacity Building, интернет-курсы по управлению интернетом, кибербезопасности и технической инфраструктуре, а также отвечает за специализацию по управлению интернетом в рамках магистратуры по современной дипломатии. Будучи оператором GIP, Diplo проводит курсы подготовки для постоянных представительств.

[29] ICANN (no date) ICANN Meeting Fellowships. Адрес в Интернете: https://www.icann.org/fellowshipprogram [просмотрено 7 августа 2018 г.].

[30] Internet Society (no date) IGF Ambassadors Programme. Адрес в Интернете: https://www.internetsociety.org/leadership/fellowship-to-ietf/ [просмотрено 7 августа 2018 г.].

Раздел 7

Социокультурные аспекты

Социокультурные аспекты

Интернет оказал значительное влияние на общественную и культурную ткань современного общества. Сложно назвать область общественной жизни, на которую он бы не повлиял. Интернет привносит в нашу жизнь новые модели социальной коммуникации, разрушает языковые барьеры и создает новые формы творческого самовыражения — и это лишь некоторые примеры его влияния. Сегодня Интернет стал в большей степени социальным, а не только технологическим явлением.

Политика в отношении содержания материалов Интернета

Содержание информационных материалов (контента) Интернета является одним из основных вопросов с точки зрения властей (введение мер по контролю над материалами исходя из разных соображений, от соображений национальной безопасности, нравственности и общественного порядка, до политически мотивированных форм цензуры), прав человека (влияние политики в области регулирования контента на право выражения мнений и право на доступ к средствам связи) и технологий (инструменты контроля над содержанием материалов).

Дискуссии о содержании материалов Интернета обычно сводятся к обсуждению трех видов материалов:

- Материалы, необходимость контролировать распространение которых ни у кого не вызывает сомнений. Среди них детская порнография, материалы, оправдывающие геноцид и связанные с организацией террористических актов или призывами к ним.
- Материалы, которые могут оказаться оскорбительными для определенных стран, регионов или этнических групп в силу их религиозных или культурных особенностей. Глобальные онлайн-коммуникации являются вызовом культурным и религиозным ценностям многих групп людей. Контроль над материалами Интернета, осуществляемый на Ближнем Востоке и в азиатских странах, официально объясняется необходимостью защиты специфических культурных ценностей. Обычно под этим подразумевается запрещение доступа к порнографическим сайтам и сайтам, связанным с азартными играми.
- Политическая цензура в Интернете, которая нередко направлена на борьбу с политическим инакомыслием якобы из соображений национальной безопасности и стабильности[1].

Каким образом осуществляется политика в отношении материалов Интернета?

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

Фильтрация материалов властями

Распространенным способом правительственной фильтрации является «интернет-индекс» веб-сайтов, доступ к которым граждан запрещен. С технической точки зрения, фильтрация в основном осуществляется посредством блокировки IP-адресов на уровне маршрутизаторов, прокси-серверов и переназначения при обращении к DNS. Фильтрация материалов применяется во многих странах. Помимо государств, которые обычно ассоциируются с этой практикой — Китай, Саудовская Аравия и Сингапур, — такие меры становятся все более востребованными и в других странах[2].

Частные системы рейтингов и фильтрации

Столкнувшись с риском дезинтеграции Интернета в связи с появлением различных государственных барьеров (систем фильтрации), W3C и другие подобные институты «сработали на опережение», предложив использовать системы рейтингов и фильтрации, контролируемые конечными пользова-

телям. В системах такого рода фильтрующие механизмы устанавливаются на персональные компьютеры или на уровне серверов, отвечающих за доступ к Интернету.

Таким образом пользователи, представляющие разные страны и культуры, получают возможность создавать собственные системы фильтрации, тем самым устраняя необходимость вмешательства со стороны государства. Это может привести к фрагментации Интернета в отдельные блоки, сформированные по национальным или культурным признакам. Будущее покажет, доверят ли власти своим гражданам задачу по фильтрации материалов в соответствии с потребностями государства. Скорее всего, такое решение не заменит фильтрацию контента властями, но даст пользователями дополнительную возможность для индивидуальной настройки Интернета.

Известно, что в ряде стран контроль над материалами Интернета осуществляется по религиозным соображениям. При этом с требованием фильтровать контент по религиозным убеждениям могут также выступать конкретные организации. Например, в 1998 г. сообщалось, что среди сайентологов было распространено программное обеспечение, которое критики окрестили «сиделкой сайентологии», поскольку эта программа якобы блокировала доступ к сайтам с критикой движения[3]. В некоторых других случаях подобные меры могли охватывать население целой страны: например, организация «Австралийское христианское лобби» потребовала, чтобы власти страны создали фильтр, который бы блокировал доступ к «материалам для взрослых» на персональных компьютерах и мобильных устройствах в Австралии[4].

Фильтрация контента на основе данных геолокации

Еще одним техническим решением, связанным с материалами Интернета, является геолокационное программное обеспечение, которое фильтрует доступ пользователей к определенным материалам в зависимости от региона или страны нахождения пользователей. С этой точки зрения значительным прецедентом стало дело Yahoo!, поскольку занимавшаяся им группа экспертов, в состав которой входил Винт Серф, заявила, что в 70-90% случаев Yahoo! имела возможность определить, находится ли пользователь, пытающийся зайти в раздел сайта с нацистской атрибутикой, во Франции[5]. Подобная техническая оценка помогла суду принять окончательное решение — от Yahoo! потребовали фильтровать доступ из Франции к размещенным на портале нацистским материалам. С тех пор решения по геолокации стали еще более точными благодаря развитию программного обеспечения в этой области.

Контроль над материалами с помощью поисковых систем

Поисковая система обычно выполняет функцию связующего звена между размещенным в Интернете материалом и конечным пользователем. Соответственно, еще одним средством ограничения доступа к определенным материалам может быть фильтрация результатов поиска. Поисковые системы зачастую создают такие средства фильтрации для выполнения нормативных требований. Один из ярких примеров подобного подхода связан с деятельностью компании Google в Китае. В 2006 г. Google решила запустить местную версию своего поисковика (google.cn) с учетом требований властей Китая по фильтрации размещенных в интернете материалов, которые считались сомнительными. В 2010 г. компания изменила свой подход и стала перенаправлять поисковые запросы, полученные на Google.cn, на гонконгские серверы (где систем по фильтрации не было). Такие действия стали причиной трений с китайскими властями, что, в конечном счете, заставило Google свернуть свою деятельность в Китае[6].

При этом фильтрацией результатов поиска занимаются не только власти. Такие инициативы могут также исходить от коммерческих структур, преследующих более или менее очевидные цели. Обозреватели уже обратили внимание на то, что поисковые системы выполняют функцию посредника между информацией и пользователями и, таким образом, могут влиять на формирование знаний и предпочтений[7]. Это привлекло внимание властей, от которых все чаще можно услышать призывы к большей прозрачности со стороны интернет-компаний. В качестве примера можно привести выступление Федерального канцлера Германии Ангелы Меркель в октябре 2016 г., когда она призвала интернет-компании обнародовать информацию о поисковых алгоритмах. По мнению Меркель, такая информация

позволила бы пользователям понять, каким образом поисковые системы отображают информацию по их запросам. Канцлер отметила: «Отсутствие прозрачности алгоритмов приводит к искажению восприятия и тем самым сужает спектр получаемой нами информации»[8].

Вызов Веб 2.0: пользователи как авторы

С развитием платформ Веб 2.0 — блогов, форумов, сервисов обмена документами и виртуальных миров — различия между пользователем и создателем контента стираются. Пользователи Интернета могут сами создавать значительную часть материалов: сообщения блогов, видео на YouTube, фотогалереи. Выявление, фильтрация и маркировка «неподходящих» сайтов становятся все сложнее. Несмотря на существование технологий автоматической фильтрации, автоматическое распознавание, фильтрация и категоризация изображений и видео пока находятся на ранних стадиях развития.

Одним из вариантов борьбы с материалами, которые власти считают предосудительным, является полная блокировка доступа к таким ресурсам, как YouTube и Twitter, по всей стране. Однако результатом подобного «максималистского» подхода становится недоступность материалов, не вызывающих возражений, в том числе образовательных. Еще одной экстремальной мерой может стать полное отключение Интернета, чтобы исключить возможность общения в социальных сетях (как это было, например, в ходе «арабской весны»)[9].

Обсуждение вопроса о том, что позволительно публиковать в Интернете, способствовало выработке социальными сетями собственных правил, на основании которых они определяют, какие материалы допустимы, а какие нет. Например, в Положении о правах и обязанностях (Statement of Rights and Responsibilities) компании Facebook говорится: «Мы оставляем за собой право удалить любой контент или информацию, опубликованные вами на Facebook, если сочтем, что они нарушают настоящее Положение или наши правила»[10]. Однако исполнение таких требований иногда приводит к непредсказуемым последствиям, когда социальные сети удаляют материалы, в которые нет никаких нарушений.

Системы автоматизированного контроля над содержанием материалов Интернета

Социальным сетям очень сложно отслеживать незаконные материалы среди миллионов видеороликов, звуковых файлов и статей, которые размещаются на их ресурсах. Одним из решений этой проблемы могло бы стать использование средств искусственного интеллекта. О большом потенциале такого подхода свидетельствует пример Conversation AI — разработанного по инициативе Google решения, которое позволяет выявлять содержание оскорбительного, ненавистнического или непристойного характера в Интернете[11]. В основе данного программного обеспечения лежат технологии Google по сбору и обработке информации. По состоянию на октябрь 2016 г. решение находилось на стадии тестирования. Однако использование методов машинного обучения при принятии решения о том, что следует считать проявлением «языка ненависти», ставит немало вопросов. В частности, способны ли такие системы почувствовать различие между языком ненависти и иронией или сарказмом?

Правовые и политические методы контроля над содержанием материалов

Письменные и устные материалы всегда были важным субъектом регулирования. Каждое общество определяет, какие материалы приемлемы с точки зрения политики, безопасности и религии, а какие нет. Политика в этой области может варьироваться от поддержки свободы выражения мнений до цензуры. Существенно упростив распространение информации, Интернет также стал субъектом регулирования. Таким образом, сложилась парадоксальная ситуация: с одной стороны, жесткое регулирование содержания материалов, с другой стороны, правовой вакуум в плане применения к Интернету существовавших норм.

Национальный уровень

Регулирование содержания материалов Интернета характеризуется правовой неопределенностью, что объясняется создавшимся в этой области правовым вакуумом. Совершенствование национальной нормативно-пра-

вовой базы могло бы сделать эту сферу более предсказуемой и обеспечить эффективную защиту прав человека, включая свободу выражения мнений и информации. Кроме того, введение четких правил помогло бы ограничить произвол властей в сфере регулирования содержания материалов Интернета. Это бы также пошло на пользу деловому сообществу, включая интернет-провайдеров и интернет-компании, которым больше бы не пришлось самостоятельно принимать решения по этому вопросу.

Грань между обоснованным контролем над содержанием материалов и цензурой весьма расплывчата, и регулировать эту сферу на законодательном уровне затруднительно. В итоге, для решения спорных вопросов приходится обращаться в суд. Например, в мае 2016 г. против нескольких социальных сетей были поданы иски в связи с размещением на их ресурсах материалов с элементами расизма и гомофобии[12]. После терактов в ноябре 2015 г. в Париже и в Израиле в 2014 и 2016 гг., против социальных сетей были выдвинуты обвинения в предоставлении террористам ресурсов для «общения, пополнения рядов, планирования и осуществления атак и устрашения врагов»[13], а также в содействии распространению террористической пропаганды[14].

Международные инициативы

В свете террористической угрозы и использования террористами все более совершенных средств для продвижения своей деятельности и идеологии в Интернете в центре внимания многосторонних форумов оказался вопрос об ограничении распространения «вредных» материалов. Например, главы стран «большой семерки» заявили о необходимости «активизировать усилия по противодействию угрозе использования террористическими группами Интернета и социальных сетей в своих целях»[15]. Кроме того, Совет Безопасности ООН поручил своему Контртеррористическому комитету разработать рекомендации по противодействию использованию террористами Интернета для продвижения своих идей и пополнения рядов[16]. УНП ООН подготовило доклад об использовании Интернета в террористических целях[17].

Подробнее о противодействии распространению террористической пропаганды и идей насильственного экстремизма в Интернете см. **Раздел 3.**

На региональном уровне основные инициативы исходят от европейских стран с мощной правовой базой, касающейся проявлений различных форм нетерпимости, включая расизм и антисемитизм. Европейские региональные институты пытались ввести эти правила применительно к киберпространству. Основным правовым инструментом, регулирующим вопросы содержания материалов Интернета, является Дополнительный протокол к Конвенции по киберпреступности Совета Европы 2003 г.[18] о криминализации проявлений расизма и ксенофобии с использованием компьютерных систем. В 2012 г. в ЕС принята Европейская стратегия по повышению безопасности Интернета для детей. В соответствии с этой стратегией проводится ряд программ и инициатив, направленных на повышение осведомленности, борьбу с незаконными материалами, внедрение решений по фильтрации и маркировке материалов, взаимодействие с гражданским обществом по вопросам безопасности детей в Интернете и создание баз данных об использовании технологий детьми[19].

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

Вопросы

Контроль над материалами Интернета и свобода выражения убеждений

Контроль над содержанием материалов Интернета нередко воспринимается как угроза свободе выражения мнений. Попытки найти сбалансированное решение этой проблемы предпринимаются во многих странах с целью содействия свободе выражения убеждений при сохранении возможности в исключительных и оправданных случаях контролировать содержание материалов. Это особенно важно в США, где Первая поправка к Конституции

гарантирует свободу выражения мнений в самом широком смысле, включая право публиковать нацистские материалы и подобную им информацию.

Свобода выражения убеждений во многом определяет позицию США в международной полемике по вопросам управления Интернетом. Так, хотя США и подписали Конвенцию о киберпреступности, они не могут подписать Дополнительный протокол к ней, посвященный нетерпимым высказываниям и контролю над материалами. Свобода выражения убеждений также рассматривалась в контексте дела Yahoo!. В ходе международных переговоров США не пойдут на компромисс, который может поставить под вопрос свободу выражения убеждений, защищаемую Первой поправкой.

Незаконно в реальной жизни — незаконно в виртуальном пространстве

Как и в случае с правами человека, согласно господствующей точке зрения, правила реального, физического мира в области контроля над содержанием материалов распространяются на Интернет.

Один из аргументов, выдвигаемых сторонниками «киберподхода» к управлению Интернетом, заключается в том, что количество (интенсивность коммуникации, количество сообщений) влияет на качество. Согласно этой точке зрения, проблема нетерпимых высказываний состоит не в том, что отсутствуют соответствующие нормативные акты, а в том, что масштабы распространения информации и обмена ей в Интернете придают правовой проблеме новые черты. Все большее число людей имеет доступ к противозаконным материалам, поэтому обеспечить соблюдение существующих норм сложно. Следовательно, уникальность Интернета с правовой точки зрения заключается не в законах, а в их применении и соблюдении.

Подробнее о «киберподходе» к регулированию Интернета см. ***Раздел 4****.*

Эффективность контроля над материалами Интернета

При обсуждении политики в отношении материалов Интернета одним из ключевых аргументов является децентрализованная природа глобальной сети, дающая пользователям возможность обходить цензуру. В странах, где

контроль над материалами Интернета ведется на государственном уровне, технически продвинутые пользователи сумели найти обходные пути (например, получение доступа к отфильтрованным материалам посредством VPN или предоставление доступа к запрещенным материалам на других ресурсах). Эксперты отмечают, что фильтрация материалов чревата негативными техническими последствиями. Так, блокировка на уровне DNS может создавать помехи в работе DNSSEC и приводить к фрагментации Интернета[20].

Кто несет ответственность за политику в отношении материалов?

В первую очередь, содержание материалов Интернета регулируют парламенты и правительства. В большинстве случаев именно они отвечают за соблюдение основных конституционных принципов, определяющих, что надлежит контролировать и каким образом. На интернет-провайдеров, как основных «посредников» в Интернете, обычно возлагается ответственность за осуществление фильтрации контента — либо в соответствии с указаниями правительства, либо на основе саморегулирования (по крайней мере, в отношении материалов, не вызывающих дискуссий, таких как детская порнография). Некоторые группы пользователей, например, родители, стремятся усилить контроль, чтобы обезопасить своих детей. С целью помочь родителям отфильтровывать не подходящие для детей веб-страницы, созданы различные системы рейтингов. Новые версии интернет-браузеров обычно включают в себя разнообразные возможности фильтрации.

Интернет-компании, такие как Facebook, Google и Twitter, начинают играть роль регуляторов де-факто. Так, компании Google пришлось рассмотреть свыше полумиллиона запросов на удаление результатов поиска в соответствии с правом на забвение.

Подробнее о деятельности интернет-компаний по урегулированию споров в отношении содержания материалов в Интернете см. ***Раздел 4.***

Такие компании в сотрудничестве с властями активно борются с незаконными материалами. В 2016 г. состоялась серия встреч между представителями технологических компаний Кремниевой долины и американскими властями по обсуждению сотрудничества в области контроля над содержанием материалов в Интернете, в частности, применительно к материалам

террористической направленности[21]. В ЕС Европейская комиссия в сотрудничестве с IT-компаниями ведет работу по созданию кодекса поведения в отношении нетерпимых высказываний в Интернете, включающего обязательства по борьбе с распространением таких материалов в Европе[22].

Интернет-образование

Интернет открыл новые возможности для образования. При реализации различных образовательных проектов Интернет обеспечивает взаимодействие между участниками образовательного процесса, которые могут находиться в любой стране мира. При этом решения в области дистанционного обучения дополняют очное обучение в традиционных университетах, тем самым создавая смешанную систему обучения. Хотя интернет-образование не может заменить традиционные подходы, эта сфера открывает новые возможности, особенно в тех случаях, когда личное присутствие на занятии невозможно в силу временных или пространственных факторов. В последнее время интернет-образование рассматривается как часть реформы высшего образования, а также элемент институциональных и организационных изменений в системе образования[23].

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

Вопросы

ВТО и образование

Одним из противоречивых аспектов переговоров в рамках ВТО является интерпретация статей 1(3) (b) и (c) Генерального соглашения по торговле услугами (GATS), которое предусматривает исключения из режима свободной торговли для услуг, предоставляемых государством. В соответствии с точкой зрения, поддерживаемой в основном США и Великобританией, эти исключения должны трактоваться в узком смысле, и де-факто в области высшего образования должна осуществляться свободная торговля. Подобный подход продиктован главным образом заинтересованностью образовательного сектора США и Великобритании в формировании глобального рынка образовательных услуг, и он вызывает целый ряд возражений со стороны других стран[24].

Ключевой вопрос заключается в том, следует ли образование считать товаром или общественным благом? Если рассматривать образование как товар, то правила свободной торговли, принятые ВТО, можно будет применять и в этой сфере. Если же относиться к образованию как к общественному благу, то сохранится ныне существующая модель образования, в соответствии с которой государственные университеты имеют особый статус учреждений, значимых для национальной культуры. На развитие интернет-образования также может повлиять либерализация торговли. Некоторые обозреватели обратили внимание на возможность возникновение «повышательной тенденции» в сфере образования[25].

Обеспечение качества и стандартизация

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

потенциал не используется. Это заставило учебные заведения приступить к разработке стандартов и руководств для оценки концепции и содержания интернет-курсов[26].

Признание академических степеней и создание общей системы зачетных единиц

Применительно к области интернет-обучения особую значимость имеет вопрос о признании степеней. Основной задачей здесь выступает обеспечение признания дипломов и степеней на региональном и глобальном уровнях.

ЕС начал разработку такой нормативной базы в виде Европейской системы взаимозачета кредитов[27]. Азиатско-Тихоокеанский регион следует примеру Европы, создавая свою собственную региональную модель для обмена студентами и систему зачетных единиц в рамках программы University Mobility in Asia and the Pacific (UMAP)[28].

По мере развития интернет-образования наметилась тенденция к признанию и зачету учебных достижений по схеме, аналогичной подходу традиционных университетов.

Развивается и проект Массового открытого интернет-курса (Massive Open Online Courses — MOOCs). Пройдя фазу становления и взрывного спроса, этот проект вышел на разработку ресурсов, призванных обеспечить за счет технологий дистанционного обучения такое взаимодействие в рамках образовательного процесса, которое бы не уступало традиционной системе образования.

Стандартизация интернет-обучения

Начальный этап развития интернет-обучения характеризовался быстрым развитием и большим разнообразием материалов с точки зрения технических платформ, содержания и дидактики. Однако существует необходимость разработки общих стандартов для зачета пройденных курсов и других академических достижений и обеспечения минимального уровня качества. Стандартизация проводится преимущественно силами частных компаний и профессиональных организаций.

ИКТ, образование и развитие

В рамках ЦУР сформулирована амбициозная цель по обеспечению всеохватного и справедливого качественного образования и поощрения возможности обучения на протяжении всей жизни (4-я цель устойчивого развития). Достижение этой цели можно связать с рядом инициатив WSIS, как это показано в сводной таблице WSIS-ЦУР[29], что подчеркивает важность ИКТ для образования.

Культурное разнообразие

Культурное разнообразие — широкое понятие, под которым понимается разнообразие с точки зрения языка, национальной идентичности, традиций и религии. Применительно к Интернету культурное разнообразие в своих различных проявлениях играет двоякую роль. С одной стороны, Интернет может способствовать продвижению культурного разнообразия в глобальном масштабе, поскольку дает возможность представителям разных культур общаться друг с другом, а также обеспечивает доступ к огромному объему информации и знаний. Используя Интернет, люди также получают возможность распространять свою национальную и культурную идентичность. С другой стороны, как подчеркивалось в ходе WSIS, культурное разнообразие является залогом развития открытого информационного общества на основе диалога и взаимоуважения культур.

