Академия ИКТ для лидеров государственного управления

Модуль 5

Управление использованием Интернета

Анг Пенг Хва

APCICT

АЗИАТСКО-ТИХООКЕАНСКИЙ УЧЕБНЫЙ ЦЕНТР ПО ИНФОРМАЦИОННЫМ И КОММУНИКАЦИОННЫМ ТЕХНОЛОГИЯМ ДЛЯ РАЗВИТИЯ

УДК 004
ББК 32.88
А 64

Серия модулей Академии ИКТ для лидеров государственного управления

Анг Пенг Хва

А 64 Модуль 5: Управление использованием Интернета. - Б.: 2009. - 68 с.

ISBN 978-9967-25-634-7
ISBN 978-9967-25-638-5 (общ.)

United Nations Asian and Pacific Training Centre for Information and Communication Technology for Development (UN-APCICT)
Bonbudong, 3rd Floor Songdo Techno Park
7-50 Songdo-dong, Yeonsu-gu, Incheon City
Republic of Korea

Телефон: +82 32 245 1700-02
Факс: +82 32 245 7712
E-mail: info@unapcict.org
http://www.unapcict.org

A 2303010000-09
ISBN 978-9967-25-634-7
ISBN 978-9967-25-638-5 (общ.)

УДК 004
ББК 32.88

ПРЕДИСЛОВИЕ К СЕРИИ МОДУЛЕЙ АКАДЕМИИ ИКТ ДЛЯ ЛИДЕРОВ ГОСУДАРСТВЕННОГО УПРАВЛЕНИЯ

21 век характеризуется растущей взаимозависимостью людей в глобализирующемся мире. Это мир, где открываются возможности для миллионов людей с помощью новых технологий, расширенного доступа к необходимой информации и знаниям, которые могут существенно улучшить жизнь людей и способствовать сокращению бедности. Но это возможно лишь в том случае, если растущая взаимозависимость сопровождается обменом ценностей, приверженностью и солидарностью для всеобъемлющего и устойчивого развития, где прогресс служит всем народам.

Что касается развития информационно-коммуникационных технологий (ИКТ), то в последние годы Азия и Тихий океан были «регионом превосходной степени». По данным Международного союза электросвязи в регионе проживают более 2 млрд. абонентов фиксированной связи и 1,4 млрд. подписчиков мобильной связи. К середине 2008 г. только в Китае и Индии насчитывалось четверть всех мобильных телефонов в мире. На Азиатско-Тихоокеанский регион также приходится 40 процентов мировых Интернет-пользователей и самый большой в мире рынок широкополосного Интернета с долей в 39 процентов от общемирового объема.

На фоне быстрого технического прогресса многие задались вопросом о возможности устранения цифрового неравенства. К сожалению, ответ на данный вопрос – пока «еще нет». Даже спустя пять лет после Всемирной встречи на высшем уровне по вопросам информационного общества (ВВУИО), состоявшейся в Женеве в 2003 году, и, несмотря на все впечатляющие технологические достижения и обязательства ключевых игроков в регионе, основные средства связи до сих пор находятся вне доступа подавляющего большинства людей, особенно бедных.

Более чем в 25 странах региона, главным образом, небольших островных развивающихся государствах и развивающихся странах, не имеющих выхода к морю, имеются менее 10 пользователей Интернета на 100 человек, и эти пользователи, в основном, сосредоточены в крупных городах, в то время как некоторые развитые страны в регионе имеют соотношение более 80 пользователей Интернета на 100 человек. Различие в обеспечении широкополосным Интернетом между развитыми и развивающимися странами еще более впечатляющее.

В целях преодоления цифрового неравенства и реализации потенциала ИКТ для всеобъемлющего социально-экономического развития в регионе разработчикам политики в развивающихся странах необходимо будет установить приоритеты, принять политику, разработать нормативно-правовую базу, выделить финансовые средства, а также содействовать налаживанию партнерских связей, способствующих развитию отрасли ИКТ-индустрии и навыков в области ИКТ среди своих граждан.

В Плане действий ВВУИО говорится: «… каждый человек должен иметь возможность приобрести необходимые навыки и знания для того, чтобы понять, участвовать и использовать преимущества информационного общества и экономики знаний». С этой целью в рамках Плана действий содержится призыв к международному и региональному сотрудничеству в области наращивания потенциала с упором на создание критической массы квалифицированных специалистов и экспертов в области ИКТ.

Именно в ответ на этот призыв Азиатско-Тихоокеанский учебный центр по информационным и коммуникационным технологиям для развития (АТУЦ ИКТР) разработал данную всеобъемлющую учебную программу по обучению ИКТ для развития – *Академия ИКТ для лидеров государственного управления* – состоящей в настоящее время из восьми самостоятельных, но взаимосвязанных модулей, направленных на распространение основных знаний и опыта, которые помогут разработчикам политики планировать и осуществлять инициативы в области ИКТ более эффективно.

АТУЦ ИКТР является одним из пяти региональных институтов Экономической и социальной комиссии для Азии и Тихого океана (ЭСКАТО). ЭСКАТО содействует устойчивому и всеобъемлющему социально-экономическому развитию в Азии и Тихоокеанском регионе на основе анализа, нормативной работы, наращивания потенциала, регионального сотрудничества и обмена знаниями. В партнерстве с другими агентствами ООН, международными организациями, национальными партнерами и заинтересованными сторонами ЭСКАТО через АТУЦ ИКТР обязуется оказывать поддержку использованию, усовершенствованию и переводу данных модулей *Академии* в разных странах, а также организацию их преподавания на регулярной основе через национальные и региональные семинары для правительственных должностных лиц старшего и среднего уровня, цель которых в том, чтобы возросший потенциал и полученные знания трансформировались в зрелое понимание выгод от ИКТ и конкретные меры в достижении целей в области развития.

Ноэлин Хейзер

Заместитель Генерального секретаря Организации Объединенных Наций
Исполнительный секретарь ЭСКАТО

ПРЕДИСЛОВИЕ

Путешествие в процесс разработки серии модулей *Академии ИКТ для лидеров государственного управления* было поистине вдохновляющим и поучительным опытом. Оно не только послужило для заполнения пробелов в создании потенциала в области ИКТ, но также проложило новый путь для разработки программ учебных курсов – через участие многочисленных людей и чувства причастности к процессу.

Академия является флагманом программ АТУЦ ИКТР, разработанного на основе активных исследований и анализа сильных и слабых сторон существующих учебных материалов, а также процесса рецензирования среди ведущих экспертов. Во многих регионах прошли обучающие семинары *Академии*, обеспечивших неоценимую возможность для обмена опытом и знаниями между участниками из разных стран, процесс, который сделал *выпускников Академии* ведущими игроками по подгонке и формированию модулей.

Начало преподавания первых восьми модулей *Академии* на национальном уровне знаменует собой зарождение жизнетворного процесса укрепления существующих партнерских отношений и построение новых для усиления потенциала в области разработки политики ИКТ для развития (ИКТР) по всему региону. АТУЦ ИКТР выражает приверженность к оказанию технической поддержки в начале деятельности *национальных Академий*, как своего ключевого подхода в обеспечении процесса охвата *Академией* всех разработчиков политики. Центр тесно сотрудничает с рядом региональных и национальных учебных заведений, которые уже имеют непосредственную связь с центральными, государственными и местными органами управления по усилению их потенциала в области ИКТР путем локализации, перевода и обучения модулей *Академии*, которые уделяют особое внимание национальным потребностям и приоритетам. Также существуют планы по дальнейшему расширению масштаба и охвата существующих модулей и разработке новых.

Кроме того, АТУЦ ИКТР берет на вооружение многоуровневый подход для обеспечения того, что содержание модулей *Академии* достигнет большей аудитории в регионе. Наряду к непосредственному обучению материалов *Академии* через региональные и национальные Академии АТУЦ ИКТР учредил Виртуальную Академию АТУЦ ИКТР (APCICT Virtual Academy, AVA), которая является сетевой дистанционной обучающей платформой *Академии* и предназначена для обеспечения участников возможностью изучать материалы по своему усмотрению. AVA гарантирует, что все модули *Академии* и сопутствующие материалы, такие как слайды презентаций и тематические исследования легко доступны в сети для загрузки, многократного использования, усовершенствования и локализации, а также она содержит различные функции, в том числе виртуальные лекции, учебные средства для организации процесса обучения и разработки нового содержания, а также сертификации.

Первоначальная серия из восьми модулей и их обучение в рамках региональных, субрегиональных и национальных семинаров *Академии* было бы невозможно без приверженности делу и инициативного участия многих людей и организаций. Я хотела бы воспользоваться этой возможностью, чтобы отметить усилия и достижения *выпускников Академии* и наших партнеров из правительственных ведомств, учебных заведений, а также региональных и национальных организаций, принявших участие в семинарах *Академии*. Они не только внесли ценный вклад в содержание модулей, но, что более важно, они стали сторонниками *Академии* в своих странах, в результате чего были подписаны соглашения между АТУЦ ИКТР и рядом национальных и региональных учреждений-партнеров в целях усовершенствования и проведения регулярных курсов *Академии* в странах.

Также я хотела бы добавить особую признательность самоотверженным усилиям многих выдающихся людей, которые сделали данное необычайное путешествие возможным. Это Шахид Акхтар, советник проекта *Академии*; Патриция Аринто, редактор; Кристина Апикул, выпускающий редактор; все авторы модулей *Академии* и команда АТУЦ ИКТР.

Для того чтобы ценные знания, изложенные в Академии, резонансно распространялись среди людей во всех уголках Азии и Тихого океана, АТУЦ ИКТР и его партнеры неустанно работали над переводом и локализацией содержания Академии. Именно благодаря этим усилиям мы в настоящее время публикуем русскую версию Академии.

Команда по подготовке русской версии *Академии* провела много времени, чтобы терминология соответствовала текущему применению в языке, нюансы и тонкости были отражены, а перевод содержания был обоснован. В этом смысле они оказались вторыми авторами модулей *Академии*. Я хотела бы выразить мою глубокую признательность Национальному центру информационных технологий в Кыргызстане, его сотрудникам за их самоотверженные усилия и приверженность этой инициативе. В частности, я хотела бы отметить выдающуюся работу, проделанную Алмазом Бакеновым, Мунар Усубалиевой, Бэллой Молдобаевой, Андреем Смиренским, Дмитрием Петренко, Аманбеком Бавланкуловым, Эмилем Албановым и Медером Мамутовым.

Я искренне надеюсь, что *Академия* будет способствовать народам по сокращению нехватки человеческих ресурсов в области ИКТ, устранению барьеров на пути внедрения ИКТ, содействовать применению ИКТ в ускорении социально-экономического развития и достижения Целей развития тысячелетия.

Хеун-Сук Ри

Директор
АТУЦ ИКТР

О СЕРИИ УЧЕБНЫХ МОДУЛЕЙ

В современный «век информации» простой доступ к информации меняет наш образ жизни, работы и развлечений. «Цифровая экономика», также известная как «экономика знаний», «сетевая экономика» или «новая экономика», характеризуется переходом от производства товаров к созданию идей. Это подчеркивает рост, если уже не главенство, роли информационных и коммуникационных технологий (ИКТ) в экономике и в обществе в целом.

Как следствие, правительства во всем мире уделяют все больше внимания на ИКТ в целях развития (ИКТР). Для правительств этих стран ИКТР заключается не только в развитии индустрии ИКТ или сектора экономики, но также и во включении ИКТ в экономику для стимулирования как социального, так и политического роста.

Тем не менее, помимо трудностей, с которыми сталкивается правительство при разработке политики в области ИКТ, существует тот факт, что разработчики политики зачастую не знакомы с технологиями, которые они используют в целях национального развития. Поскольку никто не может управлять тем, с чем не знаком, многие политики уклоняются от разработки политики в области ИКТ. Но предоставление разработки политики в области ИКТ «технарям» также неправильно, поскольку зачастую они не имеют представления о политических последствиях разработки и использования технологий.

Серия модулей Академии ИКТ для лидеров государственного управления была разработана Азиатско-Тихоокеанским учебным центром ООН по информационным и коммуникационным технологиям в целях развития (АТУЦ ИКТР) для:

1. Политиков общенационального и местного уровней управления, ответственных за разработку политики в области ИКТ;

2. Государственных должностных лиц, ответственных за разработку и внедрение приложений на основе ИКТ;

3. Руководителей государственного сектора, стремящихся использовать средства ИКТ для управления проектами.