Одним из средств достижения цели по сохранению, развитию и поощрению культурного разнообразия в Интернете является содействие созданию материалов с местной спецификой, которая отражает национальную идентичность или культурные особенности. С распространением таких оригинальных материалов в Интернете виртуальное пространство может стать более разнообразным и открытым, способствуя повышению осведомленности об идентичности и самобытности народов на глобальном уровне.

К другим способам продвижения культурного разнообразия относится перевод, адаптация и распространение в Интернете существующих мате-

риалов с местной спецификой, а также сохранение посредством цифровых технологий различных видов информации о коренных народах и их традициях. Создание цифровых архивов может также способствовать развитию местных сообществ, фиксированию и сохранению их культурного наследия. Такие инициативы имеют особое значение для изолированных и кочевых общин, технологические потребности которых нуждаются в специфических решениях. Создание и распространение программного обеспечения на местных языках также могло бы способствовать освоению интернет-технологий.

Многоязычие

С первых дней своего существования Интернет был преимущественно англоязычной средой. По статистике, немногим более 50% всех материалов в Интернете представлено на английском[30], тогда как 75% населения мира не владеет этим языком[31]. В то же время, всего 2% материалов в Интернете приходится на китайский язык, несмотря на то что на этом языке говорит больше всего людей. Согласно докладу Комиссии ООН по вопросам широкополосной связи 2015 г., в настоящее время в Интернете представлены лишь около 5% из 7 100 языков мира. В докладе также отмечается, что многие интернет-пользователи испытывают трудности с использованием латиницы, в частности в доменных именах[32].

Такая ситуация побудила многие страны принять согласованные меры с целью сохранения многоязычия и защиты культурного разнообразия. Задача поддержания многоязычия (рис. 23) связана не только с сохранением культурных особенностей, но и с необходимостью дальнейшего развития Интернета. Чтобы Интернетом могли пользоваться более широкие слои населения, материалы должны быть доступны на большем количестве языков.

Хотя английский язык до сих пор доминирует в Интернете, ситуация постепенно меняется. По мере роста числа пользователей представительство некоторых языков в Интернете также увеличивается. Например, с 2011 по 2015 гг. объем материалов в Интернете на русском языке вырос на 41,5%, испанском на 15,5% и португальском на 56%[33]. Стремительный рост числа пользователей из

Индии и Китая также может привести к повышению доли материалов на языках этих народов.

Рисунок 23. Многоязычие

Вопросы

Нелатинские алфавиты

Развитие многоязычия требует наличия технических стандартов, позволяющих использовать различные алфавиты, символы и шрифты. Одну из первых инициатив в этой области предпринял Консорциум Unicode — некоммерческая организация, разрабатывающая стандарты для использования символов различных алфавитов. В свою очередь, ICANN и IETF предприняли важные меры, направленные на продвижение интернационализированных доменов верхнего уровня (национальные домены верхнего уровня и родовые домены верхнего уровня).

Интернационализированных доменные имена (IDN) созданы для популя-

ризации доменных имен нелатинского написания (на китайском, арабском и кириллице), а также на латинице с диакритическими знаками, которые используются во французском, немецком, венгерском, румынском и других языках[34].

Подробнее о международных доменных именах см. ***Раздел 2.***

Интернационализированных доменные имена способствуют повышению открытости Интернета, поскольку с увеличением числа языков и шрифтов, на которых написаны и зарегистрированы доменные имена, возрастает и число людей, которые могут пользоваться Интернетом. Доменные имена важны не только с точки зрения маршрутизации и названий доменов, но и для доступа к материалам, что делает их особо значимыми для местных общин. Возможность написания доменного имени на своем языке способствует продвижению и созданию материалов на местных языках с использованием местных шрифтов.

Машинный перевод

Неоднократно предпринимались попытки усовершенствовать решения в области машинного перевода. Согласно правилам Евросоюза, официальные документы должны переводиться на языки всех государств-членов; в связи с этим ЕС поддерживал целых ряд проектов, направленных на усовершенствование машинного перевода. Несмотря на несомненные успехи, включая использование средств искусственного интеллекта, в основном результаты в этой области достаточно скромны.

С ростом привлекательности рынков неанглоязычных стран интернет-компании начали включать в свои ресурсы средства машинного перевода. Например, функция автоматического перевода материалов пользователей доступна в Facebook и Instagram.

Создание соответствующих нормативных рамок

Развитие многоязычия требует создания соответствующих нормативных рамок. Важным игроком в этой области является ЮНЕСКО, которая инициировала несколько проектов по развитию многоязычия и приняла ряд ключевых документов, в частности, Всеобщую декларацию по культурному разнообразию[35] 2001 г. Другой организацией, активно работающей в этой области, является Европейский Союз, провозгласивший многоязычие одним из своих главных политических и рабочих принципов[36]. Развитие и широкое использование инструментов Веб 2.0, которые позволяют обычным пользователям вносить вклад в создание материалов Интернета, открывает перспективы увеличения количества и объема материалов местного содержания на различных языках. Однако без общей политики продвижения многоязычия эти возможности могут, напротив, привести к увеличению языкового разрыва, поскольку люди стремятся использовать язык международного общения (как правило, английский), чтобы охватить самую широкую аудиторию.

Содержательный доступ

Тема лингвистического и культурного разнообразия также связана с вопросами обеспечения доступа к Интернету и содействия развитию. Доступность материалов местного характера на местных языках может быть стимулом для использования Интернета. Такие люди получают возможность для самовыражения в Интернете на собственном языке и создания собственных материалов. Таким образом, создание материалов не глобального, а местного назначения может сделать Интернет более открытым и содействовать преодолению разрыва в цифровых технологиях.

Глобальные общественные блага

Попытки придать Интернету статус глобального и общественного достояния предпринимались неоднократно. Наибольшей популярностью в этом контексте пользуется концепция «глобального общественного блага», которая дополняет теории «предметов общего пользования», «всеобщего достояния» и «общего наследия человечества». Эти концепции взаимозаменяемы и во многом пересекаются. Если рассматривать Интернет как глобальное общественное благо, существует два подхода: экономический, при котором Интернет представляет собой неконкурентный ресурс без возмож-

ности ограничения доступа, и подход с точки зрения безопасности, в рамках которого Интернет представляет собой глобальную инфраструктуру, выходящую за рамки национального суверенитета.

Экономический подход

В основе экономического подхода, при котором Интернет рассматривается как глобальное общественное благо, лежат две характеристики: отсутствие соперничества (потребление одним пользователем производится без ущерба другим пользователям) и отсутствие возможности исключать пользователей (ограничить возможность человека пользоваться Интернетом сложно, а может быть, невозможно). Исходя из этих критериев, Всемирный банк[37] пришел к выводу, что Интернет не в полной мере является «общественным благом», поскольку он соответствует лишь одной из характеристик. Интернет соответствует принципу отсутствия соперничества, поскольку пользование Интернетом одним лицом не делает Интернет менее доступным для других. Однако Интернет не соответствует другому ключевому критерию, а именно требованию неисключаемости, ведь доступ к Интернету в той или иной форме обычно обусловлен платой.

Интернет многогранен и не может считаться однородным целым. Соответственно, статус глобального общественного блага применим к доступу к Интернету, использованию знаний и данных, использованию интернет-стандартов, доступу к интернет-образованию, и т. п.

Важной особенностью Интернета является создание новых знаний и информации в результате взаимодействия пользователей по всему миру. Значительный объем знаний был создан в ходе обмена электронными сообщениями, через социальные сети и блоги. За исключением лицензии «Creative Commons»[38] не существует правовых механизмов защиты этих знаний. Без надлежащего правового регулирования эти знания могут превратиться в товар, предмет продажи. Таким образом, общий фонд знаний, важная основа для творческой деятельности, может быть исчерпан. По мере того, как материалы Интернета становятся источником прибыли, все сложнее становится осуществлять свободный обмен информацией, что может привести к сокращению творческого взаимодействия.

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

Подход с точки зрения безопасности

Если рассматривать Интернет как глобальное общественное благо с точки зрения безопасности, то речь идет о защите глобальной инфраструктуры Интернета. В рамках этого подхода Интернет подлежит защите от вмешательства со стороны национальных властей. Сторонники такого подхода часто руководствуются аналогией с международными водами.

Подробнее об аналогиях см. ***раздел 1.***

Как правило, в рамках этого подхода система доменных имен DNS, маршрутизации и интернет протоколов рассматриваются как глобальное общественное благо[39]. Интернет-стандарты (в основном, TCP/IP) открыты и являются достоянием общественности. С этой точки зрения, управление Интернетом должно быть направлено на сохранение общественной составляющей основных интернет-стандартов.

Баланс между частными и общественными интересами

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

Инфраструктура Интернета контролируется преимущественно частными компаниями. Одной из текущих задач является поиск гармоничного сочетания частной собственности на инфраструктуру Интернета и его статуса

глобального общественного блага. Государственные законы дают возможность ограничивать право частной собственности с помощью определенных требований в интересах общества — таких как предоставление равных прав всем потенциальным пользователям и невмешательство в содержание передаваемых материалов.

Примечания к разделу 7

[1] Организация Freedom House публикует ежегодные доклады «Свобода в сети» (Freedom on the Net), в которых, в частности, рассматривается вопрос о наличии цензуры и ее методах в разных странах. Freedom House (no date) About Freedom on the Net. Адрес в Интернете: https://freedomhouse.org/report-types/freedom-net [просмотрено 7 августа 2018 г.].

[2] В рамках проекта OpenNet Initiative ведется сбор, анализ и публикация данных о фильтрации материалов Интернета и слежке в разных странах мира с подготовкой справочных материалов, региональных обзоров и интерактивных карт, с которыми можно ознакомиться на сайте проекта: https://opennet.net/ [просмотрено 7 августа 2018 г.].

[3] Operation Clambake (no date) Church of Scientology Censors Net Access for Members. Адрес в Интернете: http://www.xenu.net/archive/events/censorship/ [просмотрено 7 августа 2018 г.].

[4] Taylor J (2013) Australian Christian Lobby urges Coalition rethink on Internet filtering//ZDNet, 06.09.2013. Адрес в Интернете: http://www.zdnet.com/article/australian-christian-lobby-urges-coalition-rethink-on-internet-filtering/ [просмотрено 7 августа 2018 г.].

[5] Хотя Винт Серф принимал участие в работе группы, он выразил свое несогласие с итоговым докладом, в котором, как он отметил, «уделяется недостаточно внимания недостаткам и, в целом, последствиям создания ограничителей в Интернете». Источник: Guernsey Lю Welcome to the world wide web, passport, please? // New York Times, 15.03.2001. Адрес в Интернете: http://www.nytimes.com/2001/03/15/technology/welcome-to-the-web-passport-please.html?pagewanted=all&src=pm [просмотрено 7 августа 2018 г.].

[6] Waddell K. Why Google Quit China — and Why It's Heading Back // The Atlantic, 19.01.2016. Адрес в Интернете: http://www.theatlantic.com/technology/archive/2016/01/why-goog-le-quit-china-and-why-its-heading-back/424482/ [просмотрено 7 августа 2018 г.].

[7] Хорошей отправной точкой в этой дискуссии стала статья Мэри Мерфи для блока фонда Diplo по управлению Интернетом и комментарии к ней: Google… stop thinking for me! Адрес в Интернете: https://www.diplomacy.edu/blog/google stop-thinking-me [просмотрено 7 августа 2018 г.].

[8] Connolly K. Angela Merkel: Internet search engines are distorting perception. The Guardian, 27.10.2016. Адрес в Интернете: https://www.theguardian.com/world/2016/oct/27/angela-merkel-internet-search-engines-are-distorting-our-perception [просмотрено 7 августа 2018 г.].

[9] Crete-Nishihata M and York J (2011) Egypt's Internet Blackout: Extreme Example of Just-in-time Blocking. OpenNet Initiative. Адрес в Интернете: https://opennet.net/blog/2011/01/egypt's-internet-blackout-extreme-example-just-time-blocking [просмотрено 7 августа 2018 г.].

[10] Facebook (2015) Statement of Rights and Responsibilities. Адрес в Интернете: https://www.facebook.com/terms [просмотрено 7 августа 2018 г.].

[11] Greenberg A. Inside Google's Internet justice league and its AI-powered war on trolls //Wired, 09.09.2016. Адрес в Интернете: https://www.wired.com/2016/09/inside-googles-internet-justice-league-ai-powered-war-trolls/ [просмотрено 7 августа 2018 г.].

[12] Chazan D. Facebook, YouTube and Twitter sued for 'failure to remove homophobic content' // The Telegraph, 15.05.2016. Адрес в Интернете: https://www.telegraph.co.uk/news/2016/05/15/facebook-youtube-and-twitter-sued-for-failure-to-remove-homophob/ [просмотрено 7 августа 2018 г.].

[13] Williams D. Relatives of Palestinian attack victims sue Facebook for $1 billion in U.S. // Reuters, 11.07.2016. Адрес в Интернете: http://www.reuters.com/article/us-israel-palestinians-facebook-idUSKCN0ZR1G0 [просмотрено 7 августа 2018 г.].

[14] Twitter, Facebook and Google 'aided Paris attacks' // BBC. 16.06.2016. Адрес в Интернете: http://www.bbc.com/news/technology-36548798 [просмотрено 7 августа 2018 г.].

[15] G7 (2016) G7 Action Plan on Countering Terrorism and Violent Extremism. Адрес в Интернете: http://www.mofa.go.jp/files/000160278.pdf [просмотрено 7 августа 2018 г.].

[16] Security Council requests UN panel to propose global framework on countering terrorist propaganda // UN News Centre, 11.05.2016. Адрес в Интернете: http://www.un.org/apps/news/story.asp?NewsID=53909#.V7VzGWW5oQF [просмотрено 7 августа 2018 г.].

[17] UNODC (2012) The use of the Internet for terrorist purposes. Vienna: United Nations Office at Vienna. Адрес в Интернете: https://www.unodc.org/documents/frontpage/Use_of_Internet_for_Terrorist_Purposes.pdf [просмотрено 7 августа 2018 г.].

[18] Council of Europe (2003) Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems. Адрес в Интернете: http://conventions.coe.int/Treaty/en/Treaties/html/189.htm [просмотрено 7 августа 2018 г.].

[19] European Commission (2015) From a Safer Internet to a Better Internet for Kids. Адрес в Интернете: https://ec.europa.eu/digital-single-market/safer-internet-better-internet-kids [просмотрено 29 октября 2016 г.].

[20] Подробнее о последствиях фильтрации материалов см.: ICANN Security and Stability Advisory Committee (2012) SSAC Advisory on Impacts of Content Blocking via the Domain Name System. Адрес в Интернете: https://www.icann.org/en/system/files/files/sac-056-en.pdf [просмотрено 7 августа 2018 г.], и Barnes A et al. (2016) Technical Considerations for Internet Services Blocking and Filtering (Internet Architecture Board RFC 7754). Адрес в Интернете: https://tools.ietf.org/html/rfc7754 [просмотрено 7 августа 2018 г.].

[21] Yadron D and Wong JC. Silicon Valley appears open to helping US spy agencies after terrorism summit // The Guardian, 08.01.2016. Адрес в Интернете: https://www.theguardian.com/technology/2016/jan/08/technology-executives-white-house-isis-terrorism-meeting-silicon-valley-facebook-apple-twitter-microsoft [просмотрено 7 августа 2018 г.].

[22] European Commission (2016) European Commission and IT companies announce Code of Conduct on illegal online hate speech. Адрес в Интернете: http://europa.eu/rapid/press-release_IP-16-1937_en.htm [просмотрено 7 августа 2018 г.].

[23] Willcox K et al. (2016) Online Education: A Catalyst for Higher Education Reform. Massachusetts Institute of Technology. Адрес в Интернете: https://professional.mit.edu/sites/default/files/MIT%20Online%20Education%20Policy%20Initiative%20April%202016.pdf [просмотрено 7 августа 2018 г.].

[24] Комплексный анализ Генерального соглашения о торговле услугами (GATS)

применительно к высшему образованию см.: Tilak J (2011) Trade in higher education: The role of the General Agreement on Trade in Services (GATS). Paris: UNESCO, International Institute for Educational Planning. Адрес в Интернете: http://unesdoc.unesco.org/images/0021/002149/214997e.pdf [просмотрено 7 августа 2018 г.].

[25] Knight J (2015) Trade creep: Implications of GATS for higher education policy // International Higher Education 28, pp. 5—7. Адрес в Интернете: http://ejournals.bc.edu/ojs/index.php/ihe/article/view/6658 [просмотрено 7 августа 2018 г.].

[26] Список организаций и работ, связанных с выработкой рекомендаций и стандартов в области интернет-обучения см.: WBTIC (no date) Overview of E-learning Standards. Адрес в Интернете: http://wbtic.com/primer_standards.aspx [просмотрено 7 августа 2018 г.].

[27] European Commission (no date) ECTS. Адрес в Интернете: http://ec.europa.eu/education/tools/ects_en.htm [просмотрено 7 августа 2018 г.].

[28] UMAP (no date) UMAP. Адрес в Интернете: http://umap.org/about/ [просмотрено 7 августа 2018 г.].

[29] WSIS Forum (2015) WSIS-SDG Matrix: Linking WSIS Action Lines with Sustainable Development Goals. Geneva: International Telecommunication Union. Адрес в Интернете: https://www.diplomacy.edu/blog/googlestop-thinking-me [просмотрено 7 августа 2018 г.].

[30] W3Techs (2016) Usage of content languages for websites. Адрес в Интернете: https://w3techs.com/technologies/overview/content_language/all [просмотрено 7 августа 2018 г.].

[31] British Academy Policy Centre (2011) Language Matters More and More. Адрес в Интернете: http://www.ucml.ac.uk/sites/default/files/pages/160/Language%20Matters%20more%20and%20more.pdf [просмотрено 7 августа 2018 г.].

[32] The Broadband Commission for Digital Development (2015) The State of Broadband 2015: Broadband as a Foundation for Sustainable Development. Адрес в Интернете: http://www.broadbandcommission.org/Documents/reports/bb-annualreport2015.pdf [просмотрено 7 августа 2018 г.].

[33] Wood J. Top languages of the Internet, today and tomorrow // Unbabel, 10.06.2015. Адрес в Интернете: https://unbabel.com/blog/top-languages-of-the-internet/ [просмотрено 7 августа 2018 г.].

[34] Обзор программы IDN и последнюю информацию о ее реализации см.: ICANN (no date) Internationalized Domain Names. Адрес в Интернете: https://www.icann.org/resources/pages/idn-2012-02-25-en [просмотрено 7 августа 2018 г.].

[35] UNESCO (2001) Universal Declaration on Cultural Diversity. Адрес в Интернете: http://portal.unesco.org/en/ev.php-URL_ID=13179&URL_DO=DO_TOPIC&URL_SECTION=201.html [просмотрено 7 августа 2018 г.].

[36] European Commission (no date) Multilingualism. Адрес в Интернете: http://ec.europa.eu/languages/index_en.htm [просмотрено 7 августа 2018 г.].

[37] World Bank (2016) World Development Report 2016: Digital Dividends. Адрес в Интернете: http://www.worldbank.org/en/publication/wdr2016 [просмотрено 7 августа 2018 г.].

[38] Creative Commons — некоммерческая организация, занимающаяся разработкой, поддержкой и развитием правовой и технической инфраструктуры с целью содействия творческой деятельности в Интернете, обмену знаниями и инновациям. Адрес в Интернете: http://creativecommons.org/ [просмотрено 7 августа 2018 г.].

[39] Broeders D (2015) The Public Core of the Internet. Amsterdam: Amsterdam University Press. Адрес в Интернете: https://www.wrr.nl/binaries/wrr/documenten/policy-briefs/2015/04/10/the-public-core-of-the-internet/WRR_Policy_Brief__2015__The_Public_Core_of_the_Internet.pdf [просмотрено 7 августа 2018 г.].

Раздел 8

Права человека

Права человека

Основной набор связанных с Интернетом прав человека включает в себя право на неприкосновенность частной жизни, на свободу выражения убеждений, на получение информации, на образование, различные права, защищающие культурное и языковое разнообразие, и права меньшинств. В контексте регулирования цифровых технологий не меньшее значение имеет обеспечение прав детей, а также прав, которыми пользуются журналисты и СМИ.

Хотя вопросы прав человека важны сами по себе (например, свобода выражения убеждений и неприкосновенность частной жизни в Интернете), они также включены в такие «сквозные» темы, как сетевой нейтралитет (право на доступ к информации, свобода выражения убеждений, анонимность), кибербезопасность (соблюдение прав человека при мероприятиях, направленных на обеспечение кибербезопасности), контроль над содержанием материалов Интернета и т. д.

Права человека в «реальном» и виртуальном мире

В резолюциях Генеральной Ассамблеи ООН и Совета по правам человека ООН, а также в аналогичных документах таких региональных организаций, как Совет Европы и Европейский Союз, зафиксирован принцип, согласно которому права человека, которыми обладают люди в «реальном» мире, должны быть обеспечены и в виртуальном пространстве. В Хартии прав в Интернете (Internet Rights Charter) Ассоциации прогрессивных коммуникаций говорится, что связанные с Интернетом права человека являются неотъемлемой частью системы ООН по защите прав человека, в основе которой лежит Всеобщая декларация прав человека и другие документы по данной тематике[1].