Серия модулей стремится познакомить с практическими вопросами, связанными с ИКТР, с точки зрения, как политики, так и технологии. Цель состоит не в разработке технического руководства по ИКТ, а скорее в том, чтобы обеспечить хорошее понимание возможностей современных цифровых технологий или в каком направлении они будут развиваться, и что это означает для разработки политических решений. Темы, раскрываемые в модулях, были определены на основе анализа потребностей в обучении и изучения учебных материалов, применяемых в других странах мира.

Данные модули разработаны таким образом, что они могут применяться для самостоятельного изучения отдельными читателями, либо в качестве ресурса в ходе подготовки или программы. Эти модули сами по себе являются автономными, но в то же время связаны между собой, и были предприняты усилия, чтобы связать между собой темы и обсуждения в модулях серии. Долгосрочной целью является объединение модулей в цельный курс, который может пройти соответствующую сертификацию.

В начале каждого модуля излагаются цели и задачи обучения, по которым читатель сможет оценить свои успехи. Содержание модуля разбито на отдельные разделы, включающие тематические исследования и упражнения, помогающие глубже понять ключевые концепции. Упражнения можно выполнять индивидуально и в группах. Для иллюстрации определенных аспектов обсуждения в модуль включены таблицы и рисунки. Также вниманию читателей представлены ссылки на литературные источники и Интернет-ресурсы, чтобы предоставить возможность получения дополнительной информации и знаний.

Применение ИКТР является настолько разнообразным, что некоторые тематические исследования и примеры, рассматриваемые в учебных модулях, могут показаться противоречащими друг другу. Этого следует ожидать, так как это очень новая и сложная дисциплина, и предполагается, что все страны мира должны включиться в процесс изучения возможностей ИКТ в качестве инструмента для развития.

Поддержка серии модулей Академии в печатном формате осуществляется на платформе интерактивного дистанционного обучения в сети – Виртуальной Академией АТУЦ ИКТР (AVA – http://www.unapcict.org/academy) — в которой применяются виртуальные классы, показывающие выступления преподавателей в видео формате и презентации PowerPoint учебных модулей.

Кроме того, АТУЦ ИКТР разработал электронный центр ИКТР для совместной работы (e-Collaborative Hub) (e-Co Hub – http://www.unapcict.org/ecohub), выделенный сетевой ресурс для практиков и политиков в целях повышения их опыта в области обучения и преподавания. E-Co Hub предоставляет доступ к ресурсам знаний по различным аспектам ИКТР и обеспечивает интерактивное пространство для обмена знаниями и опытом, а также сотрудничество в продвижении ИКТР.

МОДУЛЬ 5

Интернет порождает существенные вызовы для государственной политики и устойчивого развития человеческих ресурсов как в международном масштабе, так и в отдельных странах. Таким образом, дальнейшее развитие международной политики и процессов заключается в управлении использования и работы сети Интернет. Хотя Азиатско-Тихоокеанский регион обладает самой большой долей мировых Интернет-пользователей, тем не менее, он недостаточно представлен на форумах, которые разрабатывают политику, имеющую отношение к развитию Интернета. Имеется ряд вопросов и конкретных проблем, связанных с вопросами управления Интернетом в региональном контексте. Правительства с формирующейся рыночной экономикой должны понимать эти проблемы, если они собираются иметь право голоса в глобальной информационной сети.

Цели Модуля

Настоящий модуль преследует следующие цели:

1. Описать текущее развитие международной политики и процедуры, которые регулируют использование и эксплуатацию сети Интернет;
2. Дать общее представление о проблемах и конкретных задачах, связанных с управлением использованием Интернета в региональном контексте.

Итоги обучения

После завершения изучения модуля читатели должны уметь:

1. Описывать развитие международной политики и процедур, регулирующих использование и эксплуатацию сети Интернет;
2. Обсуждать ключевые вопросы управления использованием Интернета с точки зрения развивающихся стран;
3. Обозначить первые шаги в направлении более эффективного управления использованием сети Интернет в своих странах.

СОДЕРЖАНИЕ

Список тематических исследований

Список рисунков

Сокращения

АТУЦ ИКТР	Азиатско-Тихоокеанский учебный центр по информационным и коммуникационным технологиям для развития
ccTLD	Национальный домен верхнего уровня
CoE	Совет Европы
CSC	Центр общих сервисов, Индия
DEC	Корпорация цифрового оборудования
DNS	Система доменных имен
ЭСКАТО	Экономическая и социальная комиссия для Азии и Тихого океана
EC	Европейский союз
FOSS	Свободное и открытое программное обеспечение
GPS	Система глобального позиционирования
gTLD	Общий домен верхнего уровня
ICANN	Интернет-корпорация по управлению доменными именами и числовыми адресами в Интернете
ICPEN	Международная сеть по защите прав потребителей и борьбе с мошенничеством
ICRA	Ассоциация оценки содержимого Интернет
ИКТ	Информационные и коммуникационные технологии
ИКТР	Информационные и коммуникационные технологии для развития
IP	Интернет протокол
IPv4	Интернет протокол 4-й версии
IPv6	Интернет протокол 6-й версии
МСЭ	Международный союз электросвязи
ЦРТ	Цели развития Тысячелетия
ОЭСР	Организация экономического сотрудничества и развития
RIAA	Американская ассоциация звукозаписывающих компаний
RIR	Региональный Интернет-регистратор
TCP/IP	Протокол управления передачей/Интернет протокол
TLD	Домен верхнего уровня
ООН	Организация Объединенных Наций
США	Соединенные Штаты Америки
РГУИ	Рабочая группа по управлению использованием Интернет
ВВУИО	Всемирная встреча на высшем уровне по вопросам информационного общества

Список условных обозначений


Тематическое исследование


Вопросы для размышления


Практическое упражнение


Проверьте себя

1. ПРОБЛЕМЫ И ОБЛАСТЬ УПРАВЛЕНИЯ ИНТЕРНЕТОМ

Задачей данного раздела является представить краткую историю и предпосылки необходимости управления использованием Интернета и кратко обрисовать область действия управления использованием Интернета.

1.1 Введение

Очень часто предполагается, что новая среда общения, именуемая Интернетом, не может подвергаться регулированию. Это понятно, поскольку его первые пользователи часто и громко заявляли, что Интернет является изобретением, предназначенным для выживания при ядерном нападении, преодоления блокады с помощью обводной маршрутизации, пересечения многочисленных международных границ и, таким образом, быть недоступным для цензуры. Быть недоступным для цензуры означает, что его содержание трудно, если не невозможно, подчинять какой-либо политике и, как следствие, сложно управлять пользователями.[1]

Теперь, спустя 10 лет после того, как Интернет стал публично доступным, мы знаем, что эти представления об Интернете – мифы и что Интернет может быть регламентирован. В действительности, чем более развита страна, тем она больше имеет правил, касающихся Интернета, в то время как у менее развитых стран существует очень немного или отсутствуют правила, регулирующие Интернет. Отсутствие правил может привести к тому, что развивающиеся страны могут стать убежищем для тех, кто заинтересован в причинении вреда с использованием Интернета, например, как спам и мошенничество.

Дело не в количество правил и законов, которые подавляют использование Интернета. Если бы это было так, то США были бы самыми подавляющими в использовании Интернета, а такая страна, как Народно-Демократическая Республика Лаос, которая все еще возится с проблемами построения инфраструктуры, процветала бы в Интернете. Важно то, что правила, регулирующие Интернет, должны быть разработаны на основе четкого понимания юридических и технических аспектов и в рамках международного сотрудничества. Целью этого модуля является разъяснение данных вопросов и возможных путей достижения международного сотрудничества в области управления использованием Интернета.

1.2 История и технические предпосылки создания Интернет

Историческое и техническое развитие

Интернет был изобретен не для создания коммуникационной среды, которая сохранит работоспособность после ядерной атаки, а сети, которая позволит физикам распределенно использовать компьютеры для решения задач, требующих интенсивных вычислений. В то время компьютеры представляли собой громоздкое дорогостоящее оборудование, занимавшее обширные пространства.[2] Метод, по которому были

1 Peng Hwa Ang, *Ordering Chaos: Regulating the Internet* (Singapore: Thomson, 2005).
2 Katie Hafner and Mathew Lyon, *Where Wizards Stay Up Late: The Origins of the Internet* (New York: Simon and Schuster, 1998).

соединены компьютеры, использовал протокол, изобретенный в 1960-ых годах, который не зависел от используемой технологии в сети. Данное решение было нестандартным, так как любой человек подумает, что для отправки сообщения из одного места в другое необходимо использовать достаточно хорошее оборудование и технологии. Вместо этого предложенный протокол позволил посылать компьютерные сообщения и транзакции в форме отдельных пакетов, которые вновь собирались по прибытии в место назначения. Если сообщение не было получено в полном объеме или без ошибок, то оно пересылалось заново. Такой способ передачи означал, что не было необходимости передающей сети или каналу иметь свойство «интеллекта». Все, что было необходимо, - это маршрутизаторы, чтобы указать сообщениям, куда следовать, после чего сообщения находили бы свою дорогу сквозь «глупую сеть». С помощью данного «Межсетевого протокола» сообщения гораздо лучше пересекали различные сети, чем с протоколом, используемым для телефонной связи.

Превосходство Межсетевого протокола стало намного очевидней с 1970-ых годов, когда телефонные компании начали внедрять интеллектуальные технологии в свои сети.[3] Несмотря на то, что Международный союз электросвязи (МСЭ), агентство Организации Объединенных Наций (ООН) для координации глобальных сетей связи, разработал некоторые протоколы и стандарты, различие во взглядах привело к столкновению, которое, в конечном счете, свелось в пользу Межсетевого протокола над протоколом телефонных компаний.

История управления использованием Интернета[4]

Следует иметь в виду, что протоколы и стандарты имеют весьма важное значение в мире технологий, так как тот, кто контролирует их, может диктовать, а тот, кто не контролирует, будет всегда следовать по направлению развития технологий. В случае с Интернетом протокол, использовавшийся для спряжения различных сетей, теперь называется Протоколом управления передачей/Протоколом Интернета (Transmission Control Protocol/Internet Protocol - TCP/IP). Данный коммуникационный протокол, изобретенный Винтом Серфом (Vinton Cerf) и Бобом Ханом (Bob Kahn) в 1974 году, оказался настолько важен для функционирования сети, что любая сеть, которая использовала TCP/IP, рассматривалась в качестве Интернета.

Для раскрытия основной цели модуля отметим наиболее интересный принцип работы протокола – это отсутствие непосредственного управления процессом передачи данных по сети; управляется только адрес, посредством которого осуществляется коммуникация. Проблема адресов заключалась в необходимости кого-либо, кто обеспечивал бы отсутствие конфликтов адресов. Для обозначения сетей Глобальная Система адресации использовала номера. Некое лицо или учреждение должно обеспечить, чтобы никакие два адреса не использовали идентичные номера — то есть, должно быть центральное руководство для устранения таких конфликтов. Таким образом, речь идет о том, что Джон Постель (Jon Postel), получивший все свои ученые степени в университете Калифорнии в Лос-Анджелесе, а затем перебравшийся в университет Южной Калифорнии для работы в качестве директора Института информатизации (Information Sciences Institute), стал «богом Интернета», как назвал его журнал *«Экономист»*. Он разрешал такого рода конфликты, тем самым, способствуя дальнейшему росту сети.

3 David S. Isenberg, “The Dawn of the Stupid Network,” *ACM Networker* 2.1 February/March (1998): 24-31, http://www.isen.com/papers/Dawnstupid.html.

4 Any book that touches on the history of the Internet would be a good resource. Two such book are Hafner and Lyon’s *Where Wizards Stay Up Late*, and Jack Goldsmith and Tim Wu’s *Who Controls the Internet: Illusions of a Borderless World*. A reliable online resource is The Internet Society’s *Histories of the Internet* at http://www.isoc.org/internet/history.

Поскольку число сетей росло, становилось все более и более сложно запоминать номера для каждой из них. Так, в 1983 году Постель и Пол Мокапетрис (Paul Mockapetris) предложили присваивать номерам имена. Например, вместо того, чтобы набирать 64.233.161.18, можно было бы указать google.com для вызова поисковой системы. Это было эквивалентно присваиванию имен системе телефонных номеров. Таким образом, появилась Система Доменных Имен (Domain Name System, DNS).