Хотя вопрос о соотношении прав человека в «реальном» мире и в Интернете представляется решенным, применение таких норм в виртуальном

пространстве вызывает определенные проблемы. Сторонники подхода, согласно которому в Интернете должны действовать особые правила, утверждают, что ситуация в сети качественно отличается от реального мира, хотя бы в силу объема коммуникаций (то есть интенсивности контактов, количества сообщений). Так, при попытках пресечения ненавистнических высказываний проблема состоит не в том, приняты или не приняты в этом отношении соответствующие нормы, а в том, что в Интернете ненавистнические высказывания быстро распространяются, и это придает проблеме иной юридический смысл. Все больше людей становятся свидетелями или жертвами ненавистнической риторики на многочисленных интернет-ресурсах, а применение существующих нормативно-правовых требований в этой области не отличается эффективностью. Таким образом, складывается ситуация, когда правила существуют и действуют, но их применение в Интернете сопряжено с трудностями.

Технологии и права человека

Технические стандарты и протоколы оказывают воздействие на осуществление прав человека. Системы защиты, функционирующие в Интернете на техническом уровне, создаются при участии поставщиков инфраструктуры, производителей устройств и органов по стандартизации. Механизмы криптографической защиты и такие протоколы, как «Не отслеживать» (Do Not Track), могут использоваться по умолчанию для обеспечения неприкосновенности частной жизни и свободы выражения мнений.

В качестве примера можно привести спор о функционировании системы доменных имен DNS. Причиной разногласий стал домен верхнего уровня .sucks (в переводе на русский «отстой», «туфта», «лажа» — прим. пер.), появление которого было санкционировано решением ICANN от февраля 2015 г. Некоторые выступили против работы такого домена, ссылаясь на возможность вымогательства (необходимость приобретать домены второго уровня типа [название бренда].sucks), тогда как другие расценили этот факт как осуществление права на свободное выражение своего мнения. Подобные

случаи положили начало активному обсуждению вопроса о том, должна ли ICANN как организация, занимающаяся, по сути, техническими вопросами, нести ответственность за осуществление прав человека. В 2016 г. была принята новая версия устава ICANN, признающая права человека в качестве одной из основных ценностей, которыми должна руководствоваться организация в своей деятельности и в ходе принятия решений. В уставе говорится, что ICANN обязана уважать «права человека, признанные на международном уровне, в соответствии с требованиями применимого законодательства». В то же время подчеркивается, что включение прав человека в перечень основных ценностей в уставе организации не означает, что на ICANN возлагаются какие-то новые обязательства помимо ее задачи («координация глобальных систем уникальных идентификаторов Интернета на общем уровне, в частности, обеспечение стабильной и безопасной работы этих систем») и обязательств согласно действующему законодательству[2].

Появление «новых» прав человека благодаря Интернету

Право на доступ

Первой страной, гарантировавшей право на доступ в Интернет законодательным путем, стала Эстония, где соответствующая норма действует с 2000 г. С июля 2010 г. всем жителям Финляндии предоставлено право на мегабитный широкополосный доступ в Интернет (в ноябре 2015 г. норма была увеличена вдвое до 2 мегабит в секунду). Аналогичные меры по обеспечению гарантированного доступа в Интернет были приняты в ряде других стран[3]. Однако пока в мировом сообществе нет единого мнения по вопросу о признании доступа в Интернет в качестве права человека. Одни считают, что право на доступ в Интернет несопоставимо с правом на чистую воду, питание и удовлетворение других насущных потребностей, тогда как другие утверждают, что доступ в Интернет зачастую представляет необходимую предпосылку для осуществления других основных прав человека.

Вопрос о праве на доступ в Интернет привлек внимание мирового сообщества в связи с обсуждением сетевого нейтралитета и практики предоставления бесплатного доступа в Интернет. О каком доступе идет речь при обсуждении такого права? Можно ли считать осуществлением такого права предоставление доступа к ограниченному кругу сайтов и платформ, как это делается в рамках бесплатных приложений? Правительство Индии ответило на этот вопрос отрицательно, запретив предоставление таких услуг. Спор по этой проблеме в ряде стран продолжается. Пока не совсем понятно, под каким углом будет рассматриваться этот вопрос: с точки зрения прав человека (право на доступ в Интернет), экономики (новая модель коммерческой деятельности) или развития (помощь наименее обеспеченным общинам).

Право на забвение

Право на забвение или, более точно, на деиндексацию, установлено историческим решением Суда Европейского союза по делу C-131/12 «Google Spain SL, Google Inc. против Agencia Española de Protección de Datos (AEPD) и Mario Costeja González (Марио Костехи Гонзалеса)». Дело касалось уведомления о распродаже собственности г-на Костехи с аукциона из-за неуплаченного в 1998 г. долга. Заметка была опубликована в испанской газете La Vanguardia. Г-н Костеха уже давно расплатился по своим долгам, когда в один прекрасный день газета решила оцифровать свой архив. В итоге, одним из первых результатов поиска в Google при наборе имени Костеха было уведомление о торгах. Испанский суд первой инстанции, сославшись на свободу СМИ, постановил, что внесение изменений в архив газеты с целью исключения этих результатов поиска, не требуется. Однако испанское агентство по защите данных (Agencia Española de Protección de Datos) потребовало, чтобы Google удалила ссылку из результатов поиска. Компания Google оспорила это решение в высшей судебной инстанции страны (Audiencia Nacional), которая передала дело на рассмотрение Суда ЕС.

13 мая 2014 г. в ходе вынесения решения против Google Суд ЕС, во-первых, подтвердил свое право на юрисдикцию, поскольку поисковые услуги, которые предоставляются испанским дочерним предприятием компании Google Inc., зарегистрированной в США и являющейся владельцем поиско-

вого алгоритма, «были прибыльны с экономической точки зрения» и подпадали по территориальному признаку под действие Директивы ЕС о защите данных 95/46. Во-вторых, суд установил, что компания Google выступала в качестве контроллера обработки данных, и что деятельность компании заключалась в «обнаружении информации, опубликованной или размещенной в Интернете третьими лицами, осуществлении автоматического индексирования, временного хранения такой информации и, наконец, ее предоставления интернет-пользователям в соответствующей последовательности». В-третьих, суд потребовал от Google, как контроллера обработки данных на территории государств – членов ЕС, соблюдения Директивы о защите данных в целях «удаления из перечня результатов, выдаваемых при введении поискового запроса по имени лица, ссылок на интернет-страницы, опубликованные третьими лицами, в которых содержится информация о таком лице, а также в случае, если такое имя или информация не удалены заблаговременно или одновременно с этих интернет-страниц, и даже если публикация на этих страницах законна»[4]. Кроме того, суд признал, что в тех случаях, когда речь идет об общественных интересах, контроллер обработки данных обязан рассмотреть вопрос о том, должна ли та или другая ссылка оставаться доступной.

Это разбирательство привело к применению Судом ЕС нового подхода, основанного на обработке данных в зависимости от местонахождения пользователя, вне зависимости от места расположения сервера или регистрации компании[5]. Решение вызвало широкий резонанс и оставалось яблоком раздора на протяжении нескольких месяцев. Право на забвение снова оказалось в центре внимания, когда парижский Суд высокой инстанции вынес решение, которое предусматривало возможность применения данной нормы по всему миру, после чего Google был вынужден проводить деиндексацию результатов поиска в ЕС (google.it, google.fr), чтобы сделать результаты поиска, доступные через google.com, недоступными в Европе[6].

Кроме того, ЕС решил на этом не останавливаться и включил право на забвение в свое законодательство, для чего вместо Директивы 1996 г.[7] принял Общий регламент по защите данных (General Data Protection Regulation), который вступает в силу в мае 2018 г. В нем содержатся отдельные положения о «праве на удаление (праве на забвение)». Согласно документу, физические лица наделяются правом потребовать удаления своих персональных данных по определенным основаниям, а на контроллера возлагается обязанность оперативно удалить такие данные. Кроме того, при обнародовании контроллером персональных данных необходимо предпринять «разумные действия» по информированию контроллеров, ведущих обработку соответствующих данных, что субъект данных потребовал удаления любых ссылок на такие персональные данные и запрещает копировать или воспроизводить их.

По вопросу о регулировании права на забвение существуют две противоположные точки зрения. Одни эксперты считают такие меры усилением права на неприкосновенность частной жизни и защиты данных, поскольку регламентом предусмотрена процедура запроса на удаление данных, которые были собраны и хранятся интернет-компаниями. Другие рассматривают право как угрозу для свободы выражения мнений, если регламентом допускается удаление материалов, в которых не содержится нарушений прав других лиц[8]. Пока неясно, как сложится правоприменительная практика в этой области и какая из двух точек зрения возобладает.

Интернет и существующие права человека

Свобода выражения убеждений и право искать, получать и распространять информацию

В последние годы свобода выражения убеждений в Интернете стала одной из основных тем в мире дипломатии. Так, этой темой активно занимается Совет по правам человека ООН и региональные межправительственные организации, в частности, Совет Европы. Проблематика свободы выражения мнений также постоянно обсуждается в рамках многочисленных международных конференций и форумов, включая Форум по управлению Интернетом.

Один из наиболее комплексных подходов предложила Коалиция свободы в Интернете (Freedom Online Coalition). По состоянию на ноябрь 2016 г.

в эту группа входило 30 стран. Коалиция проводит ежегодные встречи и реализует исследовательские и информационные проекты по тематике свободы выражения мнений в Интернете.

Свобода выражения убеждений в Интернете входит в число наиболее спорных политических вопросов. Это одно из основополагающих прав человека, которое обычно рассматривается в рамках обсуждения политики контроля над материалами Интернета, цензуры и слежки. Кроме того, эта проблематика усложняется по мере применения новых подходов к борьбе с ненавистническими и экстремистскими высказываниями в Интернете, в рамках которых одни поддерживают меры по ограничению свободы слова, а другие выступают против[9]. Однако в настоящее время наметилась тенденция по ограничению свободы слова во имя социальной ответственности[10].

Тема свободы выражения убеждений связана с другими вопросами управления Интернетом, включая криптографическую защиту данных и анонимность, сетевой нейтралитет и права на интеллектуальную собственность. Некоторые из этих вопросов рассматриваются в докладах Специального докладчика по вопросу о поощрении и защите права на свободу мнений и их свободное выражение, в которых неоднократно подчеркивалась важность защиты права свободно выражать свое мнение в Интернете. Тема свободы выражения мнений также затрагивается в дискуссиях о правах человека и доступе к Интернету.

Свобода выражения мнений гарантирована рядом международных документов, включая Всеобщую декларацию прав человека (статья 19) и Международный пакт о гражданских и политических правах (статья 19), а также таких региональных документах, как Европейская конвенция по правам человека (статья 10) и Американская конвенция по правам человека (статья 13).

Во Всеобщей декларации прав человека ООН свободе выражения убеждений противопоставляется право государства ограничивать такую свободу в интересах удовлетворения справедливых требований морали, общественного порядка и общего благосостояния (статья 29). Таким образом, и обсуждение, и претворение в жизнь статьи 19 следует рассматривать в контексте достижения должного баланса между двумя этими потребностями[11]. Такая двусмысленная ситуация делает возможным неоднозначное толкование норм и их различное применение. Конфликт между статьями

19 и 29 в «реальном» мире находит отражение и в дискуссиях о поиске правильного баланса в Интернете.

Основной механизм регулирования свободы выражения мнений в Интернете зафиксирован в резолюции Совета по правам человека ООН о защите свободы выражения мнений в Интернете (2012).

Свобода выражения мнений привлекает особое внимание неправительственных организаций правозащитного толка, включая Human Rights Watch, Amnesty International и Freedom House. Например, Freedom House занимается оценкой уровня свободы при использовании Интернета обычными пользователями в некоторых странах. В исследовании Freedom on the Net за 2016 г. отмечается, что уже шестой год подряд положение со свободой в Интернете усугубляется, при этом ухудшение показателей наблюдается в половине из 65 стран, включенных в исследование. Это связано с цензурой и ограничением использования определенных интернет-услуг, арестами пользователей социальных сетей, ведением массовой слежки, а в некоторых случаях с отключением доступа к Интернету[12].

Тайна частной жизни и защита данных[13]

Темы обеспечения неприкосновенности частной жизни и защиты данных связаны с рядом аспектов управления Интернетом, включая права человека, развитие инфраструктуры (разработка стандартов управления данными), безопасность (доступ к данным из соображений национальной безопасности и борьбы с преступностью) и экономику (обработка данных как модель ведения коммерческой деятельности).

Защита права на неприкосновенность частной жизни и защита данных — аспекты управления Интернетом, тесно связанные между собой. Обычно под принципом неприкосновенности частной жизни понимается право любого гражданина контролировать личную информацию и принимать решения относительно нее (раскрывать либо не раскрывать эту информацию). Право на неприкосновенность частной жизни входит в число основных прав человека. Оно признается во Всеобщей декларации прав человека, в Международ-

ном пакте о гражданских и политических правах и многих других международных и региональных конвенциях по вопросам прав человека.

Границы понятия «частная жизнь» зависят от различий в национальной культуре и образе жизни. Так, соблюдению права на неприкосновенность частной жизни уделяется большое внимание в западных странах, особенно в Германии. Современные определения этого понятия делают акцент на тайне коммуникации (отсутствие слежки за перепиской) и защите частной информации (нераскрытие информации о частных лицах). Покушения на неприкосновенность раньше сводились к действиям государства, однако в последнее время отмечается все больше и больше случаев нарушения этого права со стороны частного сектора.

Вопросы

Для анализа основных вопросов, связанных с правом на неприкосновенность частной жизни, рассмотрим схему (рис. 24), где отношения между физическими лицами, государством и компаниям изображены в виде треугольника.

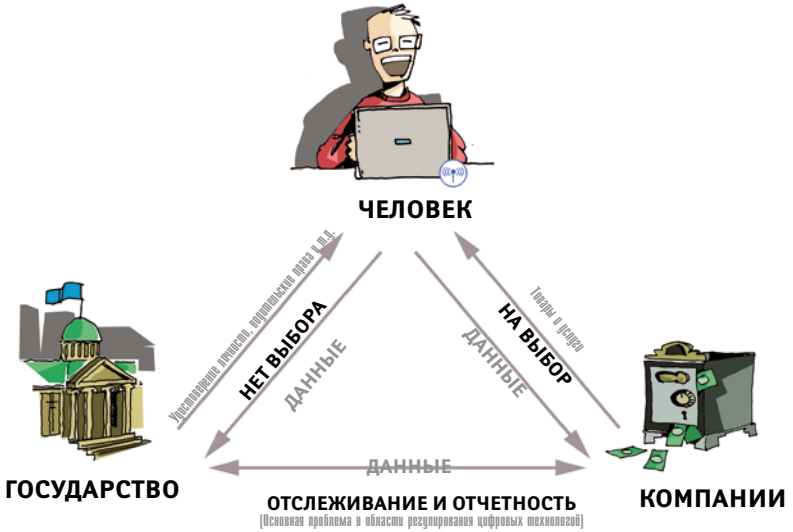


Рисунок 24. Право на неприкосновенность частной жизни в эпоху цифровых технологий

Защита права на неприкосновенность частной жизни: частные лица и государство

Информация всегда была для органов власти крайне важным инструментом контроля над территорией и населением. Правительства собирают большие объемы личной информации (данные регистрации рождений и браков, номера в системе социального страхования, данные о регистрации в качестве избирателя, судимости, налоговую информацию, данные учета жилых помещений, регистрации автомобилей и т. д.). Граждане не имеют возможности отказаться от предоставления этой информации государству, если только не эмигрируют в другую страну, где им все равно придется поделиться своими данными, только уже с другим государством. Информационные технологии, используемые для глубинной обработки данных[14], позволяют интегрировать данные из разных специализированных систем (например, налоговой, учета жилья и автомобилей) для проведения сложных аналитических процедур, поиска закономерностей и выявления несоответствий (рис. 25).

Одной из основных сложностей для любых инициатив в области электронного правительства является обеспечение надлежащего равновесия между модернизацией правительственных функций и обеспечением гарантий прав граждан на неприкосновенность частной жизни, включая введение ограничений, предусматривающих сбор только той информации, которая необходима для осуществления законных государственных функций и оказания услуг. Между тем в последние годы интерес государственных органов к сбору и расширению перечня сведений, обязательных для установления личности (биометрические данные), только возрастает.

Принятый в США после событий 11 сентября 2001 г. «Патриотический акт» (Patriot Act)[15] и аналогичные законы в других странах расширили полномочия правительственных органов в области сбора информации, включая право на законный перехват информации. Концепция законного перехвата с целью сбора улик также включена в Конвенцию по киберпреступности (статьи 20 и 21) Совета Европы.

Защита права на неприкосновенность частной жизни: частные лица и бизнес

Второй стороной треугольника, иллюстрирующего различные компоненты защиты частной жизни (рис. 24), являются взаимоотношения между частными лицами и бизнесом. Человек сообщает личную информацию о себе, открывая счет в банке, бронируя авиабилеты или отель, расплачиваясь в Интернете кредитной картой и просто работая в Интернете. В каждой из этих ситуаций остаются многочисленные «следы».

Рисунок 25. Интеллектуальный анализ данных

Успех и стабильность электронной коммерции, как между организациями (сегмент B2B), так и между организациями и частными лицами (сегмент B2C), зависят от доверия к политике обеспечения неприкосновенности частной жизни, принятой компанией, и к мерам безопасности, предпринимаемым для защиты конфиденциальной информации о клиентах от кражи и злоупотреблений. С распространением социальных сетей (например, Facebook, Twitter) появляются опасения, что хранящиеся в них личные данные однажды могут быть использованы не по назначению — не только владельцами сервисов или их администраторами, но и другими пользователями этих сетей[16]. Кроме того, интернет-компании достаточно часто вносят изменения в политику конфиденциальности, не оставляя пользователям особого выбора: либо принять изменения, либо прекратить пользоваться ресурсом[17].

В условиях информационной экономики данные о потребителях, их предпочтениях и истории покупок стали ценным товаром. Некоторые компании, в том числе Facebook, Google и Amazon, сделали информацию о предпочтениях потребителей краеугольным камнем своей бизнес-модели. По сути, пользователи оплачивают якобы бесплатные интернет-услуги своими персональными данными, будь то файлы-cookie их браузеров об истории посещения сайтов либо конкретная информация, полученная при заполнении различных формуляров или осуществлении платежей. Пользователи дают о себе все больше сведений, и количество все более сложных и изощренных[18] нарушений неприкосновенности частной жизни продолжает расти.

Защита права на неприкосновенность частной жизни: государство и бизнес

О третьей стороне треугольника известно меньше всего, хотя это, может быть, самый значимый аспект, связанный с защитой права на неприкосновенность частной жизни. Обе стороны — и государство, и бизнес — собирают значительный объем информации о частных лицах. Государство оказывает огромное давление на интернет-компании (например, на Facebook, Google), чтобы получить доступ к данным, которые можно использовать в борьбе с терроризмом и преступностью. Так, после терактов ноября 2015 г. в Париже французские власти активно использовали данные, предоставленные интернет-компаниями. Аналогичным образом, появление в интернет-отрасли все более сложных решений по шифрованию данных не может не беспокоить уполномоченные органы, поскольку это ограничивает их возможности по отслеживанию интернет-трафика.

Деловое сообщество предпринимает попытки противостоять давлению и ограничить доступ государства к их данным. Предоставление доступа к коммерческой информации негативно скажется на бизнесе интернет-компаний и подорвет доверие со стороны пользователей. В обозримом будущем противоречия между государством и компаниями в этой сфере будут оставаться одной из основных проблем регулирования цифровых технологий в мире.

Защита права на неприкосновенность частной жизни: граждане

Последним аспектом вопроса о защите неприкосновенности тайны частной жизни, не вошедшим в схему-треугольник, является потенциальная угроза, исходящая от самих граждан. Сегодня любой человек, располагающий достаточными финансами, может приобрести мощные средства ведения слежки. Даже простые мобильные телефоны с камерами могут выполнять такую функцию. Технический прогресс, по выражению одного из авторов журнала The Economist, «демократизировал слежку»[19]. Известно много случаев нарушения права на неприкосновенность частной жизни одних людей другими — от простого подглядывания за соседями до более изощренного использования камер с целью записи номеров банковских карт и электронного шпионажа.

Проблема с защитой от подобных нарушений состоит в том, что большинство законодательных положений касались угроз для неприкосновенности со стороны государства или частных компаний. Новые реалии побудили ряд стран предпринять шаги для решения этой проблемы. Конгресс США принял Акт о предотвращении видеовуайеризма, запрещающий фотографировать обнаженных людей без их согласия[20]. Германия и ряд других стран также приняли аналогичные законы, ограничивающие возможности слежки одних частных лиц за другими.

Международное регулирование в области защиты права на неприкосновенность частной жизни и конфиденциальных сведений

Одним из основных международных документов, регулирующих защиту права на неприкосновенность частной жизни и конфиденциальных данных, является Конвенция о защите физических лиц при автоматической обработке персональных данных, принятая Советом Европы в 1981 г.[21] Конвенция открыта для подписания и другими государствами, в том числе не входящими в Совет Европы. Поскольку Конвенция является технологически нейтральной, она выдержала испытание временем.

В Европейском союзе правовая основа для обработки личных данных заложена Директивой ЕС о защите данных (Directive 45/46/EC) 1995 г.[22], которая оказала значительное влияние на формирование национального законодательства не только в ЕС, но и по всему миру. В рамках реформ, направленных на приведение нормативно-правовой базы в соответствие с требованиями времени, в 2016 г. в ЕС принят Общий регламент по защите данных, которые вступит в силу в мае 2018 г. и заменит Директиву 1995 г.[23]

Еще одним ключевым международным документом по вопросам защиты права на неприкосновенность частной жизни и личных данных, не носящим обязательного характера, являются «Основные принципы защиты тайны частной жизни и трансграничных потоков личных данных», подготовленные Организацией экономического сотрудничества и развития (ОЭСР) в 1980 г. Обновленная версия этого документа была принята в 2013 г.[24] Эти принципы и последующая работа ОЭСР способствовали созданию многих норм международного, регионального и национального уровня в этой области. На сегодняшний день почти все страны ОЭСР приняли законодательство в области защиты права на неприкосновенность частной жизни и наделили свои властные органы соответствующими полномочиями.

Хотя предложенные ОЭСР принципы были приняты во многих странах и регионах, в способе их применения кроются различия. Так, европейский и американский подход к этой теме значительно отличаются друг от друга. В Европе законодательство по защите данных является всеобъемлющим, в то время как в США правовые нормы, касающиеся конфиденциальности, разрабатываются отдельно для каждой сферы деятельности. В области финансовой тайны это Акт Грэмма-Лича-Блайли, в сфере конфиденциальности в отношении детей — Акт о защите частной жизни детей в Интернете, конфиденциальность медицинской информации призван обеспечить пакет законов о здравоохранении и социальном обеспечении.

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

Соглашение о правилах обмена конфиденциальной информацией между ЕС и США

Различные подходы США и ЕС к защите права на неприкосновенность частной жизни породили ряд вопросов, большинство которых связаны с обработкой персональных данных частными компаниями. Каким образом ЕС может обеспечить защиту данных своих граждан в соответствии с действующими нормами? В соответствии с какими предписаниями (американскими или европейскими) нужно обращаться с информацией, переправляемой внутри компании по корпоративным сетям из ЕС в США? Евросоюз угрожал заблокировать передачу данных в страны, не способные обеспечить уровень защиты информации, соответствующий директиве. Такая позиция неизбежно вела к конфликту с американским подходом.

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

Концепция «безопасной гавани» легла в основу нормативно-правовой базы, регулирующей обмен информацией между ЕС и США. При ее разработке была предпринята попытка сделать так, чтобы в отношении защиты данных граждан ЕС действовали правила ЕС, даже если данные были размещены на серверах в США. Это соглашение позволило распространить действие правил ЕС на американские компании. Американские компании, работающие с данными о гражданах стран Евросоюза, могли добровольно принять на себя обязательства выполнять требования по защите конфиденциальности, принятые в ЕС. Подписав соответствующие соглашения, компании должны следовать формальным механизмам их выполнения, согласованным между США и ЕС. За 15 лет свыше 4 400 компаний приняли участие в законной передаче данных из ЕС в США в рамках соглашения о «безопасной гавани».

Однако в октябре 2015 г. Суд Евросоюза признал соглашение о «безопасной гавани» недействительным, решив, что Европейская комиссия не удостоверилась должным образом, обеспечивает ли США «по сути эквивалентный» уровень защиты данных граждан ЕС[25]. Это решение вынудило американских и европейских дипломатов сесть за стол переговоров, чтобы выработать новый механизм. Результатом их усилий стало Соглашение о правилах обмена конфиденциальной информацией между ЕС и США, которое было одобрено государствами – членами ЕС в июле 2016 г. При этом четыре страны — Австрия, Болгария, Хорватия и Словения — воздержались. В том же месяце Европейская Комиссия приняла официальное решение, подтвердив действительность Соглашения о правилах обмена конфиденциальной информацией между ЕС и США[26].

Соглашение предусматривает ужесточение требований к американским компаниям по защите персональных данных граждан ЕС и требование к властям США осуществлять более тщательный контроль над исполнением новых положений. Кроме того, Соглашение о правилах обмена конфиденциальной информацией между ЕС и США решает еще одну давнюю проблему. Речь идет о доступе властей США к персональным данным граждан ЕС. В соглашении зафиксированы гарантии американской стороны в отношении осуществления доступа под контролем и при условии соблюдения соответствующих ограничений. Кроме того, США обязались сотрудничать с органами ЕС по вопросам защиты конфиденциальной информации и учредить пост уполномоченного, который будет отвечать за рассмотрение претензий физических лиц касательно доступа американских властных структур к персональным данным пользователей и принятие соответствующих мер.

Права детей в цифровом мире

Интернет дает детям немалые преимущества, но в то же время создает многочисленные риски. Чтобы дети могли получать максимальную пользу, находясь в безопасной среде, необходимо найти равновесие между защитой от рисков и соблюдением прав детей в цифровом мире, включая право на доступ к информации и свободу слова.

Подробнее о вопросах безопасности применительно к использованию Интернета детьми см. ***Раздел 3.***

Краеугольным камнем системы по защите прав детей считается Конвенция ООН о правах ребенка (United Nations Convention on the Rights of the Child — CRC)[27], которая лидирует среди международных конвенций по числу ратификаций. На данный момент ее ратифицировали все государства – члены ООН, за исключением США.

В Конвенции о правах ребенка впервые дети рассматриваются как обладатели прав человека. В основе конвенции лежат четыре основополагающих принципа:

- Дети не должны страдать от дискриминации.
- Политические меры должны приниматься в интересах детей.
- Детям должна быть предоставлена возможность раскрыть свой потенциал.
- Взгляды и мнения детей важны и должны быть услышаны.

Вопрос о правах детей рассматривается в конвенции в трех измерениях, которые на английском языке получили название трех «П» (3 Ps): предоставление (provision), защита (protection) и продвижение (promotion) (или участие – participation) прав.

Вопросы

Охранительный подход

В вопросах защиты детей в сети центральное место обычно отводится охранительным аспектам использования технологий. Так, многие утверждают, что появление Интернета и новых технологий повышают риски для детей, соответственно, Интернет может пойти на пользу ребенку только при условии преодоления таких рисков. Однако меры, сводящиеся исключительно к борьбе с рисками, могут помешать использовать Интернет для расширения возможностей детей.

Существует также правовой подход, в основе которого лежат права детей, гарантированные такими документами, как Конвенция ООН о правах ребенка. Этот подход призван обеспечить детям и молодежи возможность максимально воспользоваться преимуществами цифрового мира, одновременно защищая их от сопутствующих рисков. Сохраняя необходимое равновесие между правами детей в мире цифровых технологий и обеспечением безопасности, этот подход становится все более популярным среди экспертов.

Применимость Конвенции ООН о правах ребенка в виртуальном мире

Конвенция ООН о правах ребенка была единогласно принята в 1989 г., то есть до начала массового использования Интернета. Применима ли эта конвенция к миру интернет-технологий и, если ответ положительный, каким образом?

В 2012 г. Совет по правам человека ООН принял резолюцию о продвижении, защите и осуществлении прав человека в Интернете[28], поставив точку в споре о том, следует ли в Интернете руководствоваться уже сформулированными правами человека или необходимо разработать новые правила. По мнению экспертов, несмотря на значимость этого достижения, необходимо продолжать работу, поскольку защита прав детей требует особого подхода[29].

В частности, Конвенция ООН о правах ребенка содержит универсальный свод принципов и норм по осуществлению прав детей в «реальном» мире. Аналогичный уровень защиты можно обеспечить путем дальнейшей разработки соответствующих принципов конвенции применительно к Интернету в виде свода руководящих принципов[30].

Конвенция ООН о правах ребенка налагает на правительства обязанность действовать наилучшим образом в интересах детей и служит основой для разработки мер и стратегий в этой области.

Права людей с ограниченными возможностями[31]

По оценкам Всемирной организации здравоохранения (ВОЗ), в мире насчитывается около 1 миллиарда людей с ограниченными возможностями[32]. Это число постоянно возрастает в результате старения населения, появления новых болезней, хронических заболеваний, вооруженных конфликтов и насилия, бедности и нездоровых жизненных условий, а также отсутствия знаний, касающихся инвалидности, ее причин, профилактики и лечения[33].

Интернет открывает новые возможности для включения инвалидов в жизнь общества. Чтобы максимизировать потенциал технологий с точки зрения помощи людям с ограниченными возможностями, необходима разработка соответствующей модели управления Интернетом. Основным международным документом в этой области является Конвенция о правах инвалидов (Convention on the Rights of Persons with Disabilities — UNCRPD), принятая ООН в 2006 г. Закрепленные в этой Конвенции права сейчас включаются в национальные системы законодательства, что в перспективе сделает возможным обеспечение их соблюдения[34].

Осознание необходимости учитывать потребности людей с ограниченными возможностями при проектировании технологических решений постепенно растет благодаря работе таких организаций, как Динамическая коалиция IGF по вопросам доступности и инвалидности[35], Секция по ограниченным возможностям и специальным потребностям Общества Интернета и Международный центр интернет-ресурсов для инвалидов.

Проблема доступности интернет-технологий для инвалидов обусловлена разрывом между навыками, необходимыми для использования аппаратного и программного обеспечения и материалов, с одной стороны, и ресурсами и физической способностью инвалида их использовать — с другой. Создать соответствующие возможности можно за счет работы в двух направлениях:

- необходимо включать стандарты доступности в требования к дизайну оборудования, ПО и материалов Интернета;
- нужно повышать доступность дополнительного оборудования и ПО, усиливающих или заменяющих определенные физические способности пользователя с ограниченными возможностями.

С точки зрения управления Интернетом в центре внимания находится вопрос о возможности использования материалов Интернета и приложений людьми с ограниченными возможностями. Международные стандарты доступности для Интернета были разработаны Консорциумом «всемирной паутины» (W3C) в рамках Инициативы по доступности сети (Web Accessibility Initiative — ИДС). Несмотря на существующие стандарты, многие интернет-приложения все еще не соответствуют установленным требованиям, что обусловлено рядом причин, включая недостаточную информированность, субъективную сложность и высокую стоимость таких решений.

Гендерный аспект прав человека в Интернете

Под правами женщин понимается широкий спектр вопросов, связанных как с доступом в Интернет (например, с насилием в Интернете), так и с его отсутствием (например, утраченные возможности в том, что касается доступа к информации, образования, бизнеса и политической деятельности).

Исторически так сложилось, что девочки и женщины сталкиваются с дискриминацией и вопиющим неравенством в образовании (включая возможность специализации в области ИКТ), здравоохранении, социальном обеспечении, политическом участии и правосудии. В сети проблема неравенства между мужчинами и женщинами в плане соблюдения их основных прав не менее актуальна. Насилие, миграционные потоки, конфликты и кризисы влияют на положение женщин и возможности реализации их потенциала как в «реальном», так и в виртуальном пространстве, и сугубо негативным образом сказываются на их личной жизни.

Женщины составляют свыше половины мирового населения, однако их участие в процессах, связанных с использованием технологий, явно недостаточно. Защита прав женщин в сети является частью более широкого движения в социокультурной и профессиональной сфере по борьбе с дискриминацией и предвзятостью в вопросах осуществления прав человека, включая предоставление женщинам равных возможностей при получении образования и участии в экономической жизни, занятии должностей и оплаты труда.

Несмотря на повышение доступности Интернета за последние два десятилетия, неравенство возможностей сохраняется в силу гендерного фактора, что приводит к существенному отставанию с точки зрения расширения прав и возможностей женщин и девочек по всему миру. По данным МСЭ за 2016 г., глобальный разрыв среди интернет-пользователей по гендерному признаку увеличился с 11% в 2013 г. до 12% в 2016 г. При этом самые высокие показатели (31%) сохраняются в наименее развитых странах, где потребность в доступе к Интернету ощущается наиболее остро. Эти данные также свидетельствуют о том, что наибольший гендерный разрыв наблюдается в Африке (23%), а наименьший на американском континенте (2%)[36].

По данным исследования Web Foundation, повышение доступности мобильных телефонов недостаточно для увеличения числа женщин, пользующихся Интернетом, или для «расширения прав и возможностей женщин посредством технологий». Хотя телефон есть у большинства женщин и мужчин, всего лишь 37% женщин могут воспользоваться доступом в Интернет (тогда как аналогичный показатель для мужчин в тех же сообществах превышает 50%). Вероятность использования Интернета женщинами в экономической или политической деятельности на 30-50% ниже, чем у мужчин. Кроме того, исследование свидетельствует о том, что показатели доступа в Интернет тесно связаны с уровнем образования. Это следует учитывать при разработке и реализации мер, направленных на обеспечение позитивных изменений[37].

Роль женщин в общественной и политической жизни растет по мере более активного использования Интернета. Однако для того, чтобы в полной мере раскрыть потенциал ИКТ, необходимо устранить ряд сдерживающих факторов, включая неравенство в доступе и насилие против женщин в сфере технологий. В число актов насилия, от которых страдают женщины в сети, входят виртуальное преследование, ведение слежки и нарушение неприкосновенности частной жизни, сексуальные домогательства, незаконное использование персональных данных и манипуляция ими, включая изображения и видеоматериалы. В эпоху повсеместной доступности Интернета повышение безопасности в виртуальном пространстве при содействии интернет-операторов могло бы стать первым шагом на пути к полному соблюдению прав женщин и расширения их возможностей.

Специальный докладчик ООН по вопросу о насилии в отношении женщин, его причинах и последствиях в своем докладе за 2016 г. подчеркнул, что насилие против женщин в сети является новой проблемой. В докладе говорится, что «использование информационно-коммуникационных технологий способствовало не только расширению прав и возможностей женщин и девочек, но и появлению феномена насилия в сети». Докладчик обращается к государствам и негосударственным субъектам с призывом «бороться с насилием против женщин и девочек в Интернете, соблюдая при этом право свободно выражать свое мнение и запрет на пропаганду насилия и ненависти в соответствии со статьей 20 Международного пакта о гражданских и политических правах»[38].

В число основных документов по защите прав женщин входят Конвенция о политических правах женщин 1952 г. и Конвенция о ликвидации всех форм дискриминации в отношении женщин 1979 г. (CEDAW). Структура Организации Объединенных Наций по вопросам гендерного равенства и расширения прав и возможностей женщин («ООН-женщины») и Совет по правам человека ООН активно занимаются различной правозащитной тематикой, однако вопросам борьбы за соблюдение прав женщин в Интернете пока уделяется недостаточно внимания. Более активную работу по защите прав женщин в сети проводят такие группы, как APC и Динамическая коалиция IGF по вопросам гендерного равенства и управления Интернетом (IGF Dynamic Coalition on Gender and Internet Governance).

По мере развития женского правозащитного движения предпринимаются попытки включить этот вопрос в более широкую гендерную проблематику, включающую права других гендерных меньшинств. Для женщин и других гендерных меньшинств, включая людей нетрадиционной сексуальной ориентации (LGBTQ), такие вопросы, как качество доступа к информации, профессиональные возможности, глобальные политические процессы и осуществление других прав человека являются важнейшим элементом правозащитной тематики в контексте управления Интернетом и требуют соответствующего внимания.

Примечания к разделу 8

[1] Хартия АПК включает следующие положения: доступ к Интернету для всех; свобода собраний и выражения мнений; доступ к знаниям; сотрудничество в обучении и творчестве — разработка программного обеспечения с открытым исходным кодом; защита неприкосновенности частной жизни, защита от слежки, шифрование данных; управление Интернетом; знание, защита и реализация своих прав. Адрес в Интернете: http://www.apc.org/en/node/5677 [просмотрено 7 августа 2018 г.].

[2] Solon O. Why the .sucks domain doesn't have to suck // Bloomberg, 19.08.2015. Адрес в Интернете: https://www.bloomberg.com/news/articles/2015-08-19/why-the-sucks-domain-doesn-t-have-to-suck [просмотрено 7 августа 2018 г.].

[3] ICANN (2016) Bylaws for Internet Corporation for Assigned Names and Numbers. Адрес в Интернете: https://www.icann.org/resources/pages/governance/bylaws-en [просмотрено 7 августа 2018 г.].

[4] Borg-Psaila S (2011) Right to access the Internet: the countries and the laws that proclaim it. Адрес в Интернете: https://www.diplomacy.edu/blog/right-access-internet-countries-and-laws-proclaim-it [просмотрено 7 августа 2018 г.].

[5] CJEU (2014) Judgement of the Court in Case C-131/12: Google Spain SL, Google Inc. v Agencia Española de Protección de Datos (AEPD), Mario Costeja González. Адрес в Интернете: http://curia.europa.eu/juris/liste.jsf?language=en&jur=C,T,F&num=C-131/12&td=ALL [просмотрено 7 августа 2018 г.].

[6] Radu R and Chenou JM (2015) Data control and digital regulatory space(s): towards a new European approach. Internet Policy Review 4(2). Адрес в Интернете: http://policyreview.info/articles/analysis/data-control-and-digital-regulatory spaces-towards-new-european-approach [просмотрено 7 августа 2018 г.].

[7] Bowcott O, Willsher K. Google's French arm faces daily €1,000 fines over links to defamatory article // The Guardian, 13.11.2014. Адрес в Интернете: https://www.theguardian.com/media/2014/nov/13/google-french-arm-fines-right-to-be-forgotten [просмотрено 7 августа 2018 г.].

[8] European Union (2016) Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC. Адрес в Интернете: http://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A32016R0679 [просмотрено 7 августа 2018 г.].

[9] Подробнее о возможных последствиях введения права на забвение см. Keller D. The new, worse 'right to be forgotten' // Politico, 27.01.2016. Адрес в Интернете: http://www.politico.eu/article/right-to-be-forgotten-google-defense-data-protection-privacy/ [просмотрено 7 августа 2018 г.].

[10] Обзор возможных оснований для ограничения экстремистских высказываний, а также аргументов в пользу расширения свободы слова, в том числе свободы выражения маргинальных взглядов, см.: Heinze E (2014) Nineteen arguments for hate speech bans — and against them. Адрес в Интернете: http://freespeechdebate.com/en/discuss/nineteen-arguments-for-hate-speech-bans-and-against-them/ [просмотрено 7 августа 2018 г.].

[11] Poushter J (2015) 40% of millennials OK with limiting speech offensive to minorities. Адрес в Интернете: http://www.pewresearch.org/fact-tank/2015/11/20/40-of-millennials-ok-with-limiting-speech-offensive-to-minorities/ [просмотрено 7 августа 2018 г.].

[12] United Nations (1948) The Universal Declaration of Human Rights. Адрес в Интернете: http://www.un.org/en/documents/udhr/ [просмотрено 7 августа 2018 г.].

[13] Freedom House (2016) Freedom on the Net 2016. Адрес в Интернете: https://freedomhouse.org/report/freedom-net/freedom-net-2016 [просмотрено 7 августа 2018 г.].

[14] Ценные комментарии и идеи для этого раздела предоставила Катитца Родригес, директор по вопросам международного права в Electronic Frontier Foundation (EFF).

[15] UCLA (no date) What is data mining? Адрес в Интернете: http://www.anderson.ucla.edu/faculty/jason.frand/teacher/technologies/palace/datamining.htm [просмотрено 7 августа 2018 г.].

[16] Подробнее о «Патриотическом акте» см.: Electronic Privacy Information Centre (no date) USA Patriot Act. Адрес в Интернете: http://epic.org/privacy/terrorism/hr3162.html [просмотрено 7 августа 2018 г.].

[17] В качестве наглядного примера проблемы конфиденциальности применительно к социальным сетям можно привести давление на компанию Facebook со стороны борцов за соблюдение прав человека в СМИ. Подробнее о различных аспектах использования этой социальной сети см.: Wikipedia (2012) Criticism of Facebook. Адрес в Интернете: http://en.wikipedia.org/wiki/Criticism_of_Facebook [просмотрено 7 августа 2018 г.].

[18] Например, в августе 2016 г. принадлежащая Facebook служба мгновенных сообщений WhatsApp внесла изменения в свою политику конфиденциальности. Принимая пользовательское соглашение WhatsApp, пользователи автоматически соглашались напрямую предоставлять свои данные компании Facebook, в частности, в целях адресной рекламы. Изначально отказаться от предоставления своих данных было невозможно, однако в WhatsApp была предусмотрена возможность частично отказаться от использования Facebook данных в рекламной деятельности. Подробнее см.: Lamas N. WhatsApp to share user data with Facebook for targeting — here's how to opt out // Techcrunch, 25.08.2016. Адрес в Интернете: https://techcrunch.com/2016/08/25/whatsapp-to-share-user-data-with-facebook-for-ad-targeting-heres-how-to-opt-out/ [просмотрено 7 августа 2018 г.].

[19] Обзор наиболее резонансных нарушений права на неприкосновенность частной жизни см.: Lord N. The History of Data Breaches // Digital Guardian, 12.10.2016. Адрес в Интернете: https://digitalguardian.com/blog/history-data-breaches [просмотрено 7 августа 2018 г.].

[20] Move over, Big Brother // The Economist. 02.12.2004. Адрес в Интернете: http://www.economist.com/node/3422918 [просмотрено 7 августа 2018 г.].

[21] Gov.track.us (no date) Video Voyeurism Prevention Act. Адрес в Интернете: https://www.govtrack.us/congress/bills/108/s1301/text [просмотрено 7 августа 2018 г.].

[22] Council of Europe (1981) Convention for the protection of individual with regard to automatic processing of personal data. Адрес в Интернете: http://conventions.coe.int/treaty/en/treaties/html/108.htm [просмотрено 7 августа 2018 г.].