DNS сама по себе также создала некоторые правовые проблемы, которые будут рассмотрены в следующем разделе. На данный момент важно просто понять работу DNS для понимания всей проблемы.[5]

DNS представляет собой иерархическую систему, использующую древовидную структуру для организации информации о сетях и компьютерах. Это напоминает почтовый адрес: точно так же как кто-либо помещает адрес улицы в начале и название страны в конце, таким же образом домен верхнего уровня (TLD) располагается в конце, а более конкретный сетевой адрес – в начале. Таким образом, когда компьютер ищет в Интернете адрес, поиск производится справа налево путем опроса каждого последующего сервера о названии с левой стороны от него.

Когда в январе 1985 года впервые были введены домены верхнего уровня (TLDs) , их было всего шесть:

COM – для коммерческих организаций
EDU – для образовательных учреждений
NET – для сетевых провайдеров
ORG – для некоммерческих организаций
MIL – для военных США
GOV – для правительства США[6]

С тех пор были добавлены другие (gTLDs) домены верхнего уровня общего назначения.[7] Пожалуй, наиболее важным для наших целей является создание страновых доменов верхнего уровня (ccTLDs). Эти коды напоминают, но не совпадают с двухбуквенными кодами ISO 3166-1 альфа-2 для стран и зависимых территорий, которые используются в международной торговле.[8] У Соединенных Штатов Америки также есть двухбуквенный код ccTLD (US). Но в силу своего исторического доминирования и преимущества первооткрывателя домены верхнего уровня общего назначения gTLD без кода страны, особенно COM, считаются под влиянием США или кого-либо, что означает выражение глобальных амбиций.

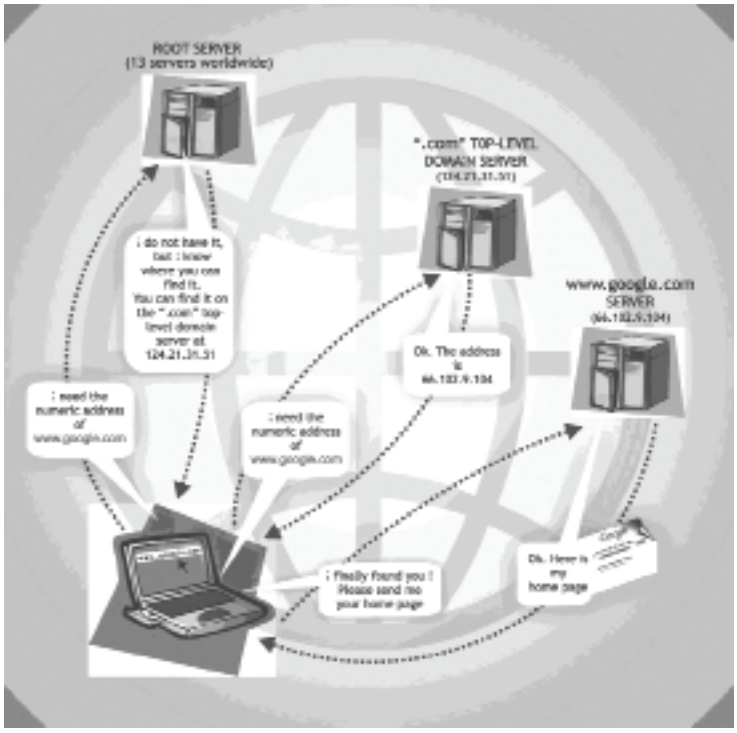
Наличие ccTLDs означает, что правительства на основании древовидной иерархической структуры могут самостоятельно распоряжаться доменами более низкого уровня. Так, yahoo.fr, например, будет подчиняться правилам, установленным администратором DNS во Франции. Так, в известном случае французский суд постановил, что Yahoo не может продавать нацистские сувениры на своем вебсайте, предназначенном для французской аудитории. Французский суд может вмешаться и навязать такое решение потому, что доменное имя — yahoo.fr — было зарегистрировано во Франции. Yahoo впоследствии переименовал свой вебсайт для франкоязычных пользователей на fr.yahoo.com. Как видите, новый адрес вебсайта находится в домене COM, на Yahoo и на сервере, маркированном FR. Новый адрес действительно означает, что Yahoo может

5 See http://en.wikipedia.org/wiki/Domain_name_system for a more detailed account of the DNS.
6 See http://en.wikipedia.org/wiki/Generic_top-level_domain for a more detailed account of the TLD system.
7 For a definitive list, see http://data.iana.org/TLD/tlds-alpha-by-domain.txt. A more reader-friendly list is available at http://en.wikipedia.org/wiki/List_of_Internet_top-level_domains.
8 See http://en.wikipedia.org/wiki/ISO_3166-1_alpha-2 for more details about ISO 3166-1 alpha-2.

пренебречь французскими законами, хотя для этого нет веских коммерческих причин. Действительно, Yahoo переименовал все свои зарубежные сайты таким образом, чтобы адреса заканчивались на COM.

Существует еще один технический вопрос, который необходимо обсудить. Это касается корневого сервера. Когда компьютер ищет адрес, он делает это справа налево. Поскольку gTLD располагается в правой части веб-адреса, первое, что должен просматривать компьютер – это то, что на самом правом конце. Так, для www.google.com компьютер должен начать поиск с .com. Современные DNS-правила «вставили» невидимый символ (предполагаемую точку): все доменные имена в Интернете на самом деле заканчиваются точкой («.») или же полной остановкой (full-stop), которая направляется на сервер, называемый корневым сервером. Существует 12 корневых организаций, называемых операторами корневых серверов, которые работают на серверах, маркированных от A до M. Сервер A функционирует в качестве основного (мастер) сервера, обменивающегося информацией с серверами от B до M несколько раз в день, так что информация всегда является текущей. На практике большая часть информации хранится на других серверах, распределенных по всему миру для резервирования, чтобы минимизировать трафик в Интернете и ускорить доступ. Вся эта область называется корневой зоной.[9] Поскольку корневая зона имеет огромное значение для работы всего Интернета, существует еще один сервер, который скрыт от хакеров, называемый скрытым сервером. Скрытый сервер и мастер-серверы A физически расположены в США.

Рисунок 1. Определение веб-сайта в Интернете
(Источник: DiploFoundation, http://textus.diplomacy.edu/textusbin/env/scripts/Pool/GetBin.asp?IDPool=1175)



Здесь возникает вопрос, а что случится с Интернетом в стране, которая окажется в состоянии войны с США. Может ли Администрация США, например, удалить эту страну из файла корневой зоны так, что она исчезнет из Интернета?

9 Wolfgang Kleinwächter, “De-Mystification of The Internet Root: Do We Need Governmental Oversight?” in *Reforming Internet Governance*, ed. William J. Drake (New York: UN ICT Task Force, 2005), 209-225, http://www.wgig.org/docs/book/WGIG_book.pdf.

Перед войной в Ираке доменное имя IQ исчезло из Интернета. Домен IQ не использовал ни один из приближенных Саддам Хуссейна, кроме палестинских арабов, живущих в Техасе. Операторы доменного имени, братья Элаши (Elashi) и их деловые партнеры, были арестованы и обвинены в 2002 году в незаконном экспорте компьютерных частей в Ливию и Сирию. Преднамеренно или нет, но система доменного имени IQ была отключена как раз перед войной. 28 июля 2005 года в то время, когда был закончен отчет под мандатом ООН Рабочей группы по управлению Интернетом (РГУИ) и до момента, когда он был переведен на официальные языки ООН, доменное имя IQ было передано иракскому правительству. Причина состояла в том, что только в это время появилось постоянное и дееспособное иракское правительство.

Контроль над корневой зоной, по-видимому, является ключевым вопросом в управлении использованием Интернета. Однако существуют и другие проблемы. Некоторые страны также обеспокоены вопросом распределения IP-адресов. Из-за случайного и незапланированного развития Интернета оказалось, что некоторые американские университеты обладают большим количеством IP-адресов, чем некоторые страны. Проблема не только в принципе распределения IP-адресов, но также и в том, что количество IP-адресов может быть исчерпано. В системе Интернет-протокола версии 4 (IPv4) для использования доступно 4,294,967,296 уникальных IP-адресов. Поскольку численность глобального населения намного больше, чем это число, существует вероятность исчерпывания IP-адресов. В определенной степени этот вопрос будет решен более эффективным использованием системы IP-адресов и внедрением Интернет-протокола версии 6 (IPv6), который имеет 340,282,366,920,938,463,374,607,43 2,768,211,456 (340 миллиардов триллионов триллионов) уникальных IP-адресов.[10]

Вопрос управления использованием Интернета был поднят во время Всемирной встречи на высшем уровне по вопросам информационного общества (ВВУИО) в 2003 году. В то время как многие страны хотели рассмотреть вопрос управления использованием Интернета, у США было свое мнение о том, что пока нет достаточного потенциала, особенно в развивающихся странах, чтобы участвовать в решении данного вопроса. Таким образом, было решено, что Генеральным секретарем ООН будет создана рабочая группа, которая представит отчет по данному вопросу. Декларация принципов ВВУИО гласит:

> 50. Вопросы управления использованием Интернета на международном уровне следует решать согласованным образом. Мы обращаемся к Генеральному секретарю Организации Объединенных Наций с просьбой учредить рабочую группу по управлению использованием Интернета в рамках открытого и всеобъемлющего процесса, обеспечивающего механизм для полномасштабного и активного участия органов государственного управления, частного сектора и гражданского общества как из развивающихся, так и развитых стран, в том числе соответствующих межправительственных и международных организаций и форумов, в целях изучения вопроса об управлении использованием Интернета и представления к 2005 году в надлежащих случаях предложений для принятия решения в отношении организации управления использованием Интернета.[11]

10 OECD, “Governments and business must tackle Internet address shortage together, says OECD,” 15 May 2008, http://www.oecd.org/document/29/0,3343,en_2649_34223_40542045_1_1_1_1,00.html.

11 World Summit on the Information Society, *Declaration of Principles – Building the Information Society: A global challenge in the new Millennium* (12 December 2003), http://www.itu.int/wsis/docs/geneva/official/dop.html.

Рабочей группе по управлению использованием Интернета (РГУИ), состоявшей из 40 человек, было поручено проведение расследования обстоятельств и установление фактов – т.е. определить, в чем заключается управление использованием Интернета, какие существуют вопросы и кто должен что делать. Это из отчета РГУИ, который будет рассмотрен далее.

Вопросы для размышления

Какое значение имеет управление использованием Интернета в вашей стране?

Проверьте себя

1. Что явилось источником происхождения Интернет? Создан ли он был для того, чтобы средства связи смогли пережить ядерную атаку?
2. Часто можно услышать о том, что Интернет не имеет центрального органа управления. Правда ли это?
3. Каким образом DNS организует Интернет?
4. В чем состоит разница между IP-адресом и доменным именем?
5. В чем практическая разница между IPv4 и IPv6?

2. МНОГОСТОРОННЕЕ И МНОГОСЕКТОРАЛЬНОЕ УПРАВЛЕНИЕ ИСПОЛЬЗОВАНИЕМ ИНТЕРНЕТА

Задачей данного раздела является дать общее представление о заключительном докладе РГУИ, политической напряженности вокруг наиболее спорных аспектов управления использованием Интернета, а также повышении роли Форума по управлению использованием Интернета.

Беспокойство в вопросах соблюдения законности в области управления использованием Интернета заключается в том, чтобы рекомендации не подорвали функционирования Интернета. Таким образом, РГУИ приняла ряд руководящих принципов по работе Интернет, а именно то, что Интернет должен продолжать быть устойчивым и безопасным, его архитектура и развитие стандартов должны оставаться открытыми и децентрализованными, а также доменные имена и числа должны и впредь управляться со знанием дела.