[23] European Union (1995) Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. Адрес в Интернете: http://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A31995L0046 [просмотрено 7 августа 2018 г.].

[24] European Union (2016) Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC. Адрес в Интернете: http://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A32016R0679 [просмотрено 7 августа 2018 г.].

[25] OECD (2013) Revised Guidelines on the Protection of Privacy and Transborder Flows of Per-sonal Data. Адрес в Интернете: http://www.oecd.org/sti/ieconomy/privacy.htm [просмотрено 7 августа 2018 г.].

[26] CJEU (2015) Judgement of the Court in Case C-362/14: Maximilliam Schrems v Data Protection Commissioner. Адрес в Интернете: http://curia.europa.eu/juris/document/document.jsf?text=&docid=169195&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=2015 [просмотрено 7 августа 2018 г.].

[27] European Commission (2016) Commission Implementing Decision on the adequacy of the protection provided by the EU-U.S. Privacy Shield. Адрес в Интернете: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ%3AJOL_2016_207_R_0001 [просмотрено 7 августа 2018 г.].

[28] United Nations (1989) Convention on the Rights of the Child. Адрес в Интернете: http://www.ohchr.org/EN/ProfessionalInterest/Pages/CRC.aspx [просмотрено 7 августа 2018 г.].

[29] UN Human Rights Council (2012) Resolution A/HRC/20/L.13. The promotion, protection and enjoyment of human rights on the Internet. Адрес в Интернете: http://ap.ohchr.org/documents/alldocs.aspx?doc_id=20280 [просмотрено 7 августа 2018 г.].

[30] Livingstone S and Bulgar M (2014) A global research agenda for children's rights in the digital age. Journal of Children and Media 8(4). Адрес в Интернете: http://www.lse.ac.uk/media@lse/WhosWho/AcademicStaff/SoniaLivingstone/pdf/Livingstone-&-Bulger-JOCAM-A-global-research-agenda-for-childrens-rights-

in-the-digital-age.pdf [просмотрено 7 августа 2018 г.].

[31] Обзор применимости положений Конвенции о правах ребенка в цифровой среде см.: Livingstone S and Bulgar M (2014), ibid, and Livingstone S and O'Neill B (2014). Children's rights online: Challenges, dilemmas and emerging directions. In S. van der Hof et al. (Eds) Minding Minors Wandering the Web: Regulating Online Child Safety. Berlin: Springer.

[32] Профессор Национального технологического университета (Буэнос-Айрес) Хорхе Плано поделился с авторами ценными комментариями и соображениями по этому вопросу.

[33] World Health Organization (2015) Disability and Health. Fact sheet No. 352. Адрес в Интернете: http://www.who.int/mediacentre/factsheets/fs352/en/ [просмотрено 7 августа 2018 г.].

[34] Disabled World (no date) Disability Statistics: Facts & Statistics on Disabilities & Disability Issues. Адрес в Интернете: https://webcache.googleusercontent.com/search?q=cache:qcsi60D3_ekJ:https://www.disabled-world.com/disability/statistics/+&cd=2&hl=en&ct=clnk&gl=rs [просмотрено 7 августа 2018 г.].

[35] United Nations (2006) Convention on the Rights of Persons with Disabilities. Адрес в Интернете: https://www.un.org/development/desa/disabilities/convention-on-the-rights-of-persons-with-disabilities.html [просмотрено 7 августа 2018 г.].

[36] Силами Динамической коалиции IGF по вопросам доступности и инвалидности разработаны рекомендации по обеспечению доступности Интернета. Адрес в Интернете: http://www.intgovforum.org/cms/dynamiccoalitions/80-accessibility-and-disability#documents [просмотрено 7 августа 2018 г.].

[37] ITU (2016) ICT Facts and Figures 2016. Адрес в Интернете: http://www.itu.int/en/ITU-D/Statistics/Documents/facts/ICTFactsFigures2016.pdf [просмотрено 7 августа 2018 г.].

[38] Web Foundation (2015) Women's Rights Online: Translating Access into Empowerment. Адрес в Интернете: http://webfoundation.org/about/research/womens-rights-online-2015 [просмотрено 7 августа 2018 г.].

[39] United Nations (2016) Report of the Special Rapporteur on violence against women, its causes and consequences. Адрес в Интернете: http://ap.ohchr.org/documents/dpage_e.aspx?si=A/HRC/32/42 [просмотрено 7 августа 2018 г.].

Раздел 9

Участники процесса управления Интернетом

Участники процесса управления Интернетом

В процесс управления Интернетом вовлечено множество различных участников, которых нередко называют заинтересованными сторонами. К ним относятся национальные органы власти, международные организации, частный сектор, организации гражданского общества, а также научное сообщество и специалисты по технологиям (в соответствии с пунктом 49 Декларации о принципах WSIS 2003 г. и пунктами 35 и 36 Тунисской программы для информационного общества WSIS). В документах WSIS закреплен многосторонний характер управления Интернетом, и основные темы, вокруг которых ведутся дискуссии, касаются распределения ролей и обязанностей между участниками с акцентом на отношения между государственными и негосударственными субъектами применительно к различным аспектам управления Интернетом.

Большинство участников процесса испытывает трудности из-за сложного междисциплинарного характера управления Интернетом, охватывающего техническую, правовую, правозащитную проблематику и социокультурные аспекты. Кроме того, вопросы управления Интернетом могут решаться на различных уровнях: локальном, национальном, региональном или глобальном. В данном разделе рассматривается деятельность основных участников процесса управления Интернетом и приводится обзор их позиций.

> В чем состоит концептуальное различие между управлением Интернетом и другими глобальными политическими процессами?
>
> В области управления Интернетом государствам пришлось адаптироваться к режиму, сформированному неправительственными организациями, включая IETF, Internet Society и ICANN, тогда как в других сферах регулирования (например, изменение климата, торговля, миграция) все было наоборот. При этом возможности участия неправительственных субъектов в межправительственном регулировании постоянно расширяются. Начиная с WSIS 2003 г., когда правительственные структуры начали подключаться к управлению Интернетом, перед участниками стояла задача синхронизировать сформированный усилиями неправительственных организацией режим управления Интернетом с традиционными методами дипломатии. В процессе обнаружились серьезные разногласия, касающиеся роли государственных органов и других участников в управлении Интернетом, и открылись возможности для создания более открытой и эффективной системы регулирования.

Государственные органы

В силу своей центральной роли в мире современных технологий Интернет оказывает влияние на вопросы геополитики (преимущественно национальной безопасности) и геоэкономики (продвижение национальных интересов экономическими средствами). Интернет также способствует росту экономической и социальной взаимозависимости, что требует поиска политических решений путем переговоров и сотрудничества. Вопрос управления Интернетом был включен в международную дипломатическую повестку в период 2003–2005 гг. в рамках процесса WSIS. С тех пор правительства многих стран пытались освоить эту непростую тематику.

Значение Интернета для внутренней политики всех стран заставляет государства прилагать дополнительные усилия для создания эффективной системы управления Интернетом на национальном уровне и активизации работы на дипломатическом фронте по защите своих интересов в сфере цифровых технологий.

Международная деятельность государств развивается в двух основных направлениях. Во-первых, Интернет рассматривается как новый, самостоятельный объект регулирования в различных многосторонних форматах сотрудничества, например ICANN и IGF, а также в рамках таких межправительственных структур, как МСЭ и Группа правительственных экспертов ООН (см., например, табл. 3, где приведены данные об участии стран в работе Группы правительственных экспертов ООН). Во-вторых, государства занимаются цифровыми аспектами традиционных областей регулирования, включая торговлю (в контексте ВТО), здравоохранение (ВОЗ) и труд (МОТ).

Проблемы в области управления Интернетом возникают даже у крупных и богатых стран в силу междисциплинарного характера управления Интернетом (необходимость учитывать технические, экономические и социальные аспекты) и участия в этом процессе различных действующих лиц. Многим правительствам приходится одновременно заниматься подготовкой государственных служащих, разрабатывать нормативно-правовую базу и принимать активное участие в различных международных мероприятиях по вопросам управления Интернетом.

Координация на национальном уровне

В 2003 г., в начале процесса WSIS, в большинстве стран вопросами управления Интернетом занимались министерства связи и соответствующие надзорные органы, то есть те, в чьем ведении находились отношения с МСЭ, основной международной организацией, занимающейся вопросами электросвязи. Постепенно, с ростом роли Интернета в политической, социальной и экономической жизни, к вопросам управления Интернетом стали привлекать и другие ведомства, в том числе учреждения, ведающие вопросами внешней политики, культуры, а также СМИ и органы правосудия.

Основной сложностью для многих государств стала разработка стратегии, направленной на получение и координацию поддержки негосударственных субъектов, обладающих необходимыми для решения вопросов управления Интернетом знаниями — университетов, частных компаний, неправительственных организаций. После WSIS 2003 г. большинству крупных и средних государств из G20 удалось приобрести необходимый институциональный потенциал для мониторинга глобальных переговоров по управлению Интернетом. Некоторые из них, такие как Бразилия, создали инновационные национальные структуры, следящие за дискуссиями по управлению Интернетом по каналам министерств связи, дипломатических ведомств, частного сектора, гражданского и научного сообщества[1]. В качестве примеров можно привести Индию, Индонезию и Кению, где на национальном уровне были созданы системы, обеспечивающие участие различных сторон в процессе управления Интернетом. Во многих странах существуют форумы по управлению Интернетом национального уровня, которые содействуют

вовлечению различных сторон в управление Интернетом и регулирование цифровой политики. По состоянию на октябрь 2016 г. в секретариате глобального Форума по управлению Интернетом было зарегистрировано 47 стран, где действовали национальные форумы по управлению Интернетом[2].

Согласованность политических курсов

Учитывая междисциплинарную природу управления Интернетом и высокую степень разнообразия участников и площадок обсуждения, достижение согласованности политических курсов в этой сфере является крайней сложным. Например, в контексте обеспечения права на неприкосновенность частной жизни и защиты данных необходимо учитывать вопросы прав человека, торговли, стандартизации и безопасности, однако нередко это делается при минимальной координации между ведомствами и группами экспертов (рис. 26). Это управленческая проблема, требующая от правительств гибкого подхода к координации процесса выработки политики, включая горизонтальные коммуникации между различными министерствами, бизнес-кругами и другими субъектами.

Помимо чисто управленческих сложностей возможность согласовать политические курсы часто ограничена существованием конкурирующих политических интересов. Это особенно справедливо в отношении стран с развитой и диверсифицированной интернет-экономикой. Например, на заре дебатов о сетевом нейтралитете регуляторы разных стран пытались обеспечить баланс между интересами интернет-отрасли, представители которой выступали за нейтралитет, и интересами телекоммуникационных и культурно-развлекательных компаний, которые рассматривали сетевой нейтралитет как препятствие на пути формирования новой бизнес-модели, рассчитанной на повышение пропускной способности Интернета для доставки мультимедийных материалов.

«Телеграфная геостратегия» и политическая (не)согласованность

Англо-французский союз (Антанта)[3] был создан в 1904 г. Однако вместо того, чтобы отдать предпочтение сотрудничеству с Великобританией,

французское Министерство телеграфов не последовало общему политическому курсу страны, установив тесное сотрудничество с Германией. Основной целью этого было уменьшить британское доминирование в глобальной «телеграфной геостратегии» за счет сотрудничества с Германией в прокладке телеграфных кабелей. В 1915 г. французский историк Шарль Лезаж так прокомментировал эту политическую (не)согласованность: «Длительное расхождение между общими принципами французской дипломатии и действиями в области телеграфа, на мой взгляд, является следствием того, что в этой стране у каждого министерства своя внешняя политика: одна у Министерства иностранных дел, другая — у Министерства финансов... У Администрации почт и телеграфов тоже время от времени имеется своя внешняя политика; и получилось так, что в эти последние годы, не будучи враждебной к Англии, она продемонстрировала сильную склонность к Германии»[4].

Рисунок 26. Сферы регулирования в области цифровых технологий

Важность постоянных представительств стран при международных организациях с точки зрения управления Интернетом

Для многих государств постоянные представительства при международных организациях в Женеве были важными, если не сказать ключевыми, игроками в процессе WSIS и с точки зрения управления Интернетом в целом. Вся деятельность, связанная с управлением Интернетом, преимущественно осуществлялась в Женеве, где расположена штаб-квартира МСЭ, игравшего основную роль в процессе. Первый саммит WSIS в 2003 г. состоялся в Женеве, и все, кроме одной, подготовительные встречи прошли там же, благодаря чему постоянные миссии в Женеве все время были вовлечены в процесс. На сегодняшний день секретариат IGF располагается в Женеве; здесь же проходят все подготовительные встречи IGF.

Для крупных развитых стран постоянные представительства были частью широкой сети организаций и деятелей, участвовавших во WSIS и процессе управления Интернетом. Для небольших и развивающихся государств постпредства были основными — а иногда и единственными — участниками процесса. Небольшим перегруженным работой представительствам развивающихся стран пришлось включить в сферу своей деятельности вопросы управления Интернетом. Нередко один и тот же дипломат отвечал за проблематику управления Интернетом наряду с другими обязанностями в таких областях, как права человека, здравоохранение, торговля и охрана труда.

Позиции стран

Соединенные Штаты

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

Одной из отличительных черт участия правительства США была политика невмешательства, обычно называемая «отдаленный опекун». Американские власти задавали лишь общие рамки, оставляя управление Интернетом в ведении тех, кто с ним непосредственно работает, в первую очередь интернет-сообщества. Однако в некоторых случаях правительство США вмешивалось в процесс более явным образом — например, как это случилось в середине 1990-х гг., когда в рамках некоммерческого проекта CORE корневые серверы и управление ключевыми ресурсами Интернета могли быть перенесены из США в Женеву[5]. Этот процесс был остановлен знаменитой, по крайней мере в истории Интернета, дипломатической нотой, направленной государственным секретарем США Мадлен Олбрайт Генеральному секретарю МСЭ[6]. Параллельно с остановкой инициативы CORE правительство США начало консультации, результатом которых стало создание ICANN в 1998 г. Власти США поручили ICANN взять на себя функции IANA, то есть координацию системы уникальных идентификаторов Интернета (в основном, систему доменных имен и IP-адреса). Власти США сохраняли контроль над деятельностью IANA до октября 2016 г., когда эти функции были переданы международному интернет-сообществу.

США особо уязвимы перед лицом кибератак в силу высокой степени развитости интернет-пространства и отрасли в целом. Этим объясняется активность американских дипломатов в международных переговорах по теме кибербезопасности. США выступают за применение к Интернету существующих норм международного права, включая право на самооборону, и не поддерживают заключение глобального договора по вопросам кибербезопасности. При этом США подписали целый ряд региональных и двухсторонних соглашений в этой области. Борьба с международной киберпреступностью осуществляется в соответствии с Конвенцией по киберпреступности Совета Европы и на основании двухсторонних соглашений, включая договоры о взаимной правовой помощи. США также содействуют развитию структур, занимающихся вопросами кибербезопасности. В качестве примера можно привести создание и укрепление групп реагирования на компьютерные инциденты (Computer Emergency Response Team - CERT).

В сфере экономики США выступают за свободу обмена данными и свободу торговли цифровыми услугами. Для продвижения идеи свободной торговли используется ВТО и другие региональные и двухсторонние торговые

соглашения. Основную выгоду от отсутствия ограничений в сфере интернет-торговли извлекает американская интернет-отрасль, и свобода обмена данными является в этой связи ключевым фактором. США являются противником налогообложения интернет-транзакций.

Европейский союз

Европейскому союзу удается уникальным образом сочетать в своей деятельности «жесткую» и «мягкую» силу для выработки сбалансированных решений в области управления Интернетом. В основе жесткой силы ЕС лежит рынок из 500 млн. человек с высоким уровнем проникновения интернет-услуг (79,3% по состоянию на 2015 г.)[7] и высокой покупательной способностью. Судя по скоплению лоббистов интернет-отрасли в Брюсселе, этот аспект имеет большое значение. Вступая в переговоры с ЕС по вопросам антимонопольной деятельности и защиты персональных данных, компании Google и Facebook, по сути, ведут переговоры с остальным миром, поскольку другие страны и регионы нередко берут за образец соглашения между ЕС и интернет-отраслью. Учитывая, что Google контролирует более 90% рынка интернет-поиска в Европейской экономической зоне, ЕС становится главной инстанцией, которая может предотвратить злоупотребления со стороны Google своим доминирующим положением на рынке[8].

Мягкая сила ЕС в области цифровых технологий заключается в превращении своих слабых сторон в сильные с помощью дипломатического айкидо. Слабой стороной считается недостаточная развитость интернет-отрасли в рамках ЕС. Как ни парадоксально, но в контексте управления Интернетом этот недостаток может превратиться в преимущество.

Поскольку Евросоюзу не требуется отстаивать экономические интересы своих интернет-компаний, он может сосредоточить внимание на продвижении и защите общественных ценностей (права пользователей, обеспечение доступности технологий и разнообразия материалов). Таким образом, он становится в ряд защитников интернет-пользователей и сторонников создания условий для развития интернет-отрасли и может преуспеть в достижении поставленных целей, как этических, так и стратегических, что удается довольно редко на международной арене.

Одним из направлений политики ЕС является сотрудничество по конкретным вопросам. На WCIT-12 Евросоюз поддержал позицию США. Что касается принципа неприкосновенности частной жизни и защиты персональных данных, то в этой сфере ЕС разделяет взгляды латиноамериканских стран. Схожие позиции по наиболее актуальным вопросам управления Интернетом занимают Норвегия и Швейцария.

В дальнейшем стратегия ЕС по вопросам управления Интернетом будет формироваться под влиянием единого рынка цифровых технологий ЕС, особенно в том, что касается налогообложения, защиты прав потребителей и обеспечения свободного обмена данными.

Отдельные страны — члены ЕС выделяют в качестве приоритетов различные аспекты управления Интернетом. Так, Германия и Австрия придают особое значение соблюдению права на неприкосновенность частной жизни и защите данных. Этим объясняется ведущая роль этих стран при обсуждении этих вопросов в ЕС и в системе ООН.

Весьма активна в сфере регулирования цифровых технологий Эстония. После DDoS-атаки 2007 г., существенно повлиявшей на работу Интернета в стране, Эстония начала уделять серьезное внимание вопросам кибербезопасности. Именно здесь расположен Центр передового опыта по совместной защите от киберугроз НАТО (Cooperative Cyber Defence Centre of Excellence). С 2010 г. Эстония проводит ежегодную конференцию по киберконфликтам, ставшую крупным отраслевым мероприятием.

Большое внимание борьбе с киберпреступностью уделяется в Румынии, где расположена штаб-квартира Программы Совета Европы по борьбе с киберпреступностью. Цель программы — оказание содействия в укреплении системы правосудия и расширении возможностей по преодолению проблем, связанных с киберпреступностью, на основе стандартов Конвенции о киберпреступности Совета Европы. Голландия проводит Глобальный экспертный форум по кибербезопасности и реализует множество других программ в этой сфере.

Китай

Китай играет огромную роль в вопросах управления Интернетом, поскольку в этой стране больше всего интернет-пользователей (свыше 700 млн.),

и интернет-отрасль стремительно развивается (четыре из десяти крупнейших интернет-компаний созданы в Китае). В вопросах регулирования цифровых технологий Китай балансирует между экономическим подходом, который предусматривает неограниченные коммуникации, и политическим подходом, основанном на идее осуществления киберсуверенитета на национальном уровне.

С точки зрения международных экономических связей, важность Интернета для экспортно-ориентированной экономики Китая сложно переоценить. Китайские компании используют Интернет в качестве информационной инфраструктуры для продвижения своей деятельности на мировом рынке. На данный момент китайская платформа электронной торговли Alibaba является мировым лидером по объему транзакций. Владелец компании Джек Ма призывает создать Международную систему электронной торговли с целью содействия включению малых и средних предприятий в международную интернет-торговлю[9]. Основными темами саммита G20 в Ханчжоу в сентябре 2016 г. стало развитие цифровой экономики и инноваций.

С политической точки зрения, краеугольным камнем внешней политики Китая является защита суверенитета. Это относится также к киберпространству. Выступая на Всемирной конференции Интернета в 2015 г., председатель КНР Си Цзиньпин дал следующее определение понятию киберсуверенитета: «Право отдельных стран самостоятельно выбирать собственный путь развития в сфере кибертехнологий, модель регулирования киберпространства и политику в этой области, а также возможность участвовать в управлении киберпространством на международном уровне на равных основаниях»[10]. В соответствии с таким подходом, к Интернету применимы законы, обычаи и нормы, действующие в «реальном» мире в пределах суверенной территории.

Китаю удается обеспечивать свой киберсуверенитет путем ограничения доступа иностранных интернет-компаний на китайский рынок (Facebook, Google, Twitter) и содействия популяризации аналогичных китайский решений. Так, китайским эквивалентом Google стал Baidu, Twitter заменил ресурс Sina Weibo, вместо Facebook можно пользоваться социальной сетью Renren, а в качестве аналога YouTube появился видеохостинг Youku. Данные китайских интернет-пользователей и учреждений преимущественно хранятся на серверах, расположенных в Китае. Ведение Китаем политики киберсуверентета подвергается критике в связи с фильтрацией интернет-материалов, которые ки-

тайские власти считают неподходящими для широкого распространения.

В вопросах регулирования цифровых технологий на международном уровне Китай поддерживает многосторонний подход и при этом принимает активное участие в деятельности таких организаций, как ICANN и IETF. С 2014 г. Китай проводит ежегодную Всемирную конференцию по Интернету, что говорит о его стремлении играть более значимую роль в регулировании цифровых технологий на международном уровне.

Можно предположить, что будущие внешнеполитические усилия Китая в сфере цифровых технологий будут сосредоточены на продвижении инициативы по созданию цифрового Шелкового пути и усиления цифровой взаимосвязанности между Азией и Европой. Этот проект реализуется в рамках более масштабной инициативы «Один пояс, один путь» по развитию морского и сухопутного сообщения между Китаем и Европой.

Бразилия

Одной из наиболее активных стран в сфере международной цифровой политики и крупнейшим интернет-рынком Латинской Америки является Бразилия. В этой демократической стране с растущей экономикой созданы все условия для развития цифровых технологий. Бразилия могла бы содействовать достижению компромисса между сторонниками управления Интернетом на межгосударственном уровне и противниками этого подхода, выступающими за отстранение государственных органов и передачу полномочий неправительственным организациям. Бразилия четко обозначила свою позицию после разоблачений Эдварда Сноудена и сделала это дипломатическим путем. В своем выступлении на 68-й сессии Генеральной Ассамблеи ООН президент Бразилии Дилма Руссеф подчеркнула, что «ведущая роль в регулировании политики государств в сфере таких технологий принадлежит Организации Объединенных Наций» и охарактеризовала действия по отслеживанию информации как «нарушение международного права» и «пренебрежение национальным суверенитетом Бразилии»[11]. Затем Дилма Руссеф предложила кандидатуру своей страны в качестве соорганизатора встречи NETmundial по разработке модели управления Интернетом с участием не только государств, но и других заинтересованных сторон, обозначив

таким образом более взвешенную позицию. Бразилии выполнила задачу и обеспечила успешное проведение мероприятия, хотя принять обязывающий документ по его итогам не удалось[12].

Бразилия активно участвует во многих процессах, связанных с цифровыми технологиями. Страна выступила принимающей стороной двух из десяти встреч Форума по управлению Интернетом и сыграла важную роль в переговорах в формате WSIS+10. Вместе с Германией Бразилия выступает за разработку международных норм по обеспечению неприкосновенности частной жизни в сети.

Индия

Индия играет важную роль в сфере регулирования цифровых технологий. В стране насчитывается большое число пользователей, достаточно развита интернет-отрасль, но есть проблемы с обеспечением доступа в Интернет. Индия занимает неоднозначную позицию по вопросу управления Интернетом, что обусловлено сложной ситуацией, сложившейся в стране в этой области. В управление Интернетом вовлечены многочисленные организации гражданского общества. Правительство предпочитало межгосударственный подход, тогда как большинство делового сообщества выступало за регулирование без участия официальных органов. Это противостояние привело к довольно неожиданным решениям. Так, чтобы добиться введения межгосударственного контроля над критически важными ресурсами Интернета, Индия предложила создать Комитет ООН по связанным с Интернетом политическим мерам. Однако в ходе WCIT-12 Индия кардинально изменила свою позицию и встала на сторону развивающихся стран, но в отличие от большинства из них не подписала новую версию РМЭ. Нынешнее правительство Индии поддерживает идею привлечения широкого круга заинтересованных лиц к управлению Интернетом, о чем оно заявило в ходе 57-й встречи ICANN, состоявшейся в Индии в ноябре 2016 г.[13]

Россия

Россия активно и последовательно поддерживает многосторонний подход к управлению Интернетом при ведущей роли официальных властей

в решении вопросов, связанных с общественными интересами. В частности, Россия полагает, что МСЭ должен взять на себя функции главного органа в области управления Интернетом. Что касается кибербезопасности, то Россия еще в 1998 г. выступила с предложениями, ставшими основой первой резолюции Генеральной Ассамблеи ООН по вопросам ИКТ и безопасности[14]. С тех пор резолюция принимается ежегодно, а проблемы кибербезопасности рассматриваются в рамках первого комитета Генеральной Ассамблеи. В последнее время такая работа также проводится в Группе правительственных экспертов ООН[15]. Во взаимодействии с Китаем, Казахстаном, Кыргызстаном, Таджикистаном и Узбекистаном Россия продвигает тему сотрудничества по вопросам кибербезопасности на других площадках. Так, в рамках ШОС в 2009 г. было подписано соглашение о международной информационной безопасности.

В сентябре 2015 г. вступил в силу закон о локализации персональных данных, согласно которому интернет-компании обязаны хранить данные российских пользователей в России. Согласно закону, крупные интернет-компании (Facebook, Twitter, Google, LinkedIn) поставлены перед выбором: перенести свои серверы в Россию или рисковать блокировкой своих услуг в России.

Кения

Кения входит в число стран, уделяющих серьезное внимание вопросам управления Интернетом. Множество заинтересованных сторон, включая действующий в стране Форум по управлению Интернетом, вовлечено в этот процесс; в государственных программах, связанных с управлением Интернетом, участвуют организации гражданского общества, деловые круги и представители научного сообщества.

Одним из основных достижений Кении в этой области стало создание платежной системы MPesa, которая обеспечила доступ миллионов кенийских граждан к финансовым услугам и способствовала развитию интернет-отрасли. В настоящее время эта система используется в ряде других стран.

Кения активно участвует в работе ассоциаций, специализирующихся на вопросах регулирования цифровых технологий на региональном и международном уровнях. В 2011 г. в Кении состоялась ежегодная встреча IGF. Кенийские официальные лица, представители деловых кругов и гражданского

Таблица 3. Членство в пяти Группах правительственных экспертов ООН с 2004 г.

Страна \ Год	2004-2005	2009-2010	2012-2013	2014-2015	2016-2017
Австралия			■		■
Аргентина			■		
Беларусь	■	■	■	■	
Ботсвана					■
Бразилия	■	■		■	■
Гана				■	
Германия	■	■	■	■	■
Египет			■	■	■
Израиль		■		■	
Индия	■	■	■		■
Индонезия			■		■
Иордания	■				
Испания				■	
Италия		■			
Казахстан					■
Канада			■		■
Катар		■			
Кения				■	■
Китай	■	■	■	■	■
Колумбия				■	
Республика Корея	■	■		■	■
Куба					■
Малайзия	■			■	
Мали	■				
Мексика	■			■	■
Нидерланды					■
Пакистан				■	
Российская Федерация	■	■	■	■	■
Сенегал					■
Сербия					■
Соединенное Королевство	■	■	■	■	■
Соединенные Штаты Америки	■	■	■	■	■
Финляндия					■
Франция	■	■	■	■	■
Швейцария					■
Эстония		■	■	■	■
Южная Африка	■	■			
Япония			■	■	■

общества сотрудничают с такими организациями, как МСЭ, ICANN, IGF и Группа правительственных экспертов ООН.

Индонезия

В Индонезии Интернет развивается стремительными темпами: в 2016 г. в стране насчитывалось 53 млн. пользователей. Интернет является объектом критически важной инфраструктуры в стране-архипелаге, обеспечивая связь между более чем 6 тыс. островов.

В состав индонезийского национального Форума по управлению Интернетом входят представители органов власти, частных компаний, научных кругов и гражданского общества. Основной проблемой в сфере безопасности является использование Интернета террористическими группами. Что касается экономики, то Индонезия рассматривает вопрос о введении специального налога на Google и другие интернет-компании. В целях обеспечения неприкосновенности частной жизни и защиты персональных данных в законодательство Индонезии включено положение о праве на забвение. По сравнению с европейской трактовкой права на забвение (удаление определенных материалов из результатов поиска), индонезийская норма является более жесткой и предусматривает возможность требовать удаления определенных материалов с сайтов.

Индонезия активно участвует в международных программах сотрудничества в сфере цифровых технологий. Она выступила принимающей стороной встречи IGF 2013 г., является членом таких организаций, как МСЭ, ICANN, IGF и Группа правительственных экспертов ООН.

Швейцария

Швейцария входит в число первопроходцев в создании глобальной экосистемы управления Интернетом: первая встреча WSIS состоялась в 2003 г. в Женеве. Швейцарский дипломат Маркус Куммер председательствовал в Рабочей группе по управлению Интернетом (WGIG), а в 2010 г. возглавил секретариат IGF. С 2014 г. в Правительственном консультативном совете ICANN председательствует Томас Шнайдер из Федерального управления связи Швейцарии.

Швейцария активно содействовала разработке мер укрепления доверия в сфере кибербезопасности, и в 2016–2017 гг. входила в Группу правительственных экспертов ООН.

В рамках ООН и других международных форумов Швейцария наряду с другими странами твердо отстаивает принцип неприкосновенности частной жизни в сети.

Малые государства

Сложность вопросов и динамика деятельности в процессе управления Интернетом не позволяли небольшим государствам, в особенности развивающимся, следить за происходящим, а тем более оказывать на процесс сколько-нибудь значительное влияние. В результате, многие малые государства выступили за управление Интернетом по принципу «одного окна»[16]. Емкость повестки дня и ограниченные возможности развивающихся стран (как в самой стране, так и в ее дипломатических представительствах) остаются важными препятствиями для их полноценного участия в процессе управления Интернетом. Необходимость развивать потенциал в данной сфере была признана в качестве приоритета в Тунисской программе для информационного общества WSIS.

> Управление Интернетом — подход с «переменной геометрией»
>
> Управление Интернетом требует участия различных заинтересованных сторон, отличающихся по многим параметрам, включая международную правоспособность, заинтересованность в конкретных вопросах управления Интернетом и наличие экспертных знаний. Такое разнообразие можно интегрировать в единую модель управления Интернетом за счет использования подхода «с переменной геометрией». Этот подход нашел отражение в статье 49 Декларации принципов WSIS17, определяющей следующие роли для основных заинтересованных сторон:
>
> • государства — «политические полномочия по связанным с Интернетом вопросам государственной политики» (включая международные аспекты);
>
> • частный сектор — «развитие Интернета как в технической, так и в экономической сфере»;

• гражданское общество — «важная роль в относящихся к Интернету вопросах, в особенности на низовом уровне»;
• межправительственные организации — «координация связанных с Интернетом вопросов государственной политики»;
• международные организации — «разработка относящихся к Интернету технических стандартов и соответствующей политики».

Этот подход уже нашел практическое применение. Так, государства играют ведущую роль в вопросах кибербезопасности и электронной коммерции, тогда как основные функции по стандартизации и управлению системой доменных имен и номеров выполняют технические эксперты и деловое сообщество.

Деловое сообщество[18]

На ранних стадиях развития Интернета центральной проблемой с точки зрения делового сообщества была защита торговых марок. Многие компании сталкивались с проблемами киберсквоттинга и неправомерного использования своих торговых марок людьми, которые успели первыми зарегистрировать соответствующие доменные имена. При создании ICANN в 1998 г. бизнес-круги явно обозначили защиту торговых марок в качестве приоритета. Развитие Интернета и электронной коммерции способствовали повышению интереса делового сообщества и к другим вопросам, включая обеспечение права на неприкосновенность частной жизни и защиту данных, а также соблюдение других прав человека в Интернете, кибербезопасность, интернет-банкинг, налогообложение, регулирование материалов Интернета и многоязычие. В настоящее время в сфере управления Интернетом сложно найти вопрос, который не был бы актуален для делового сообщества. Однако приоритеты могут меняться в зависимости от отрасли.

Международная торговая палата

Международная торговая палата (МТП) позиционировала себя в качестве одного из ключевых представителей бизнеса в глобальных процессах управления Интернетом. МТП активно участвовала в переговорах WGIG и WSIS на ранних этапах и продолжает вносить весомый вклад в процесс IGF.

В силу постоянного развития Интернета, возрос и интерес бизнеса к управлению глобальной сетью. С этой точки зрения компании можно разделить на следующие основные группы: компании, занимающиеся доменными именами; интернет-провайдеры; телекоммуникационные компании; поставщики материалов для Интернета.

Компании, занимающиеся доменными именами

К компаниям, занимающимся доменными именами, относятся регистратуры, которые управляют доменами верхнего уровня (например, .com и .net), и регистраторы, которые оказывают услуги по регистрации доменов конечным пользователям. Среди основных игроков в этом секторе — компании VeriSign и Affilias. На деятельность регистратур и регистраторов непосредственно влияют решения, принимаемые ICANN в таких областях, как создание новых доменов верхнего уровня и разрешение споров. Поэтому эти компании играют столь важную роль в процессе выработки ICANN своих решений. Некоторые регистратуры и регистраторы поодиночке или в рамках ассоциаций также участвовали в более широком процессе управления Интернетом (WSIS, WGIG, IGF).

Интернет-провайдеры

Поскольку провайдеры являются ключевыми посредниками при работе в сети, они особенно важны с точки зрения управления Интернетом. Их основное участие в этом процессе происходит на национальном уровне в форме взаимодействия с правительственными органами и ведомствами. На глобальном уровне некоторые провайдеры, особенно из США и Европы, активно участвовали в процессах WSIS, WGIG, IGF и ICANN как на индивидуальной основе, так и по каналам национальных, региональных и отраслевых бизнес-ассоциаций, включая Information Technology Association of America (ITAA), European Internet Service Providers Association (EuroISPA) и другие.

Телекоммуникационные компании

Телекоммуникационные компании обеспечивают передачу интернет-трафика и обслуживают инфраструктуру Интернета. Среди основных игроков в этом сегменте — такие компании, как Verizon, AT&T, Vodafone, Deutsche Telekom и Telefonica. Телекоммуникационные компании традиционно участвовали в выработке международной политики в области электросвязи через МСЭ. Они все более активно вовлекаются в деятельность ICANN и IGF. Их основной интерес с точки зрения управления Интернетом — гарантировать благоприятную среду для бизнеса, позволяющую развивать телекоммуникационную инфраструктуру Интернета.

Наряду с этим телекоммуникационные компании считают важным вопрос о перераспределении доходов, получаемых посредством Интернета. Они утверждают, что, поскольку доступ в Интернет предоставляют они, им причитается более высокая доля доходов, генерируемых Интернетом, основными получателями которых оказываются поставщики материалов, зарабатывающие на рекламе.

Подробнее о перераспределении доходов между интернет-компаниями и телекоммуникационными операторами см. ***Раздел 5.***

Телекоммуникационные компании предпринимают попытки увеличить доходы за счет предоставления новых услуг и повышения платы для поставщиков материалов за скорость соединения. Большинство таких предложений строятся на неравном обращении с различными видами интернет-трафика, что нарушает принцип цифрового нейтралитета и превращает телекоммуникационные компании в рьяных противников этого принципа.

Подробнее о сетевом нейтралитете см. ***Раздел 2.***

Попытки решить вопрос о перераспределении доходов от Интернета все больше размывают грань между телекоммуникационными операторами и интернет-компаниями. Телекоммуникационные компании теперь поставляют материалы и услуги связи, а интернет-компании начинают инвестировать в телекоммуникационную инфраструктуру. Например, Google и Facebook финансируют прокладку трансатлантического и транстихоокеанского оптоволоконных кабелей.

Интернет-отрасль

Интернет-отрасль нередко называют сегментом OTT. К нему относятся все компании, у которых в основе бизнес-модели лежит Интернет. Они делятся на три основных сегмента: поставщики материалов, коммуникационные компании и поставщики услуг. Большинство крупных компаний обычно работают сразу в нескольких сегментах. Например, Google и Facebook одновременно поставляют и материалы, и услуги.

Поставщики материалов

Ключевую роль в интернет-отрасли играет информационное наполнение. Поисковая система Google обеспечивает доступ к широкому кругу материалов, YouTube обеспечивает доступ к видеоконтенту, а Facebook упорядочивает материалы, созданные пользователями. Некоторые компании, например, Disney, раньше работали вне интернет-пространства, но смогли стать поставщиками материалов для Интернета. Приоритетные направления развития таких компаний тесно связаны с вопросами управления Интернетом, включая права интеллектуальной собственности, право на неприкосновенность частной жизни, кибербезопасность и сетевой нейтралитет. Они играют все более заметную роль в управлении Интернетом на международном уровне, в том числе в рамках ВТО, ВОИС и IGF.

Поставщики услуг связи

К крупнейшим поставщикам услуг связи относятся Skype, WhatsApp, WeChat, Snapchat и Google Talk. Сообщения с использованием этих платформ все чаще снабжаются криптографической защитой, тогда как официальные власти пытаются противиться этой тенденции. Таким образом, основная задача для этого сегмента состоит в том, чтобы обеспечить шифрование сообщений и защитить право своих пользователей на неприкосновенность частной жизни.

Поставщики услуг

Этот сегмент также называют отраслью платформ. Сюда относятся новые виды услуг, включая Uber и Airbnb. Такие компании используют Интернет для предоставления новых видов услуг, включая использование частного автопарка как средства передвижения (Uber). Применительно к их модели ведения бизнеса актуальны многие вопросы управления Интернетом, включая налогообложение, защиту прав потребителей и трудовое законодательство.

Гражданское общество

Гражданское общество всегда было самым активным сторонником вовлечения различных участников в управление Интернетом. Гражданское общество можно охарактеризовать как пестрый конгломерат участников процессов, связанных с управлением Интернетом. Организации гражданского общества занимаются различными аспектами управления Интернетом. Многие из них выступают за усиление защиты прав человека в Интернете, включая право на свободное выражение мнения и неприкосновенность частной жизни. Одним из ключевых факторов, разделяющих организации гражданского общества, является отношение к участию государства в управлении Интернетом. Среди представителей гражданского общества официальные власти традиционно считались равнозначным участником процесса управления Интернетом наравне с гражданским обществом, компаниями и профессиональным техническим сообществом. Однако в последнее время все более популярной становится идея о том, что главную роль в защите общественных интересов в силу своей легитимности должно играть правительство. В частности, в пользу такой позиции говорит то, что только государство способно противостоять влиянию делового сообщества в сфере цифровых технологий.

Формированию скоординированной позиции по различным аспектам управления Интернетом мешает разнообразие взглядов среди гражданского общества. Однако в процессе WSIS представители гражданского общества сумели справиться с присущей этому сектору сложностью и разнообразием,

опираясь на несколько организационных форм, в том числе Бюро гражданского общества (Civil Society Bureau), Пленум гражданского общества (Civil Society Plenary) и тематические группы. Во WGIG гражданское общество было представлено более широко благодаря многосторонней природе Рабочей группы. Организации гражданского общества предложили восьмерых кандидатов для участия в WGIG, все из которых были впоследствии одобрены Генеральным секретарем ООН. Участвуя в деятельности Рабочей группы, они сумели повлиять на многие принятые решения, в том числе, на решение создать Форум по управлению интернетом (IGF) как пространство для обсуждения вопросов управления Интернетом с участием различных заинтересованных сторон.

Гражданское общество продолжает принимать активное участие в деятельности IGF. Своеобразной формой привлечения гражданского общества к управлению Интернетом стало Совещание по управлению Интернетом (Internet Governance Caucus — IGC), которое организовано в форме переписки. Его проводят люди, заинтересованные в обмене мнениями, обсуждении вопросов управления Интернетом и обмене опытом по этой проблематике.

Организации гражданского обществе принимают деятельное участие в обсуждении всех аспектов управления Интернетом, от инфраструктурного развития до экономических моделей, прав и свобод с акцентом на защиту общественных интересов. Многие организации нанимают экспертов и ученых, хорошо разбирающихся в Интернете, и вносят существенный вклад в принятие решений.

Одной из основных проблем гражданского общества является обеспечение устойчивой деятельности своих организаций. На ранних стадиях процесса WSIS участие гражданского общества сводилось к работе нескольких преданных своему делу энтузиастов. Это придавало процессу определенную динамику без привлечения гражданского общества на постоянной основе. Для обеспечения постоянного участия гражданского общества нужны стабильные структуры. Одной из первых организаций, включившихся в управление Интернетом, стала APC. Затем к процессу присоединились Best Bytes и Just Net Coalition[19].

В мире сейчас несколько миллиардов интернет-пользователей. Действующие в этой сфере организации гражданского общества отражают разноо-

бразие и отличительные черты современного общества. Основная проблема гражданского общества заключается в том, чтобы представлять все разнообразие взглядов и позиций по вопросу о регулировании и развитии цифровых технологий.

Международные организации

МСЭ был основной международной организацией в процессе WSIS. Он организовывал работу Секретариата WSIS и участвовал в выработке политики по важнейшим вопросам. Участие МСЭ в процессе WSIS связано с активными попытками организации определить и укрепить свою позицию на быстро меняющейся арене глобальных телекоммуникаций, которая во все большей степени зависит от Интернета. Влиянию МСЭ в области глобальных телекоммуникаций угрожают, например, такие тенденции, как либерализация глобального рынка телекоммуникаций, проводимая в рамках ВТО, и перевод телефонного трафика с традиционных телекоммуникационных каналов в Интернет (с помощью технологии Voice over IP).

Возможность того, что по итогам WSIS МСЭ может де-факто стать «Международной организацией Интернета», вызвала озабоченность в США и ряде развитых стран, хотя получила поддержку некоторых развивающихся государств. На протяжении всего процесса WSIS эта перспектива создавала скрытое напряжение. В особенности это было заметно в области управления Интернетом, где напряженность в отношениях между ICANN и МСЭ существовала с момента создания ICANN в 1998 г. WSIS не ослабила эту напряженность, однако, в дальнейшем она спала. С учетом усиливающейся интеграции различных коммуникационных технологий, вполне вероятно, что вопрос о повышении роли МСЭ в области управления Интернетом будет вновь появляться в политических дискуссиях. Так, МСЭ уже активизировал свою деятельность в сфере кибербезопасности и защиты детей в Интернете.