2.1 Определение

Рассмотрение определения управления использованием Интернета началось с некоторых противоречий. В своем обращении к РГУИ Генеральный секретарь МСЭ Ёшио Утсуми (Yoshio Utsumi), выступая в роли Генерального секретаря ВВУИО, выразил желание сузить определение управления использованием Интернета. Он заявил:

> ...Многие из вопросов, которые могли подпадать под более широкое политическое понятие «управления Интернетом», были уже широко обсуждены в ходе первого этапа ВВУИО, и в заключительных документах первого этапа были оговорены согласованные принципы и действия. Существует обширное соглашение между правительствами, как заявлено в Хаммамете, о том, что данные вопросы не должны вновь обсуждаться. Таким образом, нет никакой необходимости, например, обсуждать такие вопросы, как свободная передача информации, противостояние спаму, безопасность сети, региональные корневые серверы, защита конфиденциальной информации или неправильное использование ИКТ. Вместо этого мы должны сосредоточиться на основной деятельности ICANN (Internet Corporation for Assigned Names and Numbers – Международная некоммерческая организация для регулирования вопросов, связанных с доменными именами и IP-адресами) по управлению Интернет-ресурсами, в особенности на доменах верхнего уровня, которые являются более важными вопросами, оставшимися нерешенными.[12]

12 Yoshio, Utsumi, Welcome Speech (First Meeting of the Working Group on Internet Governance Geneva, Switzerland, 23-25 November 2004), http://www.wgig.org/docs/Utsumi.pdf.

Рабочая группа не согласилась с данной узкой точкой зрения и приняла вместо этого более широкое определение управления использованием Интернета:

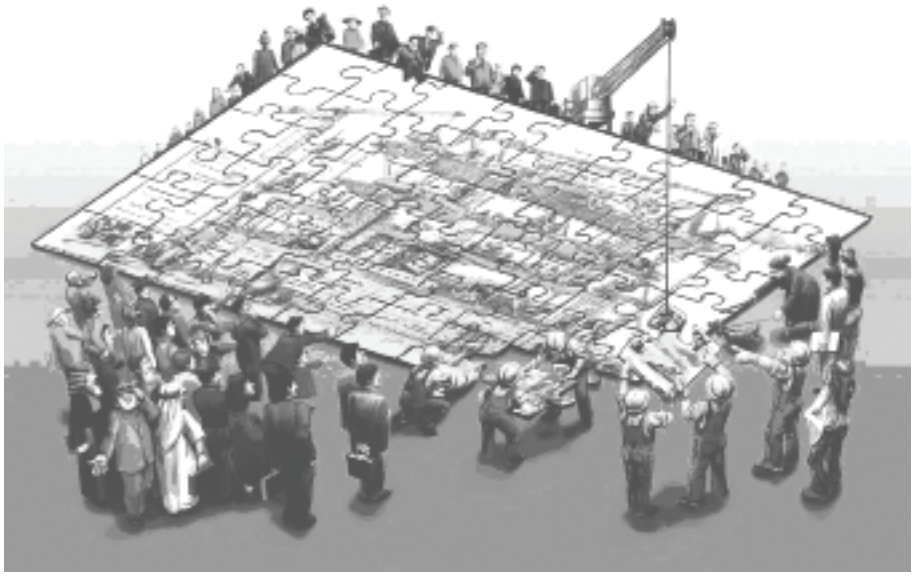
> Управление Интернетом представляет собой разработку и применение правительствами, частным сектором и гражданским обществом, при выполнении ими своей соответствующей роли, общих принципов, норм, правил, процедур принятия решений и программ, регулирующих эволюцию и применение Интернета.[13]

Данное определение было кратким, особенно при сравнении с другими, которые были предложены.[14] В определении присутствуют несколько существенных моментов. Во-первых, было отклонено узкое представление управления использованием Интернета, сводящееся просто к функциям ICANN, которое МСЭ расценило эквивалентным тому, что уже выполняется. Во-вторых, определение охватывает такие важные вопросы государственной политики, как: спам, неприкосновенность частной жизни, киберпреступление, безопасность и развитие Интернета — вопросы, которые не совпадают организационно со структурой МСЭ. В-третьих, определение включило частный сектор и гражданское общество при разработке многостороннего подхода, а МСЭ не могло свободно привлекать их на свои заседания, потому что членами МСЭ были телекоммуникационные компании, которые во многих странах являлись предприятиями, связанными с государством. Это определение также предполагало, что управление использованием Интернета было нечто большим, чем просто законы, принятые правительствами. Оно включало социальные нормы и правила, разработанные Интернет-сообществом. А это дало признание гражданскому обществу, которое сыграло определенную роль в развитии Интернета.

Определение, дополненное утверждениями из Декларации ВВУИО, подразумевало, что процесс управления использованием Интернета должен учитывать мнения всех заинтересованных сторон (включая правительство, частный и государственный секторы), должен быть многосторонним (с участием многих стран), а также прозрачным и демократичным (уважая пожелания большинства). Это подчеркнуло важность процесса в управлении использованием Интернета.

13 WGIG, *Report of the Working Group on Internet Governance* (2005), 4, http://www.wgig.org.
14 WGIG, *Background Report* (2005), http://www.wgig.org.

Рисунок 2. Многостороннее и многосекторальное участие
в управлении использованием Интернета
(Источник: DiploFounation, http://textus.diplomacy.edu/textusbin/env/scripts/Pool/GetBin.asp?IDPool=1188)



2.2 Рекомендации

Рабочая группа также вынесла ряд рекомендаций. Первой был форум для всех заинтересованных сторон для рассмотрения вопросов, связанных с Интернетом. Форум должен был быть недорогой организационной структурой без мандата принятия решений. Его цель заключалась в том, чтобы предоставить возможность заинтересованным сторонам обсудить проблемы и поделиться передовым опытом. Первый Форум по управлению использованием Интернета прошел в Афинах в 2006 году. Второе заседание состоялось в Рио-де-Жанейро, Бразилия. Третья встреча намечена на декабрь 2008 года в Хайдарабаде, Индия.

Вторая рекомендация РГУИ имела отношение к надзору в Интернете. Рабочая группа рекомендовала интернационализацию надзора, основываясь на принципах ВВУИО, согласно которому такой контроль должен быть с участием многих заинтересованных сторон, многосторонним, прозрачным и демократичным. Так как такой надзор не должен вмешиваться в повседневное функционирование Интернета, рабочая группа неявно высказала мнение о том, что американское правительство должно отказаться от своего единственного органа надзора над ICANN.

Несмотря на то, что в докладе РГУИ ICANN расценивается в качестве наиболее транспарентной среди международных учреждений, связанных с Интернетом, были также подняты проблемы, связанные с ICANN. Первая заключается в том, что ICANN не предлагает каких-либо сроков по созданию новых доменов gTLD. Наличие такого расписания полезно для тех, кто предлагает новый gTLD, и для тех, у кого могут быть замечания относительно предложенных gTLD. Во-вторых, было признано, что наименее прозрачной частью ICANN является Правительственный консультативный комитет (Government Advisory Committee) - форум, на котором правительства вносят свои предложения. Однако основные проблемы управления заключаются в том, что,

во-первых, ICANN – это американская компания с контрактом с единственной фирмой-претендентом, а не договором, заключенным на основании тендера в соответствии с передовым опытом. Во-вторых, ICANN находится под контролем Министерства торговли США, закрепленным меморандумом о взаимопонимании, подписанным между ними.

Правительство США привело две причины в пользу их надзора над ICANN: (1) с целью обеспечения стабильности и безопасности Интернета; и (2) недопущение цензуры Интернета другими странами.[15] Обе причины являются спорными. Первая предполагает отсутствие экспертов по обеспечению непрерывного функционирования Интернета за пределами США. Вторая причина идет вразрез с фактической цензурой пространства доменных имен, когда пространство доменного имени XXX, которое было предназначено для использования в порнографических сайтах, было вначале одобрено, а затем отозвано и отклонено. Хотя это решение было принято ICANN, частной компанией, отзыв, по-видимому, был инициирован американской лоббирующей группой и поддержан со стороны правительства США.[16]

Но что будет, если США поведут себя так, как будто им принадлежит Интернет? Можно привести примеры двух аналогичных технологий, где присутствует международная напряженность, обусловленная доминированием США. Первой является глобальная система глобального позиционирования (GPS – global positioning system), контролируемая вооруженными силами и в настоящее время доступная для гражданского применения. Европейцы разработали параллельную систему под названием Galileo с тем, чтобы обеспечить доступность системы навигации в том случае, если США закроют доступ к GPS.[17] Второй технологией, где присутствует доминирование США, является программа по созданию перехватчика Joint Strike Fighter. Общая стоимость программы с участием 10 стран оценивается в более чем 40 млрд. долл. США, вклад каждой страны-партнера составляет более 4 млрд. долл. США. Исходный код компьютерной программы, которая является основным элементом для управления самолетом, находится в руках США. Первоначально существовало сопротивление по совместному использованию исходного кода программы даже с Великобританией, которая внесла 2,5 млрд. долл. США - самый большой вклад среди партнеров. После того, как Великобритания пригрозила выйти из проекта и отменить запланированную покупку 150 самолетов, правительство США подписало соглашение, позволяющее Великобритании сохранять «эксплуатационную независимость» над самолетами.[18]

В целом отметим, что наличие параллельной системы увеличивает стоимость развития обеих систем. В случае с GPS система Galileo обещает быть более точной, чем американская система. В случае программы Joint Strike Fighter отношение США будет источником приостановления сотрудничества по реализации аналогичных программ в будущем.

Третья рекомендация РГУИ состояла в том, что должно быть улучшено международное сотрудничество среди различных организаций и учреждений, участвующих в управлении использованием Интернета. Среди межправительственных организаций – это МСЭ, Всемирная организация по охране интеллектуальной собственности (World Intellectual Property Organization, WIPO) и Организация Объединенных Наций по вопросам образования, науки и культуры ЮНЕСКО (United Nations Educational, Scientific and

15 See, for example, the letter by US Congressman Edward Markey as chairman of the Subcommittee on Telecommunications and the Internet in “Markey, Committee Members Comment on Possible Changes to Internet Watchdog Agency,” Office of Congressman Markey (6 May 2008), http://markey.house.gov/index.php?option=content&task=view&id=3342&Itemid=125.
16 Milton Mueller, “XXX Puzzle Pieces Start to Come Together: And the Picture is Ugly,” *CircleID*, 17 August 2005, http://www.circleid.com/posts/xxx_puzzle_pieces_start_to_come_together_and_the_picture_is_ugly.
17 Directorate-General Energy and Transportation, “Galileo FAQ,” http://ec.europa.eu/dgs/energy_transport/galileo/faq/index_en.htm.
18 “Joint Strike Fighter deal agreed,” *BBC News*, 12 December 2006, http://news.bbc.co.uk/2/hi/uk_news/politics/6173143.stm.

Cultural Organization, UNESCO). Среди Интернет-организаций – это ICANN, Сообщество пользователей Интернет (Internet Society), специальная комиссия в области Интернет-разработок (Internet Engineering Task Force, IETF), Консорциум Всемирной паутины (Worldwide Web Consortium, W3C) и региональные Интернет-регистраторы (Regional Internet Registries, RIRs). Эта рекомендация РГУИ указала на то, что помимо МСЭ существуют много других учреждений, которые участвуют в управлении использованием Интернета. Короче говоря, МСЭ не доказала, что может эксклюзивно претендовать на управление использованием Интернета.

Четвертая рекомендация РГУИ касается региональной и национальной координации политики. Эта рекомендация призывает к установлению более тесных рабочих отношений между страновыми доменами ccTLDs и правительствами, а также к формированию политики, «дружественной для развития Интернета». Также рекомендуется, чтобы правительства сформировали «руководящие комитеты по национальным вопросам управления Интернетом». В частности, данные комитеты должны рассмотреть следующие вопросы:

- Администрирование файлов корневой зоны и системы корневого сервера DNS
- IP-адресация
- Затраты на межсетевые соединения
- Стабильное функционирование Интернет, безопасность сетей и киберпреступность
- Спам
- Свобода выражения мнений
- Реальное участие в разработке глобальной политики
- Защита данных и права на неприкосновенность частной жизни
- Права потребителей
- Многоязычие

Данные вопросы были разбиты на четыре группы следующим образом:

Физическая инфраструктура – в данном кластере обсуждаются темы больше политической направленности, такие как: вопросы, связанные с ICANN относительно IP-адресов, доменных имен и сервера корневой зоны. Также к данной категории можно отнести вопросы финансовых расходов.

Использование и злоупотребления в Интернете - В этом кластере рассматриваются такие вопросы, как: спам, сетевая безопасность и киберпреступность. Решение данных проблем должно увеличить использование Интернета при одновременном сведении к минимуму его неправильного применения.