Еще один вопрос касался увязки междисциплинарной повестки WSIS с работой специализированных агентств ООН. Нетехнические аспекты коммуникаций и интернет-технологий (социальные, экономические, культурные

вопросы) входят в мандат других организаций ООН. Наиболее заметным игроком в этом контексте является ЮНЕСКО, которая занимается такими вопросами, как многоязычие, культурное разнообразие, общество знаний и обмен информацией. В обсуждении вопросов управления Интернетом также активно участвует ВОИС применительно к вопросам защит прав на интеллектуальную собственность в цифровом пространстве.

В процессе WSIS значительные усилия были направлены на поддержание равновесия между МСЭ и другими организациями системы ООН. Оно сохраняется и в процессах, инициированных WSIS, основными участниками которых являются МСЭ, ЮНЕСКО и Программа развития ООН (ПРООН) и ЮНКТАД. Эти агентства ООН выступают в качестве основных организаторов ежегодного Форума WSIS, на котором в последние годы все больше обсуждаются вопросы, связанные с управлением Интернетом.

Профессиональное техническое сообщество

Профессиональное техническое сообщество состоит из институтов и индивидов, развивавших и продвигавших Интернет и/или управление техническими ресурсами Интернета. В рамках этого сообщества также сложился традиционный «дух Интернета», основанный на принципах обмена ресурсами, открытого доступа и противодействия участию правительства в регулировании глобальной сети. Члены сообщества всегда защищали исконную концепцию Интернета от излишней коммерциализации и чрезмерного влияния правительства.

> Терминология: профессиональное техническое сообщество
>
> Наряду с термином «профессиональное техническое сообщество» для обозначения того же понятия используются такие словосочетания как «интернет-сообщество», «разработчики Интернета», «основатели Интернета», «отцы Интернета» и «технологи». Термин профессиональное техническое сообщество используется в декларациях WSIS и других документах.

> Профессиональное техническое сообщество соответствует всем критериям «эпистемического сообщества», о котором писал Питер Хаас[20]: «Профессиональная группа, члены которой придерживаются общих ценностей и взглядов на причинно-следственные связи и критерии истинности; члены сообщества также имеют общее понимание проблемы и путей ее решения».

На ранних этапах интернет-сообщество регулировалось несколькими, в основном неформализованными правилами и одной формальной процедурой — запросом комментариев (Request for Comments, RFC). Все основные стандарты Интернета описаны с помощью RFC. Несмотря на отсутствие строгих правил и формальной структуры, на ранних этапах интернет-сообщества регулировались силой традиций и влияния участников друг на друга. Большинство участников процесса разделяло общие ценности, приоритеты и отношение к ключевым проблемам.

Техническое регулирование глобальной сети силами профессионального технического сообщества было поставлено под вопрос в середине 1990-х гг., когда Интернет стал частью глобальной общественной и экономической жизни. Рост Интернета привел к появлению новых заинтересованных сторон (например бизнеса), которые привнесли иную профессиональную культуру и понимание того, что есть Интернет и как им управлять. Это привело к нарастанию напряженности. Так, в 1990-х годах интернет-сообщество и компания Network Solutions[21] были вовлечены в так называемую войну DNS, конфликт по поводу контроля над корневыми серверами и системой доменных имен.

Одним из основных представителей профессионального технического сообщества является организация Internet Society, которая проводит IETF, выступает за открытый Интернет и активно наращивает потенциал.

Профессиональное техническое сообщество сыграло важную роль в создании ICANN и обеспечении ее функционирования. Один из создателей Интернета, Винт Серф, был председателем совета директоров этой организации с 2000 по 2007 г. Члены профессионального технического сообщества занимают важные должности в различных структурах ICANN.

Однако сейчас, когда число интернет-пользователей превысило три

миллиарда, Интернет «перерос» созданную ICANN модель Интернета, ориентированную на профессиональное техническое сообщество. Как указывают критики, по мере того как стирается грань между гражданами и пользователями Интернета, в управлении глобальной сетью требуется все большее участие правительств и других структур, представляющих граждан, а не только объединений интернет-пользователей (то есть профессиональное техническое сообщество). К этому аргументу особенно часто прибегают те, кто выступает за расширение роли государства в управлении Интернетом.

Профессиональное техническое сообщество обычно обосновывает свою особую позицию в управлении Интернетом наличием специальных технических знаний. Его представители подчеркивают, что ICANN — в первую очередь техническая организация, поэтому ей должны управлять специалисты, опирающиеся на технические знания. Поскольку ограничить деятельность ICANN исключительно техническими вопросами становится все сложнее, это обоснование подвергается частой критике. Весьма вероятно, что к профессиональному техническому сообществу постепенно подключатся другие ключевые группы участников, в первую очередь гражданское общество, бизнес, научное сообщество, а также власти.

Интернет-корпорация по присвоению имен и адресов (ICANN)

Корпорация по присвоению имен и номеров (ICANN) была создана в 1998 г. в США со статусом некоммерческой организации. Американские власти поручили корпорации взять на себя функции IANA, то есть заниматься общим управлением ключевой инфраструктурой Интернета, состоящей из IP-адресов, доменных имен и корневых серверов.

Интерес к роли ICANN возрос вместе со стремительным ростом Интернета в начале 2000-х гг., и в рамках WSIS 2003-2005 гг. ICANN оказалась в поле внимания глобальных политических кругов.

В соответствии с утвержденным в 2016 г. новым уставом ICANN, корпорация призвана обеспечить стабильную и безопасную работу систем уникальных идентификаторов Интернета. В этих целях организация координи-

рует назначение и передачу имен в корневой системе серверов имен DNS, разработку глобальной политики в отношении родовых доменов верхнего уровня, координирует работу и развитие корневой системы серверов имен DNS, а также назначение и передачу адресов интернет-протокола («IP-адресов») и номеров автономной системы.

Хотя ICANN является центральным участником процесса управления Интернетом, она не регулирует все аспекты Интернета, поэтому некорректно называть ее «правительством Интернета», как это иногда делают. ICANN управляет техническими ресурсами Интернета, но не имеет полномочий в отношении других аспектов управления Интернетом, таких как кибербезопасность, контроль над материалами Интернета, защита авторских прав, защита конфиденциальности, поддержание культурного разнообразия или преодоление цифрового разрыва.

ICANN является многосторонней организацией, включающей широкий спектр участников с разными полномочиями и ролями. Они делятся на три основные группы:

- Профессиональное техническое сообщество и деловые круги, роль которых в системе ICANN заключается в разработке рекомендаций для Правления ICANN по вопросам, связанным с миссией корпорации (например, в отношении родовых доменов верхнего уровня, безопасности и стабильности работы системы DNS).
- Официальные представители стран, которые со времен WSIS выражают желание играть более активную роль в деятельности ICANN. При разработке мер и политики ICANN государствам отводится роль консультантов Правления ICANN, в частности, по вопросам регулирования.
- Интернет-пользователи (сообщество в широком смысле), которые также выполняют функции консультантов.

Вовлечение интернет-пользователей

ICANN экспериментировала с различными подходами, стараясь включить в процесс управления пользователей Интернета. На ранних этапах ее существования предпринимались попытки выбирать представителей пользователей в руководящие органы путем прямых выборов, что также было призвано укрепить легитимность ICANN. Из-за низкой активности избирателей и злоупотреблений прямые выборы не смогли обеспечить реальное представительство пользователей. В последнее время ICANN пытается вовлечь в свою деятельность пользователей Интернета через «представляющие всех» (at-large) структуры управления (At-Large Advisory Committee — ALAC), проведение открытых слушаний и краудсорсинг[22]. Эти эксперименты с организацией ICANN имеют огромное значение для обеспечения легитимности корпорации.

На процесс принятия решений в ICANN повлияли ранние модели управления Интернетом, основанные на принципах демократии, прозрачности, открытости и всеобщего участия. Основным различием между интернет-сообществом 1980-х гг. и сегодняшним контекстом принятия решения в ICANN является уровень «социального капитала». В прошлом интернет-сообщество обладало более высоким уровнем взаимного доверия и солидарности, что значительно упрощало процесс принятия решений и разрешения споров. С развитием Интернета количество новых интернет-пользователей и заинтересованных сторон достигло миллиардов и вышло далеко за пределы первоначального технического сообщества. Таким образом, стремительный рост Интернета сократил социальный капитал, существовавший в первые годы появления Интернета. Поэтому требование профессионального технического сообщества сохранить процедуры принятия решений, существовавшие на ранних этапах развития Интернета, по большей части утопично. Без опоры на социальный капитал единственным способом обеспечить функционирование процесса принятия решений является его формализация и разработка различных механизмов сдержек и противовесов.

Некоторые изменения процедур принятия решений, отражающие новые реалии, уже были сделаны. Наиболее важным из них является реформа ICANN в 2002 г., частью которой было усиление правительственного консультационного комитета и отказ от системы прямого голосования для интернет-пользователей. Осуществляются и другие меры с целью повышения подотчетности ICANN глобальному интернет-сообществу.

Вопросы

Технический или политический вопрос?

Противоречие между решением технических и политических вопросов всегда создавало напряженность в деятельности ICANN. ICANN позиционировала себя как «техническую координационную структуру», которая занимается только техническими вопросами и не затрагивает политические аспекты Интернета. Официальные лица ICANN считали эту специфически техническую природу основным концептуальным аргументом в защиту уникального статуса и организационной структуры организации. Первый председатель ICANN Эстер Дайсон подчеркивала, что «ICANN не стремится решать какие-либо вопросы управления Интернетом; по сути, она управляет инфраструктурой, а не людьми. Ее мандат жестко ограничен администрированием определенных (преимущественно технических) аспектов интернет-инфраструктуры в целом и DNS в частности»[23].

Критики этого утверждения обычно указывают на то, что технически нейтральных решений не существует. В конечном итоге, каждое техническое решение продвигает определенные интересы, усиливает определенные группы и влияет на общественную, политическую и экономическую жизнь. Создание домена верхнего уровня .xxx и появление новых общих доменных имен в 2014 г. являются одними из тех случаев, когда ICANN приходилось решать политические вопросы, связанные с ее технической деятельностью.

Передача функций IANA и подотчетность ICANN

До октября 2016 г. ICANN выполняла функции IANA на основании договора с правительством США (Национальным управлением по телекоммуникациям и информации Министерства торговли США). В соответствии с этим договором, США имели решающий голос по всем вопросам, связанным с внесением изменений в систему DNS (например, при принятии ICANN решения одобрить новые родовые доменные имена верхнего уровня требуется формальное согласие правительства США).

В марте 2014 г. правительство США объявило о своем намерении передать координирующую роль в осуществлении функций IANA глобальному сообществу, в котором представлены различные заинтересованные стороны[24]. ICANN было поручено подготовить предложение по переходному периоду. Параллельно разрабатывалась серия рекомендаций по совершенствованию системы отчетности ICANN. С 2014 по 2016 г. сообщество ICANN активно работало над этими вопросами. В марте 2016 г. предложения были утверждены Правлением ICANN, а в июне 2016 г. их одобрило правительство США.

В соответствии с предложением ICANN о передаче координирующей роли IANA, корпорация создала дочернее предприятие PTI, на которое были возложены функции по присваиванию имен, которое действует на основании договора с ICANN. Таким образом, связанные с доменными именами функции IANA все еще исполняются в рамках ICANN, хотя теперь ее техническая и политическая деятельность более четко разграничены. В новой версии устава ICANN, вступившего в силу 1 октября 2016 г., также оговорены условия, на которых исполняющие функции IANA операторы могут стать независимыми от ICANN. Если раньше все существенные решения в отношении корневой зоны Интернета подлежали согласованию с властями США, то теперь они утверждаются Советом директоров ICANN.

На PTI также возложены функции IANA, связанные с IP-адресами и параметрами протоколов. Между ICANN и организациями по присваиванию адресов (в основном, региональными интернет-регистратурами, отвечающими за присваивание IP-адресов и управление ими на региональном уровне) с одной стороны и организациями по разработке параметров протоколов (IETF и IAB) с другой были заключены соглашения об осуществлении таких функций, после чего были подписаны договоры подряда между ICANN и PTI.

С отказом властей США от своей координирующей роли, в организации были созданы новые механизмы для обеспечения подотчетности ICANN широким слоям интернет-сообщества. Наиболее значимым событием в этой области стало создание так называемого «компетентного сообщества» (empowered community). Эта организация представляет собой объединение без образования юридического лица, уполномоченное осуществлять ряд полномочий, включая завершение полномочий членов Правления ICANN, отклонение бюджета или внесение изменений в Устав организации. Данное ведомство действует в соответствии с указаниями правомочных участников,

то есть Консультационных комитетов ICANN и связанных с ней организаций, которые представляют интернет-пользователей, а также интересы правительства, частного сектора и финансовых организаций[25].

Примечания к разделу 9

[1] Бразилия обычно приводится в качестве примера создания системы управления доменным пространством на основании многостороннего подхода с участием различных заинтересованных сторон. В деятельности национального координатора доменного пространства CGI могут принимать участие все пользователи, включая представителей государственных органов, деловых кругов и гражданского общества. Указанная модель успешно применяется и в других областях управления Интернетом, включая подготовку Форумов по управлению Интернетом в 2007 г. в Рио-де-Жанейро и в 2014 г в Жуан-Песоа. Бразилия продолжает активно заниматься вопросами управления Интернетом, в том числе в рамках встречи NetMundial (http://netmundial.br), организованной в октябре 2013 г. по инициативе президента Дилмы Руссеф и главы ICANN Фади Шехади, и созданной по итогам NetMundial программе NetMundial Initiative (https://www.netmundial.org/).

[2] Обновленный перечень инициатив IGF см.: Internet Governance Forum (no date) National IGF initiatives. Адрес в Интернете: http://www.intgovforum.org/multilingual/content/national-igf-initiatives [просмотрено 7 августа 2018 г.]. На сайте IGF также приведен список утвержденных региональных инициатив: Internet Governance Forum (no date) Regional IGF initiatives. Адрес в Интернете: http://www.intgovforum.org/multilingual/content/regional-igf-initiatives [просмотрено 7 августа 2018 г.].

[3] Géraud A (1954) The rise and fall of the Anglo-French Entente. Foreign Affairs. Адрес в Интернете: http://www.foreignaffairs.com/articles/71095/andre-geraud-pertinax/rise-and-fall-of-the-anglo-french-entente [просмотрено 7 августа 2018 г.].

[4] Lesage C (1915) La rivalite franco-britannique. Les cables sous-marins allemands Paris. p. 257—258; quoted in: Headrick D (1991) The Invisible Weapon: Telecommunications and International Politics 1851—1945. Oxford: Oxford University Press. p. 110.

[5] Mueller M. ICANN and internet governance: Sorting through the debris of 'self-regulation'. info // The Journal of Policy, Regulation and Strategy for Telecommunications Information and Media. 1999, 1(6), p 497—520. Адрес в Интернете: http://www.icannwatch.org/archive/mueller_icann_and_internet_governance.pdf [просмотрено 7 августа 2018 г.].

[6] МСЭ была подвергнута критике со стороны госсекретаря США за «проведение глобальной встречи без согласия стран-членов, несанкционированное расходование ресурсов и заключение международных соглашений». Цит. по Drake W (2004) Reframing Internet Governance Discourse: Fifteen Baseline Propositions, p. 9. Адрес в Интернете: http://www.unngls.org/orf/drake.pdf [просмотрено 7 августа 2018 г.].

[7] Internet World Stats (2015) Internet Usage in the European Union. Адрес в Интернете: http://www.internetworldstats.com/stats9.htm [просмотрено 7 августа 2018 г.].

[8] European Commission (2013) Antitrust: Commission seeks feedback on commitments offered by Google to address competition concerns. European Commission — IP/13/371. Адрес в Интернете: http://europa.eu/rapid/press-release_IP-13-371_en.htm [просмотрено 7 августа 2018 г.].

[9] Alibaba Group (no date) Electronic World Trade Platform. Адрес в Интернете: http://www.alizila.com/wp-content/uploads/2016/09/eWTP.pdf [просмотрено 7 августа 2018 г.].

[10] Ministry of Foreign Affairs of the People's Republic of China (2015) Remarks by H.E. Xi Jinping, President of the People's Republic of China At the Opening Ceremony of the Second World Internet Conference. Адрес в Интернете: http://www.fmprc.gov.cn/mfa_eng/wjdt_665385/zyjh_665391/t1327570.shtml [просмотрено 7 августа 2018 г.].

[11] Rousseff D (2013) Statement by H.E. Dilma Rousseff, president of the Federative Republic of Brazil, at the opening of the general debate of the 68th Session of the United Nations General Assembly. Адрес в Интернете: https://gadebate.un.org/sites/default/files/gastatements/68/BR_en.pdf [просмотрено 7 августа 2018 г.].

[12] NETmundial (2014) NETmundial Multistakeholder Statement. Адрес в Интернете: http://netmundial.br/wp-content/uploads/2014/04/NETmundial-Multistakeholder-Document.pdf [просмотрено 7 августа 2018 г.].

[13] Goldstein D. Indian Minister of Electronics and Information Technology Reaffirms Support of the Multistakeholder Model at ICANN's 57th Public Meeting // Domain Pulse, 06.11.2016. Адрес в Интернете: http://www.domainpulse.com/2016/11/06/india-reaffirms-support-multistakeholder-model-icann57/ [просмотрено 7 августа 2018 г.].

[14] United Nations General Assembly (1999) Resolution A/53/70. Developments in the Field of Information and Telecommunications in the Context of International Security. Адрес в Интернете: http://www.un.org/ga/search/view_doc.asp?symbol=A/RES/53/70 [просмотрено 7 августа 2018 г.].

[15] Radu R (2013) Negotiating meanings for security in the cyberspace. Info 15(6), pp. 32—41. Адрес в Интернете: https://www.researchgate.net/publication/255697155_Negotiating_meanings_for_security_in_the_cyberspace [просмотрено 7 августа 2018 г.].

[16] Удобство «одного окна» было одним из аргументов в пользу утверждения МСЭ в качестве центрального игрока управления Интернетом.

[17] WSIS (2003) Declaration of principles. Адрес в Интернете: http://www.itu.int/wsis/docs/geneva/official/dop.html [просмотрено 7 августа 2018 г.].

[18] Ценные комментарии по этому вопросу дала Аиша Хасан (Ayesha Hassan).

[19] Такой взгляд нашел воплощение в различных заявлениях и декларациях коалиции и Just Net Coalition. Подробнее см.: Just Net Coalition (no date) Statements. Адрес в Интернете: http://justnetcoalition.org/statements [просмотрено 7 августа 2018 г.].

[20] Haas P (1990) Saving the Mediterranean: The Politics of International Environmental Cooperation. New York: Columbia University Press, p.55.

[21] Технологическая компания Network Solutions (www.networksolutions.com) основана в 1979 г. Главным направлением деятельности компании была регистрация доменных имен. Компания диверсифицировала свою деятельность, освоив оказание электронных услуг малым предприятиям.

[22] Radu R et al. (2015) Crowdsourcing ideas as an emerging form of multistakeholder participation in Internet governance. Policy & Internet 7(3), pp. 362—382.

[23] Dyson E (1999) Esther Dyson's response to Ralph Nader's Questions. Адрес в Интернете: http://www.icann.org/en/correspondence/dyson-response-to-nader-15jun99.htm [просмотрено 7 августа 2018 г.].

[24] NTIA (2014) NTIA Announces Intent to Transition Key Internet Domain Name Functions. Адрес в Интернете: https://www.ntia.doc.gov/press-release/2014/ntia-announces-intent-transition-key-internet-domain-name-functions [просмотрено 7 августа 2018 г.].

[25] Подробнее о передаче координирующих функций IANA и подотчетности ICANN см.: GIP Digital Watch observatory (no date) IANA Transition and ICANN Accountability. Адрес в Интернете: http://digitalwatch.giplatform.org/processes/iana [просмотрено 7 августа 2018 г.].

КООРДИНАЦИОННЫЙ ЦЕНТР
ДОМЕНОВ .RU/.РФ

Координационный центр национального домена сети Интернет (сокращенное название — Координационный центр доменов .RU/.РФ), создан в 2001 году для выработки правил регистрации доменных имен в доменах .RU и .РФ, аккредитации регистраторов и исследования перспективных проектов, связанных с развитием российского национального домена. Организации-учредители: общественно-государственное объединение «Ассоциация документальной электросвязи»(АДЭ), «Союз операторов интернет» (СОИ), Региональная организация «Центр интернет-технологий» (РОЦИТ) и Российский НИИ развития общественных сетей (РосНИИРОС). В 2015 году в состав учредителей также вошли Министерство связи и массовых коммуникаций Российской Федерации и Институт развития Интернета (ИРИ).

В своей деятельности Координационный центр опирается на опыт международных организаций, таких как Интернет-корпорация по присвоению имен и адресов (ICANN), Совет европейских национальных регистратур доменов верхнего уровня (CENTR), Азиатско-тихоокеанская ассоциация доменов верхнего уровня (APTLD), Международный союз электросвязи (МСЭ), Форум по управлению Интернет (IGF) и другие.

На сегодняшний день в ведении Координационного центра находятся вопросы, связанные с функционированием двух национальных доменов: домена .RU и кириллического домена .РФ. Как администратор национальных доменов .RU и .РФ, Координационный центр уделяет особое внимание их популяризации, расширению использования доменов частными лицами и организациями и, как следствие, росту числа зарегистрированных доменов второго уровня, а также повышению осведомленности российских интернет-пользователей о работе системы регистрации доменных имен.