Вопросы, связанные с Интернетом, но с более широким воздействием - Политика, которая затрагивает Интернет, может также оказывать влияние вне Интернета. Основными областями, где это проявляется очевидным образом, являются политика в области конкуренции, электронная коммерция и права на интеллектуальную собственность.

Аспекты развития Интернета – Принимая во внимание тот факт, что развитие является одной из движущих сил ВВУИО, дискуссии по управлению использованием Интернета, развитию являются темами, кочующими из одной дискуссии в другую. Для содействия в использовании информационных и коммуникационных технологий для развития (ИКТР) был создан Фонд цифровой солидарности (Digital Solidarity Fund). Развитие в этом контексте следует привести в соответствие с Целями Развития Тысячелетия (ЦРТ).

Эти четыре категории вопросов будут рассмотрены в последующих разделах настоящего модуля.

Практическое упражнение

1. Перечислите политики в отношении Интернета, существующие в вашей стране.

2. Кратко изложите, как эти политики в отношении Интернета были разработаны в вашей стране.

Развивающиеся страны сталкиваются с двумя вопросами в отношении управления использованием Интернета: (1) как обеспечить эффективное и конструктивное участие в механизмах управления использованием Интернета; и (2) как создать потенциал для решения этих вопросов.

ВВУИО в Тунисе, рассмотрев доклад РГУИ, оставил механизм управления использованием Интернета приблизительно в той форме, в какой он был с той оговоркой, что национальные правительства имеют исключительную власть над своими ccTLD. Это позволило любому, кто хотел, объявить о победе.

Заключение

Доклад РГУИ является замечательной аннотацией основных вопросов, касающихся управления использованием Интернета. Он также представляет собой модель для организации процесса управления использованием Интернета. Доклад охватывает правительство, частный сектор и гражданское общество в качестве ключевых заинтересованных сторон в управлении использованием Интернета. Процесс работы РГУИ сам по себе оказался образцом открытости и прозрачности. Тем не менее, доклад РГУИ не является ни перспективным планом, ни планом действий.

Проверьте себя

1. Какое определение управления использованием Интернета поддерживается РГУИ. В чем заключается смысл определения?

2. Каковы основные рекомендации РГУИ?

3. Какие основные уроки по управлению использованием Интернета можно извлечь из доклада РГУИ?

3. РАМКИ УПРАВЛЕНИЯ ИНТЕРНЕТОМ 1 – ИСПОЛЬЗОВАНИЕ ИНТЕРНЕТА

Задачей данного раздела является описание различных режимов регулирования Интернета.

Зная проблемы, как можно ввести в обращение правила и нормы в Интернете? Действительно ли возможно регулировать Интернет?

По сути, в определенных пределах можно применить некоторые правила к Интернету для стимулирования его использования и извлечения выгод.

3.1 Режимы регулирования

Существуют четыре режима регулирования, а именно:

- Законодательство - Через государственные и частные санкции и применение силы, в том числе саморегулирования, особенно когда это делегировано правительством.
- Нормы общественного поведения - Через ожидание, поощрение или порицание.
- Рыночные механизмы - Обычно через установление цен и обеспечение доступности.
- Архитектура - Что технология разрешает, предотвращает или запрещает.[19]

Архитектура

Термин «архитектура» относится к разработке технологии таким образом, что определенное поведение либо поощряется, либо не одобряется. Например, для борьбы с превышением скорости можно было бы увеличить количество транспортной полиции на дорогах или же установить на дорогах «лежачие полицейские». В Сингапуре дороги в жилых районах сделаны извилистыми, чтобы замедлить движение транспорта, а также украсить район. Подобным образом производители внедряют различные замки и блокировки, чтобы помешать копированию музыки и видео.

Что касается Интернета, то некоторые люди считают, что сам дизайн Интернета способствует большей свободе выражения мнений. Это означает, что тот, кто захочет регулировать содержание Интернета, обнаружит, что это очень трудно осуществить. В Республике Корея вместо того, чтобы попытаться отследить и поймать хакеров и тех, кто использует бот-сети (botnets) для атак в Интернете, Агентство по безопасности разработало «сети-ловушки» (honeynet), чтобы одурачить направление атак бот-сетей доступом к ложной сети.

Рыночные механизмы

Данный способ регулирования, как правило, имеет дело с процессами ценообразования и доступности товаров и услуг. Правила, которые используют рыночные механизмы в качестве регулирующего инструмента, включают в себя правила честной игры, четкие договорные условия, а также развитие конкуренции на рынке. На базовом уровне – это понятия торговли, покупки и продажи.

19 Lawrence Lessig, *Code 2.0* (New York: Basic Books, 2007).

Торговля конфиденциальной информацией в Интернете, например, путем предоставления кого-либо адреса электронной почты в обмен на право знакомиться или получать какое-либо информационное содержание, является примером использования рыночного механизма в качестве одной из форм регулирования. Идея состоит в том, что если кто-то оценивает свою частную жизнь больше, чем право знакомиться или получать какой-либо контент, тогда данное лицо никогда не предоставит адрес электронной почты. В США частные компании, такие как Trust-e, появились для предоставления пользователям защиты частной информации. В Европейском союзе (ЕС) наоборот полагают, что неприкосновенность частной жизни должна регулироваться не частным соглашением между физическим лицом и компанией, а в соответствии с законом.

Нормы общественного поведения

Использование общественных норм в качестве механизма регулирования предполагает, что давление со стороны общества может диктовать поведение человека. Сетевой этикет, или этикет пребывания в «сети», является примером использования социальных норм в качестве регулирующего механизма. Сетевой этикет требует, среди прочего, того, что сообщения, публикуемые на форуме, должны быть по существу или относиться к теме обсуждения, и, если кто-то ответил «пожалуйста» на ваше «спасибо», нет никакой необходимости в дальнейших ответных действиях.

Использование норм общественного поведения облегчается, когда это происходит в социальной группе, потому что тогда группа выступает в качестве надзорного и исполнительного органа. Те, кто нарушает нормы, могут быть исключены из социальной группы. Такая санкция может быть действенной, когда членство в социальной группе считается важным.

Законы, в том числе саморегулирование

Законы являются проявлением политики и принимаются парламентом или Национальным собранием. В целом, следует проявлять осторожность по поводу принятия законов в быстро меняющихся условиях, таких как технологии. Здесь существует неудобство первопроходца. Например, Закон о цифровой подписи штата Юта, который был первым подобным законом в мире, вскоре устарел, потому что появились новые технологии, вследствие которых технологично-ориентированный подход перестал работать. Сингапур и США, принявшие первые законы по иммунизации операторов сети (в случае Сингапура) и других посредников (в случае США), вскоре обнаружили, что другие страны приняли свои законы и усовершенствовали их возможными превосходящими путями.

Пожалуй, лучший совет заключается в том, что законы должны отставать, а не опережать технологии, и что следует всегда применять многосторонний подход с широкими консультациями прежде, чем принимать законы. Необходимо иметь в виду, что Интернет все еще находится на относительно ранней стадии развития.

Саморегулирование

В Интернет-индустрии, как правило, понятие саморегулирования рассматривается в качестве одного из способов обеспечения большей гибкости в принятии и обеспечении соблюдения законов. Первоначально саморегулирование означало регулирование индустрии отраслью, а не физическое лицо или компанию, регулирующих себя непосредственно. На практике саморегулирование часто представляло собой делегирование полномочий с окончательной властью санкционирования, все еще находящейся в руках правительства. Это означает, что правительство позволило отрасли взять на себя инициативу в регулировании рассматриваемого сектора.

Реклама представляет собой область, где правительства, особенно в развитых странах, склоняются к использованию саморегулирования. Правительство может подать судебный иск против злостных правонарушителей, игнорирующих решения отрасли, за вводящую в заблуждение или оскорбляющую рекламу.

Однако саморегулирование нуждается в мотивированном частном секторе. Это, кажется, работает в рекламной индустрии, так как использование государственного вмешательства для одобрения рекламы будет замедлять данный стремительно изменяющийся сектор и, весьма вероятно, задушит креативность. Интернет-индустрия менее расположена к саморегулированию. Некоторые в этой отрасли даже жаловались, что саморегулирование означает, что отрасль выполняет работу правительства.

Вопросы для размышления

В какой мере применяются четыре режима регулирования в вашей стране? Какой из видов регулирования не будет хорошо работать в вашей стране, и почему? Какой режим или режимы будут работать лучше и почему?

3.2 Предлагаемая «дорожная карта»

Поскольку определение управления использованием Интернета является широким по своему охвату, предлагается следующее в качестве «дорожной карты» для разработки рамочной политической структуры. «Дорожная карта» охватывает ряд вопросов и указывает контрольные точки хода планирования так, чтобы каждый видел ориентир для определения эффективности разрабатываемых правил и политики. «Дорожная карта» является надежной в том смысле, что она прошла «проверку» на реальных событиях.[20]

Когда в 1996 году был разработана «дорожная карта», многие страны даже не имели элементарных правил по работе с электронными уликами. Сегодня найдется не так много стран, не имеющих базовых правил. Тем не менее, данная рамочная структура по-прежнему применяется, поскольку ведет к совершенствованию правил и политики, связанных с Интернетом.

Вопросы приводятся примерно в убывающем порядке по критерию важности, на которые следует обратить внимание:

1. Предоставление доступа и сервиса
2. Электронная коммерция
3. Регулирование контента
4. Безопасность
5. Права интеллектуальной собственности
6. Конфиденциальность

Важно, в первую очередь, обратиться к решению вопросов доступа и стоимости, потому что именно это позволит сделать Интернет более доступным. В свою очередь, наличие доступа породит множество вопросов, связанных с приведением в соответствие сетевого мира к реальному миру. Например, если кто-то совершает банковское

20 See Ang (2005) for a fuller discussion.

мошенничество, используя Интернет, являются ли нормы доказательного права применимыми так, чтобы человек мог быть привлечен к ответственности на основании доказательств, собранных в сети? Существует коммерческий стимул для решения этих основных вопросов в согласовании законов реального мира с миром онлайн. Вопросы по регулированию контента и безопасности будут возникать из-за напряженности между тем, что доступно и может быть сделано в Интернете, по сравнению с тем, что доступно и может быть сделано в офлайновом мире. Многие страны уже отказались от регулирования контента в Интернете, за исключением случаев защиты детей младше 12 лет. Существует определенная срочность в разрешении регулирования контента и вопросов безопасности, поскольку есть потенциальные пользователи, которые избегают Интернета, так как они не хотят, например, чтобы порнография была доступна дома или их компьютер мог быть взломан хакерами. Права на интеллектуальную собственность и защита частной жизни получают все большее значение, поскольку использование Интернета становится более широко распространенным.

Предоставление доступа и сервиса

Вопросы, которые должны быть рассмотрены под данным заголовком, связаны с обеспечением доступа к Интернету, приемлемого в ценовом отношении. Данные вопросы формулируются следующим образом:

- Как управлять техническими стандартами в сетевой среде.
- Как обеспечить взаимодействие и совместимость компьютерных систем и сетей.
- Каким образом можно регулировать цены и качество информационных услуг.
- Уточнение обязанностей и ответственности поставщиков услуг и сетевого доступа, таких как: защита поставщиков услуг и сетевого доступа от ответственности за содержание третьей стороны.

Вопрос иммунитета имеет важное значение, поскольку без него электронная коммерция может быть задушена.

Вопросы для размышления

Во многих странах закон о диффамации (клевете) означает, что любой, кто нанесет вред другому человеку на основе ложных показаний, должен будет компенсировать потерпевшему лицу. В некоторых странах размер компенсации может зависеть от того, было ли ложное утверждение сделано умышленно или нет. В других странах не имеет значения, было ли ложное утверждение сделано по незнанию. Насколько телерантны законы в вашей стране к ошибочным заявлениям, сделанным на (а) сайте книжного обозрения, (б) сайте обзора гостиниц, а также (в) на аукционном сайте? Будет ли поставщик Интернет-услуг в вашей стране нести ответственность за передачу ошибочных утверждений?

Электронная коммерция

С коммерческой точки зрения электронная коммерция имеет много преимуществ. Фирма, начинающая бизнес в электронной коммерции, открывает круглосуточный магазин, где устраняется посредник и открываются новые рынки сбыта. Электронная коммерция может сделать бизнес более эффективным, поскольку она позволяет автоматизировать бизнес.

Однако электронная коммерция подходит не для всех типов бизнеса. Электронная коммерция не может обеспечить работу предприятий, которые продают дорогие предметы, такие как мебель, поскольку клиенты, прежде чем покупать их, как правило, хотят проверить эти вещи. Кроме того, в некоторых культурах посещение магазина является видом проведения досуга, который может отнять электронная коммерция.

Имеет смысл попытаться решить вопросы организации электронной коммерции, потому что от них зависят решения целого ряда проблем, которые являются препятствиями на пути более широкого использования Интернета. Необходимо рассмотреть следующие вопросы:

- Юридическое признание электронной среды
- Признание электронных свидетельств
- Признание электронных транзакций
- Признание цифровой подписи и цифровых сертификатов
- Уточнение прав, обязанностей и ответственности различных сторон, а также механизмы урегулирования споров
- Поощрение электронных платежных механизмов и их использование
- Предоставление полномочий полиции на обеспечение соблюдения законов в области электронной коммерции
- Уточнение налогообложения в области электронной коммерции

Вероятно, будет необходимо принять законодательный акт в направлении разработки так называемого закона по электронной коммерции или электронных сделок (транзакций). Такой закон подготовит условия для электронной коммерции.

Признание электронных свидетельств

Во многих странах признание электронного доказательства в его различных формах стало необходимым в связи с широкой публичной доступностью Интернета с середины 1990-ых годов. Например, нормы доказательного права необходимо было усовершенствовать, когда были изобретены цифровые подписи. В 1996 году в Сингапуре были внесены изменения в закон об электронных сделках. В Индии были внесены поправки в Акт об информационных технологиях от 2000 года. Короче говоря, новые законы, обновляющие офлайновый мир для соответствия с миром онлайн, имеют достаточно недавнее происхождение.

Практическое упражнение

Опишите правила для усиления или способствования развития электронной коммерции в вашей стране. Если нет таких правил, перечислите, какие соответствующие правила, на ваш взгляд, могли бы способствовать развитию или распространению электронной коммерции в вашей стране.

Регулирование контента

Некоторые пользователи ссылаются на нежелательный контент в качестве основания для того, чтобы не подключаться к Интернету. Однако критерии нежелательного носят индивидуальный характер. Поэтому решение этого вопроса требует балансирования конкурирующих интересов. Главным достоинством отсутствия любой фильтрации является неограниченная доступность контента. Иногда фильтры усердствуют в «блокировании» настолько, что даже блокируется безобидное содержание.

Необходимо обратить внимание на решение следующих вопросов по регулированию контента:

- Как блокировать нежелательный материал в Интернете, главным образом, в интересах детей.
- Как защитить национальные интересы от нежелательных зарубежных материалов.
- Каким образом можно примирить конфликтующие культурные ценности в информационном содержании.

Незаконный контент: глобальная координация

Из-за культурных различий трудно достигнуть универсального соглашения в отношении того, что является неприемлемым. Однако существует более общее соглашение по поводу того, что является незаконным, что, как правило, наносит ущерб. Сразу приходит на ум детская порнография.

Глобальная координация со стороны правоохранительных органов действует при проверке распространения детской порнографии. Правоохранительные органы сотрудничали для проведения периодических зачисток. Совсем недавно, в конце 1990-ых годов, большая часть изображений детской порнографии была отсканирована из офлайнового мира. Но с развитием Интернета появились изображения реального надругательства над детьми, переданные через веб-камеру. Чтобы прекратить такие злоупотребления, полицейские агентства вычисляют тех, кто загружает изображения жестокого обращения над детьми. В 1998 (операция «Кафедральный собор») и 1999 (операция «Руда») годах были осуществлены серии скоординированных кампаний, которые привели к сотням арестов во многих странах.

Для получения дополнительной информации см. WGIG, Background Report (2005), 34 (paragraph 141), http://www.wgig.org.

Безопасность

Данная тема приобрела большое значение, так как Интернет-черви, вирусы и троянские программы становятся все более изощренными.

Вирус «ILoveYou»

Наиболее разрушительный из когда-либо созданных компьютерный вирус распространился настолько быстро, что такие учреждения, как Пентагон, Центральное разведывательное управление и парламент Великобритании вынуждены были закрыть свои системы электронной почты, чтобы избавиться от него. Вирус распространялся быстро, потому что он воспроизводил себя на адреса электронной почты пользователей, которые были сохранены в адресной книжке Microsoft Outlook. Поскольку электронные письма приходили от знакомых, пользователи, не задумываясь, открывали сообщения и распространяли вирус.

Несмотря на огромные расходы по удалению вируса в компьютерных системах во всем мире, автор вируса остался безнаказанным даже при том, что он был опознан. В мае 2000 года, когда вирус был запущен, на Филиппинах, где жил автор вируса, не было никакого закона, запрещающего распространение вредоносных программ. В июне 2000 года был принят закон об электронной коммерции Филиппин, который до этого был на стадии разработки. Он включает в себя положения, устанавливающие уголовную ответственность за распространение компьютерных вирусов.

Источник: Peng Hwa Ang, “Policing Asia’s Internet,” *Asian Wall Street Journal*, 7 September 2000, 8.

По сути, вопросами безопасности являются:

- Как защититься от нарушения безопасности компьютерных систем и сетей.
- Как предотвратить преступления в цифровой среде.

В модуле 6 из серии модулей ИКТ Академии для лидеров государственного управления рассматриваются вопросы обеспечения сетевой и информационной безопасности и неприкосновенности частной жизни.

Права интеллектуальной собственности

Цифровой мир позволяет сделать идеальные копии оригинала. В отличие от аналоговой мира здесь отсутствуют потери качества. Тем не менее, легкость, с которой можно сделать отличные копии, означает, что также легко можно нарушить права на интеллектуальную собственность.

Поэтому современной системе прав на интеллектуальную собственность следует рассмотреть следующие вопросы:

- Как дополнить текущую систему авторских прав, включив в нее цифровые работы.
- Как получать, защищать и управлять правами в цифровой среде.
- Как предотвратить пиратство работ, защищенных авторским правом.

Нелицензированное использование музыки

Музыка, вероятно, является наиболее подверженной пиратскому использованию в глобальном масштабе. В то время как продажи iPod и других музыкальных проигрывателей продолжали расти, продажи музыкальных компакт-дисков уменьшались на протяжении нескольких лет. Широко распространенный обмен и загрузка песен через пиринговые программы подпитывают пиратство.

Несмотря на широко распространенное заблуждение, те, кто распространяет песни в онлайне, могут быть отслежены и преследоваться по закону. Заблуждение, вероятно, возникло потому, что с помощью пиринговых программ, таких как BitTorrent (БитТоррент) и LimeWire, пользователи загружают песни от других лиц. Пользователи, похоже, забыли, что из-за масштабности один человек может передать песню многим другим по типу распространения вирусов.

Владельцы музыки сопротивлялись, причем наиболее агрессивно вела себя Ассоциации звукозаписывающей индустрии США (Recording Industry Association of America, RIAA). RIAA преследовала в судебном порядке студентов, зная, что они финансово несостоятельны, для того, чтобы подать пример другим. По некоторым данным RIAA даже побуждал студентов бросить школу и работать, чтобы оплатить урегулирование исков.

Практическое упражнение

Какие законы и другие меры по защите авторского права существуют в вашей стране. Оцените, насколько эффективны они в цифровой среде (то есть, в свете развития цифровых технологий).

Неприкосновенность частной жизни

Самым строгим режимом неприкосновенности частной жизни является Директива ЕС о защите данных, которая требует, чтобы у третьих сторон был «адекватный уровень» защиты данных прежде, чем они смогут обрабатывать данные из стран ЕС. Но его выполнение было отсрочено нежеланием правительства США иметь аналогичный режим. США предложили творческую альтернативу - условие «безопасной гавани», в котором те, кто выполняет Директиву, будут рассматриваться как участники безопасной гавани и будут считаться соответствующими данной Директиве.

Организация экономического сотрудничества и развития (ОЭСР) также разработала руководящие принципы неприкосновенности частной жизни, которые пытаются установить менее требовательный взгляд на неприкосновенность частной жизни по сравнению с позицией ЕС о конфиденциальности.[21]

21 OECD. “OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data,” http://www.oecd.org/document/18/0,2340,es_2649_34255_1815186_1_1_1_1,00.html.

Основной вопрос в правилах по конфиденциальности заключается в том, чтобы регулировать использование личной информации со стороны государственных и частных учреждений.

Соответствие стандарту ЕС

Позиция ЕС о неприкосновенности частной жизни хорошо продумана. Частью ее нового подхода является требование о том, что данные из стран ЕС не могут быть переданы в другую страну для обработки, если у той страны нет того же самого уровня защиты данных, как в ЕС. На практике существуют исключения, как, например, для полетов самолета. Но политика ЕС вынуждает многие страны обновить свои законы о защите данных в целях соответствия стандарту ЕС.

Нет никакого сомнения, что стандарт ЕС налагает некоторые бизнес-затраты. Поэтому понятно, что бизнес-ассоциации пытаются соответствовать минимальным требованиям стандарта, где это возможно.

У США имеется положение о безопасной гавани, о которых частично договорилось правительство США, хотя внешне это было сделано со стороны частного сектора. Американское положение безопасной гавани означает, что те компании, стандарты защиты данных которых соответствуют саморегулирующим стандартам безопасной гавани, будут иметь возможность получать и обрабатывать данные из стран ЕС.

В Австралии правительство попыталось обновить свои законы о неприкосновенности частной жизни, чтобы привести их к уровню, «адекватному» для ЕС. Тем не менее, по-видимому, из-за лоббирования со стороны деловых кругов положения были размыты, и некоторые меры безопасности отсутствуют.

Существует, следовательно, равновесие между интересами бизнеса и стандартом ЕС по защите частной жизни.

Веб-страница Европейской комиссии по защите данных http://ec.europa.eu/justice_home/fsj/privacy/index_en.htm содержит ссылки на ресурсы и дополнительную информацию по неприкосновенности частной жизни.

Заключение

Подходы к решению вопросов, имеющих отношение к Интернету и изложенных выше, основаны на международных нормах, так как Интернет является международным по своему охвату, и ни одна страна не может быть изолирована от остальной части международного сообщества. Кроме того, необходимо провести широкие консультации с заинтересованными сторонами, представляющими, например, индустрию и гражданское общество, как для просвещения общин, так и для того, чтобы быть информированными о проблемах.

Практическое упражнение

Как вы думаете, является ли классификация шести категорий вопросов, описанных выше, целесообразной в контексте вашей страны. Если вы считаете, что данное ранжирование не подходит для вашей страны, предложите, как эти категории вопросов должны быть расставлены в зависимости от степени важности в вашей стране. Обоснуйте свое предложение.

Проверьте себя

1. Какие существуют четыре способа регулирования Интернета? Каковы их ограничения в отношении регулирования Интернета?

2. Предложенная «дорожная карта» по регулированию Интернет является лишь предлагаемым руководством. Предложите практические меры для осуществления данной «дорожной карты»?

4. РАМКИ УПРАВЛЕНИЯ ИНТЕРНЕТОМ 2 – ЗЛОУПОТРЕБЛЕНИЯ В ИНТЕРНЕТЕ

Задачей данного раздела является повышение осведомленности о наиболее распространенных нарушениях прав в Интернете и мерах, которые могут быть предприняты для их решения.

4.1 Что особенного в Интернете

Некоторые считают, что Интернет является простым отражением офлайнового мира и поэтому не нужно придумывать специальных правил для него. Тем не менее, при этом упускаются несколько характерных особенностей Интернета.

Во-первых, в Интернете легко быть анонимным. Безусловно, сотрудники правоохранительных органов могут отследить пользователей. Но для этого требуются особые усилия и ресурсы. Сила анонимности заключается в том, что она предоставляет возможность открытого и откровенного общения на такие темы, как медицинские заболевания. Вместе с тем, анонимность также может служить прикрытием для преступников.