Подробнее о Координационном центре доменов .RU/.РФ см.:
http://www.cctld.ru

RIGF RUSSIAN INTERNET GOVERNANCE FORUM

В настоящее время в поддержку глобального IGF ряд стран и регионов, заинтересованных в наиболее активном участии в вопросах управления интернетом, организуют региональные и национальные форумы IGF. Участники таких форумов обсуждают технические, организационные и правовые вопросы использования интернета на национальном уровне. Такие региональные площадки позволяют более глубоко и эффективно изучать проблемы управления интернетом на локальном уровне и в дальнейшем транслировать сформулированные выводы и предложения национальными представителями государственных органов, бизнес- структур и профессиональных интернет-сообществ на мировой уровень в рамках всемирного IGF.

В 2010 году к «семейству» мировых IGF присоединилась Россия. Проведение Первого российского форума по управлению интернетом, организованного Координационным центром национального домена сети Интернет при поддержке Минкомсвязи России, имело огромное значение. Данный форум стал первым региональным мероприятием подобного рода, проведенным на территории не только России, но и Восточной Европы. Российский форум по управлению интернетом проводится ежегодно, традиционно дата его проведения привязана к дню рождения домена .RU — 7 апреля.

В 2018 году в России прошел уже девятый по счету Российский форум по управлению интернетом. Он продолжил практику активного вовлечения в процесс глобального управления интернетом новых участников и изменения текущей повестки, которая требует обсуждения все более широкого круга смежных вопросов. Организатор RIGF 2018, как и всех предыдущих российских форумов — Координационный центр доменов .RU/.РФ.

Подробная информация о Российском форуме по управлению интернетом — на сайте форума http://rigf2018.ru/.

Фонд DiploFoundation — некоммерческая организация, ставящая своей целью повышение эффективности и открытости дипломатии и международного управления. В частности, деятельность фонда направлена на то, чтобы обеспечить:

- наращивание потенциала малых и развивающихся стран с целью полноценного участия в международной жизни;
- повышение подотчетности и открытости на международном уровне;
- легитимность международной политики;
- совершенствование методов глобального управления и международного нормотворчества.

Основные направления деятельности фонда Diplo:

Наращивание потенциала: В своей деятельности по наращиванию потенциала фонд Diplo уделяет основное внимание подготовке кадров и повышению квалификации специалистов различных организаций, их развитию и укреплению институциональной базы. Мы разрабатываем интернет-курсы и проводим исследования в области государственной политики, анализируем правоприменительную практику и оцениваем накопленный опыт. В зависимости от конкретной ситуации и потребностей комплекс мер может варьироваться. Темы, которыми мы занимаемся, включают управление Интернетом, вопросы электронной дипломатии, общественной и гуманитарной дипломатии, а также дипломатии в сфере глобального здравоохранения.

Мероприятия: Целевой аудиторией специальных мероприятий по вопросам глобального управления являются люди различных взглядов, включая дипломатов, представителей бизнеса и гражданского общества. При помощи электронных средств мы стремимся расширить доступ к нашим мероприятиям, в том числе посредством удаленного участия. В ходе мероприятий разрабатываются новые образовательные программы и публикации, осуществляется общение в режиме реального времени.

Курсы. Мы предлагаем курсы последипломного уровня и образовательные семинары по широкому спектру тем, связанных с дипломатией. Наша аудитория — дипломаты, государственные служащие, сотрудники международных и неправительственных организаций, а также все, кто изучает международные отношения. Использование новейших методик обучения на нашей уникальной образовательной площадке придает обучению гибкость, индивидуальный характер, интерактивный формат и способствует сплочению коллектива. Курсы проводятся в формате вебинара, очной или в очно-заочной форме.

Исследования. Мы расширяем потенциал нашей исследовательской методологии, используя, наряду с традиционными методами, интернет-технологии, в том числе краудсорсинг, анализ тенденций и проведение совместных исследований. Мы изучаем такие темы, как дипломатия, управление Интернетом и использование Интернета в обучении.

Публикации. Наши публикации посвящены как исследованиям современных тенденций, так и новому осмыслению традиционных аспектов дипломатии. Многие из наших публикаций доступны в электронном и печатном виде, а часть из них переведены на несколько языков.

Фонд Diplo был основан в 2002 г. правительствами Мальты и Швейцарии. Офисы фонда расположены в г. Мсида, Мальта, в Женеве, Швейцария и в Белграде, Сербия. С 2006 г. фонд Diplo имеет консультативный статус при ЭКОСОС ООН.

Подробнее о фонде Diplo см.: https://www.diplomacy.edu

Geneva Internet Platform

Женевская интернет-платформа (Geneva Internet Platform — GIP) создана по инициативе Федерального департамента иностранных дел Швейцарии (Swiss Federal Department of Foreign Affairs — EDA) и Федерального управления по связи (Federal Office of Communications — OFCOM). В задачи GIP входит наблюдение за развитием Интернета, проведение очных и заочных программ обучения и содействие обсуждению актуальных вопросов в этой области. GIP работает при поддержке швейцарских властей, а за оперативное управление организацией отвечает фонд Diplo.

В деятельности GIP существует три основных направления:

- Физическая платформа в Женеве
- Интернет-платформа и обсерватория
- Лаборатория инноваций

Особое внимание GIP уделяет поддержке небольших и развивающихся стран, чтобы помочь им включиться в управление Интернетом. Деятельность по этому направлению зависит от потребностей таких стран, и включает обучение, информационные компании, консультирование и проведение семинаров.

Подробнее о деятельности GIP см. http://www.giplatform.org

DigitalWatch

Инициатива GIP Digital Watch призвана обеспечить участникам процесса управления Интернетом и регулирования цифровых технологий возможность получать новейшую информацию о регулировании Интернета, участниках этого процесса и последних событиях. В основе работы GIP Digital Watch лежат материалы, знания в области управления и контакты, наработанные фондом Diplo за последние 20 лет.

В деятельности GIP Digital Watch выделяются три основных направления:

Обсерватория GIP Digital Watch — единый источник объективной информации о последних событиях, обзоров и пояснений, отчетов о мероприятиях, ресурсов и других материалов, связанных с вопросами управления Интернетом и его регулирования.

Информационный бюллетень Geneva Digital Watch — ежемесячное издание, содержащее обзор событий, интервью с видными экспертами и статьи по различным вопросам политики в сфере цифровых технологий.

Ежемесячные брифинги GIP по вопросам управления Интернетом из Женевы транслируются в Интернете. Такие мероприятия проводятся в последний четверг каждого месяца. По состоянию на 2016 г. по всему миру действуют отделения, которые занимаются повышением осведомленности местного населения и обменом опыта в ходе ежемесячных брифингов.

Подробнее о GIP Digital Watch см. https://digitalwatch.giplatform.org.

Глоссарий

3G	мобильные сети третьего поколения
4G	мобильные сети четвертого поколения
5G	мобильные сети пятого поколения
ACTA	Международное соглашение по борьбе с контрафактной продукцией
ADR	альтернативные средства урегулирования споров
AFRINIC	Африканский сетевой информационный центр
AFTLD	Ассоциация доменов верхнего уровня Африки
AI	Искусственный интеллект
ALAC	Расширенный консультативный комитет по делам индивидуальных пользователей (ICANN)
APC	Ассоциация прогрессивных коммуникационных технологий
APNIC	Азиатско-Тихоокеанский сетевой информационный центр
APTLD	Ассоциация доменов верхнего уровня Азиатско-Тихоокеанского региона
ARF	Региональный форум по безопасности Ассоциации стран Юго-Восточной Азии (АСЕАН)
ARIN	Американский регистр номеров Интернета
ARPAnet	Компьютерная сеть по перспективным исследованиям
ASEAN	Ассоциация стран Юго-Восточной Азии
AU	Африканский союз
AXIS	Проект Африканского союза по созданию точек обмена интернет-трафиком
BEREC	Совет европейских регуляторов рынка электронной связи
BGPSec	протокол BGPSec
BRICS	Бразилия, Россия, Индия, Китай и Южная Африка
BTA	базовое соглашение о телекоммуникациях
CA	служба сертификации
CBMs	меры по укреплению доверия
CCD COE	Центр повышения квалификации в области кибероборонь (НАТО)
ccNSO	Организация поддержки национальных доменов верхнего уровня (ICANN)
ccTLD	национальные домены верхнего уровня
CDNs	сети доставки контента
CEDAW	Конвенция о ликвидации всех форм дискриминации в отношении женщин (ООН)
CEFACT	Центр ООН по упрощению торговых процедур и электронному бизнесу
CEN	Европейский комитет по стандартизации
CENTR	Совет европейских национальных регистратур доменов верхнего уровня
CERN	Европейская организация ядерных исследований
CERT	Компьютерная группа реагирования на чрезвычайные ситуации
CGI.br	Управляющий комитет Бразилии по обеспечению работы интернета
CI	критически важный объект инфраструктуры
CIA	конфиденциальность, честность, доступность
CICTE	Межамериканский комитет по борьбе с терроризмом
CIDR	Механизм бесклассовой адресации
CIGF	Форум Содружества по управлению Интернетом
CII	ключевой объект информационной инфраструктуры
CIIP	защита ключевых объектов информационной инфраструктуры
CIR	критически важные ресурсы Интернета
CITEL	Межамериканская телекоммуникационная комиссия
CJEU	Суд Европейского союза
CND	сеть доставки контента
CoE	Совет Европы
COMESA	Общий рынок Восточной и Южной Африки
COP	Инициатива по защите ребенка в киберпространстве (МСЭ)
CRC	Конвенция ООН о правах ребенка
CRPD	Конвенция о правах инвалидов (ООН)
CSIRT	Группа реагирования на инциденты, связанные с компьютерной безопасностью
CSS	каскадные таблицы стилей
DDoS	распределенная атака типа «отказ в обслуживании»
DMCA	Закон об авторских правах в цифровую эпоху (США)
DNS	система доменных имен

DNSSEC	набор расширений для протокола DNS, обеспечивающих безопасность
DOA	цифровые идентификаторы объекта
DoS	отказ в обслуживании
DSL	цифровые абонентские линии
DWDM	спектральное уплотнение
ebXML	стандарт Electronic Business XML
ECTS	европейская система взаимозачета кредитов
EDI	электронный обмен данными
eIDAS	Постановление об оказании электронных услуг по идентификации и доверительных услуг в отношении электронных операций на внутреннем рынке (ЕС)
ENISA	Европейское агентство по сетевой и информационной безопасности
EPC	электронный код продукта
EPCIP	программа защиты критически важных объектов инфраструктуры
ETNO	Европейская ассоциация сетевых операторов
ETSI	Европейский институт по стандартизации в области электросвязи
EuroDIG	Европейский диалог об управлении Интернетом
EuroISPA	Европейская ассоциация поставщиков интернет-услуг
Europol	Европейское полицейское ведомство
FATF	Целевая группа по финансовым мероприятиям
FBI	Федеральное бюро расследований (США)
FCC	Федеральная комиссия по связи (США)
FIRST	Форум групп реагирования на инциденты и обеспечения безопасности
GAC	Правительственный консультативный комитет (ICANN)
GATS	Генеральное соглашение по торговле услугами
GATT	Генеральное соглашение по тарифам и торговле
GCA	Глобальная программа кибербезопасности
GCCS	Глобальная конференция по киберпространству
GCI	глобальный индекс кибербезопасности
GFCE	Глобальный форум по киберэкспертизе
GICGM	Комиссия высокого уровня по вопросам глобального сотрудничества и управления Интернетом
GIP	Женевская интернет-платформа

GSM	Глобальная система мобильной связи
GSMA	Ассоциация GSM
gTLD	родовой домен верхнего уровня
HD	высокое разрешение
HTCIA	Ассоциация по расследованию преступлений в сфере высоких технологий
HTML	язык разметки гипертекста
IaaS	инфраструктура как услуга
IAB	Совет по архитектуре Интернета
IANA	Уполномоченная организация по распределению нумерации в сети Интернет
IBP	оптовые поставщики услуг широкополосной связи
ICANN	Интернет корпорация по назначению имен и нумерации
ICC	Международная торговая палата
ICMEC	Международный центр по делам пропавших и эксплуатируемых детей
ICT	информационно-телекоммуникационные технологии
IDC	компания International Data Corporation
IDN	интернационализированные доменные имена
IEEE	Институт инженеров по электротехнике и электронике
IETF	Инженерный совет Интернета
IGC	Совещание по управлению Интернетом
IGF	Форум по управлению Интернетом
IMPACT	Международное многостороннее партнерство против киберугроз
INHOPE	Международная ассоциация горячих линий Интернета
INSAFE	Сеть безопасных интернет-центров
IoT	Интернет вещей
IP	интернет-протокол
IPR	права интеллектуальной собственности
IPSec	функция обеспечения сохранности IP-адресов
ISP	интернет-провайдер
ITAA	Американская ассоциация по информационным технологиям
IXP	точка обмена интернет-трафиком
LACNIC	Реестр адресов Интернета для стран Латинской Америки и Карибского бассейна

LACTLD	Ассоциация доменов верхнего уровня Латинской Америки и стран Карибского бассейна
LAN	локальная вычислительная сеть
LDCs	наименее развитые страны
LED	светоизлучающий диод
LGBTQ	лесбиянки, геи, бисексуалы, трансгендеры и гендерквиры
LIR	местная интернет-регистратура
LPWAN	энергоэффективная сеть дальнего радиуса действия
LTE	стандарт беспроводной высокоскоростной передачи данных
M3AAWG	Рабочая группа по противодействию компьютерным злоумышленникам в области передачи сообщений
MIS-NET	Комитет экспертов по интернет-посредникам (Совет Европы)
MLAT	договор о взаимной правовой помощи
MoU	меморандум о взаимопонимании
NAT	технология преобразования сетевых адресов
NIR	национальная интернет-регистратура
NRI	индекс сетевой готовности (WEF)
NSA	Агентство национальной безопасности (США)
NSI	компания Network Solutions Inc.
NTIA	Национальное управление по телекоммуникациям и информации (США)
OASIS	Организация по развитию стандартов структурированной информации
ODR	урегулирование споров в Интернете
OTT	технология OTT (услуги)
P2P	одноранговая сеть
PaaS	платформа как услуга
PIPA	Закон о защите прав на интеллектуальную собственность
PKI	инфраструктура «открытого ключа»
PLC	Интернет из розетки
PRISM	методология информационной системы по сбору персональных данных
PTI	общедоступные технические идентификаторы (ICANN)
QoS	качество услуг

REMJA	Объединение министров юстиции и других министров или генеральных прокуроров Американского континента
RFC	процедура запроса комментариев
RFID	радиочастотные метки-идентификаторы
RSPG	Группа по политике в области спектра радиочастот (ЕС)
SaaS	Программное обеспечение как услуга
SCADA	Система оперативно-диспетчерского управления
SGML	стандартный обобщенный язык разметки документов
SNA	сетевая архитектура системы
SOPA	Закон об интернет-пиратстве (США)
SOXA	Акт Сарбанеса-Оксли
SSL	уровень защищенных сокетов
TACD	Трансатлантический потребительский диалог
TASIM	Трансевроазиатская информационная магистраль
TCP/IP	протокол управления передачей / интернет-протокол
TLD	доменное имя верхнего уровня
TPP	Транстихоокеанское партнерство
TRIPS	Соглашение по торговым аспектам прав интеллектуальной собственности
TTIP	Трансатлантическое и инвестиционное партнерство
UDRP	Единая политика рассмотрения споров о доменных именах
UMAP	Университетская мобильность в регионе Азии и Тихого океана
UN	Организация Объединенных Наций
UN GGE	Группа правительственных экспертов ООН по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности
UNCITRAL	Комиссия ООН по праву международной торговли
UNGA	Генеральная Ассамблея ООН
UNTOC	Конвенция Организации Объединенных Наций против транснациональной организованной преступности
UPC	универсальный товарный код
US(A)	Соединенные Штаты Америки
VCR	видеокассетный магнитофон
VoIP	протокол передачи голоса по Интернету

VPN	частная виртуальная сеть
W3C	консорциум «Всемирная паутина»
WCIT	Всемирная конференция по международной электросвязи
WEF	Всемирный экономический форум
WGIG	Рабочая группа по управлению использованием Интернета
WiMax	технология широкополосного доступа в микроволновом диапазоне
WLAN	беспроводная локальная вычислительная сеть
WML	язык разметки для беспроводных устройств
WSIS	Всемирная встреча на высшем уровне по вопросам информационного общества
WTSA	Всемирная ассамблея МСЭ по стандартизации электросвязи
www	система World Wide Web
XHTML	расширяемый язык гипертекстовой разметки XHTML
XML	расширяемый язык разметки
ZB	зеттабайты
АТЭС	Азиатско-Тихоокеанское экономическое сотрудничество
БМР	Банк международных расчетов
ВДПЧ	Всеобщая декларация прав человека
ВОЗ	Всемирная организация здравоохранения
ВОИС	Всемирная организация интеллектуальной собственности
ВТО	Всемирная торговая организация
ГЧП	государственно-частное партнерство
ЕСПЧ	Европейский суд по правам человека
Интерпол	Международная организация уголовной полиции
КНТР	Комиссия по науке и технике в целях развития (ООН)
МВФ	Международный валютный фонд
МОТ	Международная организация труда
МСП	малые и средние предприятия
МСЭ	Международный союз электросвязи
МСЭ-D	Сектор развития электросвязи МСЭ
МСЭ-T	Сектор стандартизации электросвязи МСЭ
НАТО	Организация Североатлантического договора
НДС	налог на добавленную стоимость
ОАГ	Организация американских государств

ОБСЕ	Организация по безопасности и сотрудничеству в Европе
ОЭСР	Организация экономического сотрудничества и развития
ПРООН	Программа развития ООН
РМЭ	Регламент международной электросвязи
СПЧ ООН	Совет по правам человека ООН
УНП ООН	Управление по наркотикам и преступности ООН
ЦРТ	Цели развития тысячелетия
ЦУР	Цели устойчивого развития
ШОС	Шанхайская организация сотрудничества
ЭКОСОС	Экономический и социальный совет ООН
ЭСКАТО	Экономическая и социальная комиссия ООН для Азии и Тихого океана

Более полный перечень аббревиатур и сокращений по вопросам управления Интернетом содержится в глоссарии Internet Governance Acronym Glossary фонда Diplo по адресу:

https://www.diplomacy.edu/resources/books/internet-governance-acronym-glossary

Йован Курбалийя
директор фонда DiploFoundation
глава Geneva Internet Platform (GIP)

Йован Курбалийя является основателем и директором фонда DiploFoundation, а также главой Geneva Internet Platform (GIP). В прошлом профессиональный дипломат, он имеет опыт работы и исследований в области права, дипломатии и информационных технологий. В 1992 г. Й. Курбалийя создал Центр по информационным технологиям и дипломатии в Средиземноморской академии дипломатических исследований на Мальте. После более чем десяти лет успешной работы в сфере обучения, исследований и подготовки публикаций в 2003 г. Центр превратился в фонд DiploFoundation.

С 1994 г. доктор Курбалийя ведет курсы по влиянию ИКТ/Интернета на дипломатию и по управлению Интернетом. В настоящее время он читает лекции в Европейском колледже в Брюгге, Бельгия, а также в Университете Санкт-Галлена в Швейцарии. Раньше он преподавал в Средиземноморской академии дипломатических исследований на Мальте, Венской дипломатической академии в Австрии, Нидерландском институте международных отношений (Клингендал), Институте международных исследований и проблем развития в Женеве, Швейцария, Колледже персонала системы ООН в Турине, Италия, и Университете Южной Калифорнии в Лос-Анжелесе. Он разработал и в настоящее время возглавляет «Программу развития потенциала в области управления Интернетом» DiploFoundation (с 2005 г.). Основные исследовательские интересы доктора Курбалийи: становление международного режима Интернета, использование Интернета в дипломатии и переговорах, влияние Интернета на современные международные отношения.

Доктор Курбалийя — автор и редактор многочисленных книг, статей и глав. Среди его работ «Руководство по Интернету для дипломатов», «Знания и дипломатия», «Влияние информационных технологий на дипломатическую практику», «Информационные технологии и дипломатическая служба развивающихся стран», «Современная дипломатия» и «Язык и дипломатия». Совместно со Стефано Балди и Эдуардо Гелбстайном он является автором «Библиотеки информационного общества», серии из восьми брошюр, рассматривающих широкий спектр различных вопросов, связанных с Интернетом.

jovank@diplomacy.edu

УПРАВЛЕНИЕ ИНТЕРНЕТОМ

Йован Курбалийя

Введение в управление Интернетом представляет комплексный обзор основных вопросов и действующих лиц в области управления Интернетом. В книге, написанной простым и понятным широкому читателю языком и снабженной иллюстрациями и таблицами, рассматриваются технические, правовые, экономические, социокультурные и правозащитные аспекты управления Интернетом, а также вопросы безопасности и развития в этой сфере. Автор вводит читателей в круг проблем, анализирует основные направления деятельности и спорные вопросы, представляет различные точки зрения и подходы к решению стоящих перед отраслью задач, дает практическую основу для дальнейшего анализа и обсуждения вопросов управления Интернетом.

С 1997 г. в образовательных программах по материалам этой книги приняли участие свыше 3 тыс. дипломатов, специалистов в области компьютерных технологий, участников правозащитных организаций и представителей научного сообщества. Материалы обновляются и совершенствуются при проведении каждого курса, что делает книгу особо ценным методическим пособием для введения в вопросы управления Интернетом.