Во-вторых, в Интернете есть культура анархии и беззакония, которая, вероятно, лучше всего проиллюстрирована в «Декларации независимости киберпространства» Джона Перри Барлоу:

> Правительства промышленно развитых стран, вы изнуренные гиганты плоти и стали, я пришел из киберпространства, нового пристанища Разума. От имени будущего я прошу, чтобы вы из прошлого оставили нас в покое. Вы не приветствуетесь среди нас. У вас нет суверенитета там, где мы собираемся.[22]

Конечно, данное заявление было безнадежно нереалистичным «воздушным замком», что свидетельствует о непонимании законов: законы не регулируют места, а регулируют их обитателей. До тех пор, пока есть люди, всегда будет существовать потребность в законах, обстоятельно разъясняющих права и действующих в качестве социальной смазки для минимизации трения между людьми.

В-третьих, как мы начали понимать, Интернет является мощным инструментом для налаживания связей. Этот потенциал, который лучше всего представляют вебсайты «социальных сетей», таких как MySpace и FaceBook, теперь известен в качестве Web 2.0. В Web 2.0 прежде группы маленьких ниш получили возможность собираться и формировать крупные глобальные сообщества. Одним из примеров является barefooters.org, участники которого ходят босиком, за исключением формальных случаев. В 1999 году их было только 400 человек по всему миру. К 2007 году их уже насчитывалось около 2 000, живущих в нескольких странах. На глобальном уровне они признаются достаточно большой группой, чтобы иметь свой собственный логотип.

22 John Perry Barlow, “A Declaration of the Independence of Cyberspace” (8 February 1996), http://homes.eff.org/~barlow/Declaration-Final.html.

Аналогичным образом Интернет предоставляет возможность злоумышленникам собраться и создать проблемы, о чем говорится далее.

4.2 Злоупотребления в Интернете

Детская порнография

Первоначально детская порнография состояла из содержания, преобразованного из печатной версии в цифровую копию. Но в связи с развитием технологий стало возможным иметь порнографию по запросу, где детская порнография также готовится по запросу.[23]

Необходимо было международное сотрудничество для пресечения этих объединений преступников. Интерполом были проведены рейды одновременно в нескольких странах, а также произведен обмен информацией в рамках операций «Кафедральный собор» (Cathedral) в 1999 году и «Руда» (Ore) в 2002 году.[24] Международное сотрудничество стало возможным, потому что детская порнография является одной из немногих областей, где присутствует почти всеобщее согласие о том, что это преступное деяние.

Обман потребителей

Интернет показал, что иногда законы офлайнового мира необходимо изменить, чтобы справиться с вызовами новой экономики. Один из примеров - законы по проведению аукционов. Во многих странах Британского Содружества на аукционе требуется физическое присутствие кого-то с лицензией, дающей право на проведение аукционов. На первый взгляд, такой закон кажется старомодным. Это означало бы, например, что аукционисты eBay должны быть проверены на предмет наличия у них лицензий. Однако, как только был принят закон, разрешающий электронные аукционы, очень быстро стало ясным логическое обоснование для закона: аукционное мошенничество стало наиболее частой разновидностью онлайнового мошенничества.[25]

Обман потребителей является еще одной областью, где существует почти всеобщее согласие о том, что с этим надо бороться. Борьба с такого рода мошенничеством будет способствовать увеличению применения Интернета. С 1996 года проводятся ежегодные зачистки Интернета от мошенничеств по обману потребителей. Число стран, вовлеченных в зачистку, постоянно растет.

23 Ethel Quayle and Max Taylor, *Child Pornography: An Internet Crime* (New York: Brunner-Routledge, 2003).
24 See Ang (2005).
25 See Ang (2005).

Ежегодные потребительские зачистки

Почти 40 стран объединились для решения проблемы обмана потребителей в сети под эгидой Международной правоохранительной сети по защите потребителей (International Consumer Protection and Enforcement Network, ICPEN). Данная сеть проводит ежегодный Международный день зачистки Интернета по устранению вебсайтов, которые вводят в заблуждения потребителей. В частности, зачистки нацелены на борьбу с онлайн-аферами и мошенничеством.

Следует отметить, что такие онлайновые зачистки работают только в том случае, если присутствуют эффективные офлайновые законы, предлагающие защиту потребителей. Поэтому более развитые страны являются более активными в таких зачистках.

С более подробной информацией об ICPEN и ее деятельности можно ознакомиться на веб-сайте http://www.icpen.org.

Вопросы для размышления

Насколько эффективным является законодательство в отношении детской порнографии и обмана потребителей в вашей стране?

Спам, мошенничество, вредоносные программы, фишинг

Спам или незапрашиваемая масса коммерческой электронной рассылки является проблемой, которая постепенно получает возрастающую политическую и коммерческую поддержку. Это объясняется тем, что спам тратит впустую полосу пропускания трафика. Еще важнее то, что он может представлять собой значительную угрозу для безопасности, поскольку спам в наши дни может содержать вредоносные программы, что дает возможность осуществления фишинга, который является «преступно-мошенническим процессом, который пытается получить конфиденциальную информацию, такую как имена пользователей, пароли и детали кредитной карты, маскируясь под заслуживающее доверие юридическое лицо в процессе электронного обмена информацией».[26]

Из-за своего университетского происхождения Интернет начал свое развитие на основе открытой и доверчивой культуры. В первые годы, когда пользователи (которые часто являлись студентами американских университетов) отправляли сообщения по электронной почте, многие оставляли свои телефонные номера после подписи, которая была признаком правдивости того, что они только что отправили. Сегодня, с массовой доступностью Интернета, телефонный номер в сообщении электронной почты привлек бы все возможные способы атак.

Возможно, что первый спам направил маркетинговый представитель корпорации Digital Equipment Corporation (DEC), выпустившей миникомпьютеры для Интернета. Это было коммерческое сообщение, рекламирующее представление продукта. Пользователи пожаловались и, в отличие от сегодняшних дней, когда спамера не так легко проследить, были приняты меры против спамера.[27]

26 Wikipedia, “Phishing,” Wikimedia Foundation, Inc., http://en.wikipedia.org/wiki/Phishing.
27 Brad Templeton, “Reaction to the DEC Spam of 1978,” http://www.templetons.com/brad/spamreact.html.

Несмотря на то, что наиболее широко признанным видом спама сегодня является рассылка спама через электронную почту, данный термин применяется для аналогичных нарушений в других средствах передачи данных по Интернету, таких как: мгновенный обмен сообщениями, телеконференция Usenet, поисковые системы, блоги, вики, передача сообщений по мобильному телефону и игры. На международном уровне спамом через электронную почту называется «незапрашиваемая массовая электронная рассылка»: электронная почта является частью более крупной коллекции по существу идентичных электронных писем, на рассылку которых получатели не соглашались. Поэтому спам представляет собой вопрос согласия, а не содержания.[28] Это означает, что законодательство в отношении спама должно рассматривать согласие, а не содержание.

Спам, спам – когда он закончится

Первым законом, нацеленным на борьбу со спамом, стал американский акт CAN-SPAM от 2003 года. Его полное название: Закон о контроле нападения незапрашиваемыми материалами порнографического и рекламного характера (Controlling the Assault of Non-Solicited Pornography and Marketing Act). Закон наделяет правом подавать судебные иски со стороны частных лиц, и использовался для судебного преследования известных операторов спама в США. Оценка эффективности закона проводилась в 2005 году, и в него не было внесено каких-либо существенных изменений. Тем не менее, уровень спама в США таков, что страна занимает первое или второе место в мире по спаму. Китай и Республика Корея также занимают лидирующие позиции.

Создается впечатление, что спам процветает там, где существует большой уровень проникновения Интернета, как в случае Республики Корея, и там, где законы и правоприменение слабые, как в Китае.

Коалиция деловых и регулирующих кругов занимаются спамом в рамках Лондонского плана действий (http://www.londonactionplan.org), а также Альянса по прекращению спама (http://stopspamalliance.org). На их соответствующих сайтах можно найти более подробную информацию о спаме, а также последнюю информацию о передовом опыте и деятельности.

Киберзапугивание, киберпреследование, кража личных данных, Интернет-зависимость

Вред в этой группе является следствием работы в сети. Так, вероятность возникновения данных угроз тем выше, чем больше времени пользователь проводит в Интернете. Киберзапугивание представляет собой преследование несовершеннолетнего другим несовершеннолетним с использованием Интернета и других электронных средств коммуникации. Зачастую это связано с передачей унизительных и оскорбительных сообщений. Если преследование осуществляется взрослым, то это кибер-домогательство.

Киберпреследованием является использование Интернета и других электронных средств коммуникации для преследования жертвы. Это часто вытекает из офлайнового преследования, но это может также быть прелюдией к офлайновому преследованию. Некоторые жертвы были убиты их киберпреследователями (кибersталкерами).

28 Spamhaus, “The Definition of Spam,” http://www.spamhaus.org/definition.html.

Хищение персональных данных предполагает использование личных данных для получения выгоды или во избежание некоторых обязательств. Распространенные примеры включают в себя использование персональной информации жертвы для получения кредитной карты.

Эти мошенничества могут нанести серьезный вред, как и в случае кибersталкера, убившего женщину, которую он преследовал. Решение заключается в принятии законов для борьбы с такими явлениями.

В случае интернет-зависимости, которая заключается в чрезмерном увлечении Интернетом в ущерб школе или офисной работе, в Республике Корея организованы новые консультативные службы для решения данных проблем.

Решение проблемы Интернет-зависимости

Отметим, что Интернет-зависимость постоянно растет как компульсивное расстройство, подобно маниакальному увлечению азартными играми. Пристрастившиеся люди могут потратить 17-18 часов в Интернете. К странам, в которых насчитывается наибольшее количестве Интернет-наркоманов, относятся Китай, Япония, Республика Корея и Тайвань. Эти многочисленные случаи Интернет-зависимости в Азии поднимают вопрос о степени воздействия культурных факторов на подобное компульсивное поведение. Проводится много исследований для определения того, является ли это расстройство проявлением других компульсивных расстройств.

Ссылка в Википедии по теме «Расстройство Интернет-зависимость» (http://en.wikipedia.org/wiki/Internet_addiction_disorder), где приведен довольно сбалансированный отчет аргументов за и против признания такого явления истинным расстройством.

Практическое упражнение

Проведите быструю неофициальную оценку уровня понимания спама, мошенничества, фишинга, киберзапугивания, киберпреследования, кражи личных данных и Интернет-зависимости в вашей организации, правительстве и обществе в целом. Приведите доказательства или обоснуйте свою оценку.

Политическая воля

Борьба против такого рода негативного использования Интернета требует политической воли. Во-первых, рассматриваемые деяния должны быть незаконными в стране. В некоторых странах законодательство о защите потребителей настолько слабо, что их приведение в исполнение невозможно или неэффективно. Во-вторых, должна быть политическая воля к сотрудничеству на международном уровне. Например, нигерийское мошенничество 419 по-прежнему продолжается из-за практически несуществующего исполнения законов со стороны нигерийского правительства. Результатом этого является низкий уровень доверия к нигерийской электронной коммерции.

Предоплата или нигерийское мошенничество 419

Достойно сожаления то, что Нигерия, которая лидирует по показателям глобальных индексов коррупции, ассоциируется с общим онлайн-мошенничеством, названным в честь постановления в их уголовном кодексе в отношении получения собственности под фальшивыми предлогами. Нигерийское мошенничество 419 является мошенничеством на основе предоплаты, где жертву побуждают послать деньги в надежде на получение возврата большей суммы денег.

Типичное электронное сообщение жертве приходит от кого-то, кто нуждается в помощи для получения доступа к финансовым средствам. Финансовыми средствами предположительно могут выступать наследство ребенка свергнутого правителя, неактивный счет в банке или даже некоторые суммы взяток. Любого, кто проглотит наживку, попросят послать еще и еще денег, чтобы решить некие непредвиденные трудности.

Из-за вовлеченных денежных сумм эти операции часто профессионально организуются при попустительстве государственных должностных лиц. Некоторые из тех, кто отправился в Нигерию для расследования, пропали без вести или были убиты.

Ссылка в Википедии на тему «Мошенничество по предолате» (http://en.wikipedia.org/wiki/Advance_fee_fraud) приводит историю жульничества, а также подробности его вариантов. Вебсайт американской компании в области электроники (http://home.rica.net/alphae/419coal/) предоставляет консультации по вопросам, что делать, если кто-то получит такое сообщение мошенников.

4.3 Санкции

Любое обсуждение вопросов управления должно коснуться вопроса исполнения законов. Без исполнения законов, в лучшем случае, правила рассматриваются в качестве идеального примера; в худшем случае, их рассматривают с цинизмом, как законы, которые можно попирать. Данный раздел описывает то, как можно применить санкции, чтобы привести в жизнь согласованные нормы, имеющие отношение к Интернету.

Нормы киберсообщества: сетевой этикет и санкции, применяемые сообществом

У киберсообществ могут быть свои собственные традиции сетевого этикета, нормы и правила поведения. В таких случаях наиболее тяжелой формой санкций, администрируемых сообществом, будет социальная изоляция и изгнание. Такое случилось в известном примере с «удалением» (“toading”) г-на Бангл (Bungle), который совершил насилие в онлайне против двух игроков в игре. Он был изолирован и, в конечном итоге, ему пришлось покинуть игру.[29]

29 Julian Dibbell, “A Rape In Cyberspace,” *The Village Voice*, 23 December 1993, http://www.juliandibbell.com/texts/bungle_vv.html.

Насилие в киберпространстве

Онлайн-сообщества существовали до появления Интернета. Сообщества были меньшими по численности, и обмен данными проходил на основе текста. Это имело место также и во многопользовательских онлайн-играх, которые могут расцениваться как предшественники современных многопользовательских игр, таких как «World of Warcraft». В одной из таких игр, LambdaMOO, игрок по имени г-н Бангл использовал программу, которая позволила ему сделать так, как будто текст был от другого игрока. Среди действий, которые описал г-н Бангл, были половые акты между аватаром, которым он управлял, и другим аватаром, который появлялся по его желанию. Действия нарушили нормы сообщества и продолжались в течение многих часов.

Несколько дней спустя пользователи LambdaMOO встретились в онлайне, чтобы обсудить меры, которые будут направлены против г-на Бангла. После встречи один из основных программистов сообщества в одностороннем порядке решил отключить учетную запись г-на Бангла. С тех пор пользователи LambdoMOO установили программу временного удаления пользователя, нарушившего правила их сообщества.

Тем не менее, такие санкции сообщества редки, потому что часто бывает трудно прийти к соглашению о том, что действие является неправильным, и к соглашению о степени «неправильности» и мере наказания. Кроме того, возможно, санкции социальной изоляции не могут быть достаточно серьезными для некоторых людей. Короче говоря, санкции сообщества работают, но в ограниченной форме.

Самопомощь

В некоторых случаях потерпевшая сторона может прибегнуть к самопомощи. Например, у владельцев авторского права есть история использования самопомощи в преследовании в судебном порядке тех, кто посягал на их авторское право, и на самом деле очень часто система соблюдения правопорядка осуществляется именно таким образом. Это означает, что значительная часть работы по расследованию и обеспечению соблюдения правовых действий предпринята непосредственно владельцами авторского права, а не полицией, даже при том, что законы авторского права относятся к уголовным деяниям.

В 2000 году в Сиднее Олимпийский комитет нанял частную компанию под названием «Copyright Control Services» («Служба контроля по вопросам авторского права») для «патрулирования» в Интернете по обнаружению сайтов, несанкционированно распространяющих новости об Олимпийских играх. Причина состоит в том, что права на трансляцию результатов были проданы на торгах за 200 млн. долл. США, и любые несанкционированные утечки информации подрывали бы права победившего покупателя. Приблизительно 60 лицам, которые «патрулировали» Интернет, удалось остановить крупномасштабное несанкционированное вещание. Российская телевизионная станция, Москва TV6, действительно пыталась привести доводы в пользу свободы выражения, когда начала транслировать видео в интернет. Но московский канал TV6 должен был прекратить несанкционированную трансляцию, потому что было поставлено условие, что, если они продолжат вещание, подача видеосигнала к телестанции будет остановлена.[30] С тех пор организуются подобные патрульные команды и для летних и для зимних Олимпийских игр.

30 "Violators caught as Olympic video monitored on Internet," *CNN*, 22 September 2000, http://edition.cnn.com/2000/TECH/computing/09/22/olympics.netpolice.ap/index.html.

Был разговор о разработке международного права, позволявшего расследование и судебное преследование киберпреступлений. В сущности, такой закон создал бы единый кодекс для определения, преследования по суду и соблюдения правил против киберпреступлений. Существует международное сотрудничество, но в нем принимают участие немногие страны.

Конвенция Совета Европы о киберпреступности представляет собой региональную попытку реализации такого кодекса. Поскольку Европа достаточно разнообразна, Конвенция может иметь в перспективе более широкое применение. Конвенция также учитывает потребность в соблюдении свободы выражения мнений.

Конвенция Совета Европы о киберпреступности

Чтобы быть эффективными в киберпространстве, правоохранительные органы должны принимать во внимание легкость, с которой Интернет позволяет пересекать границы и юрисдикции. Это означает, что если правоохранительные органы не объединятся, чтобы договориться о некоторых универсальных правилах, будет трудно преследовать нарушителей.

Однако Интернет-сообщество опасается претворения законов в жизнь. В Интернете существует культура «почти все, что идет» (‘almost anything goes’), где приветствуется свобода выражения. Поскольку Интернет находится все еще на стадии становления, существует мнение, что законы, принятые для соблюдения правопорядка, могут задушить его развитие.

Конвенция Совета Европы о киберпреступности пытается решить данные проблемы. Совет Европы (СЕ) состоит из почти всех стран Европы. Он включает больше государств-членов, чем ЕС, который является другой организацией. СЕ разрабатывает соглашения, которые государства-члены могут ратифицировать, а могут и отклонить, в то время как ЕС провозглашает декларации, которые государства-члены должны ратифицировать в качестве внутригосударственных законов.

Из-за большого количества стран (почти 50), участвующих в СЕ, разработка соглашений о киберпреступности вызвала много вопросов. Но поскольку Совет Европы является региональной организацией, близкая культура и физическое соседство означают, что дипломатические трения, неизбежные в процессе обсуждения этих вопросов, будут сведены к минимуму. Кроме того, природа соглашений означает, что страны могут достичь согласия по тексту, но могут не принимать или же принимать избирательно. Эта возможность принимать или нет оставляет право принятия решения в отношении законов в руках национальных парламентов. Это отличается от правил, принимаемых в парламенте ЕС, которые должны быть реализованы в качестве законов в национальном законодательстве.

Поэтому правила СЕ находят компромисс между разнообразными проблемами. Конвенция о киберпреступности подверглась нескольким раундам международного обзора, с предложениями от таких организаций, как Американский союз гражданских свобод (American Civil Liberties Union), в отношении потенциальных конфликтных ситуаций при свободных выражениях.

Конвенция устанавливает руководящие принципы для стран, намеревающихся создать законы о киберпреступности. Она вступила в силу в июле 2004 года. Существует положение о международном сотрудничестве, означающее о том, что страны, не входящие в СЕ, могут присоединиться к Конвенции. Действительно, в январе 2007 года США присоединились к Конвенции.

За дополнительной информацией, пожалуйста, обращайтесь к «Совет Европы, «Киберпреступность: угроза демократии, правам человека и верховенству закона», http://www.coe.int/t/dc/files/themes/cybercrime/default_en.asp.

Возможно, еще один механизм для международного консенсуса заключается в активных объединениях на Форуме по вопросам управления использованием Интернета. Активные объединения представляют собой свободное группирование заинтересованных сторон вокруг важных вопросов. Динамичная коалиция, специализирующаяся на спаме, была довольно активна.

Альянс борьбы со спамом

Проблема спама состоит в том, что в отличие от традиционной рекламы большую часть ее расходов несет получатель, а не отправитель. По данным различных исследований значительная часть трафика электронной почты состоит из спама.

«Первое поколение» спама представляло собой раздражающую почту, большую часть которой пользователи и системные администраторы могли отфильтровать. Более новое поколение спама вызывает тревогу. С нарастающими темпами спам теперь несет вредоносное программное обеспечение, которое запускается без ведома пользователя. Компьютер может быть превращен в «bot», сетевого агента-робота, управляемого спамером для рассылки спама. В некоторых случаях спам может содержать программу для получения паролей и других конфиденциальных данных. Изощренность и масштабы этих операций наводят на мысль об уровне организаций, часто ассоциируемых с преступными бандами.

Это игра в кошки-мышки со спамерами, разрабатывающими все более изощренные методы рассылки спама, когда их предыдущие методы были побеждены. Для обмена передовым опытом и профессиональными идеями было сформировано активное объединение по спаму (Dynamic Coalition on Spam) в Форуме по управлению использованием Интернета. Коалиция объединила группы, которые уже работали в данном направлении. Эта работа продолжается, и группа теперь называется Альянсом борьбы со спамом (http://stopspamalliance.org).

Вопросы для размышления

В какой степени ваша страна участвует в международном сотрудничестве по решению проблемы злоупотреблений в Интернете?

Заключение

Нет никаких сомнений в том, почему сами по себе возможности Интернета, делающие его такой мощной средой, могут использоваться в темных целях. Нет сомнений в том, что существует необходимость в регулировании некоторых наиболее зловещих сторон использования Интернета.

Из-за трудностей в получении согласия на определение того, что является повсеместно оскорбительным, существуют затруднения в решении некоторых проблем, наносящих вред и убытки в Интернете. Наиболее заметные успехи были достигнуты в вопросах по обману потребителей и детской порнографии.

Первым делом необходимо международное соглашение для учреждения законов, а затем для их исполнения. Конвенция Совета Европы о киберпреступности может послужить основанием для будущего соглашения и сотрудничества.

Проверьте себя

1. С какими трудностями сталкиваются правоохранительные органы при борьбе со злоупотреблениями в Интернете?

2. Что признается всемирным сообществом в качестве киберпреступлений, с которыми необходимо бороться?

3. Какие новые преступления появились из-за бурного развития Интернета?

4. Какие санкции в отношении этих преступлений могут быть применены с помощью Интернета?

5. ВОПРОСЫ, ПЕРЕКРЫВАЮЩИЕСЯ С РЕАЛЬНЫМ МИРОМ

Задачей настоящего раздела является повышение осведомленности о совпадении деятельности Интернета с реальным миром в ключевых областях, касающихся экономики и государственного управления, а также по отношению к контенту, и осознание необходимости создания соответствующей нормативной базы.

Интернет оказывает влияние на реальный мир. Должен ли офлайновый мир быть изменен так, чтобы он более похож на виртуальный мир? Или должны ли применяться правила офлайн к сетевому миру? Ответ, конечно, находится где-то посередине.

5.1 Конкурентная политика

Насколько это возможно, доступ к Интернету должен быть конкурентоспособным. Это означает либерализацию сектора электросвязи, особенно, если сектор является монополистическим или того хуже, целой монополией. Либерализация в этом секторе, как показывает опыт, улучшает качество обслуживания и одновременно приводит к снижению цен. Низкие расценки, как было показано, приводят к увеличению проникновения Интернета. А в случае с широкополосным доступом к Интернету снижение стоимости меняет схему его использования. Теория игр утверждает о том, что нужно иметь, по меньшей мере, трех игроков в целях эффективной конкуренции.

Либерализация сектора электросвязи и стоимость Интернет-услуг

Как уже было сказано, одной из причин развития Интернета в США была либерализация сектора электросвязи. Интернет, в конце концов, зависит от международной протяженной электросвязи. Конкуренция в данном секторе снизила цены. Наиболее очевидное воздействие либерализации можно было заметить в США, где началось движение по либерализации рынка электросвязи: дешевле организовать свой сайт в США, чем в большинстве других стран. Это приводит к эффективному циклу, где экономия, обусловленная ростом масштабов производства, в свою очередь, позволяет сохранить низкие цены.

Исследования показали, что потребности в электросвязи являются достаточно эластичными. То есть, падение цены на X процентов приводит к увеличению спроса на более чем X процентов. Также исследования показали, что стимулирование конкуренции в местной петле электросвязи будет способствовать более глубокому проникновению Интернета.

Франция, Япония и Республика Корея увеличили широкополосный доступ через конкурентную политику. Республика Корея обладает наивысшим показателем широкополосного доступа в мире. Этому послужила политика, допускающая свободный доступ к основным средствам сферы электросвязи с 1980-ых годов. Случаи Франции и Японии являются более поучительными, поскольку темпы проникновения были не столь высоки приблизительно до 2005 года. С тех пор политика, стимулирующая конкуренцию, снизила цены, а распространение широкополосного доступа прыгнуло вверх.

С середины 1980-ых до середины 1990-ых во многих книгах и статьях обсуждаются преимущества либерализации сектора электросвязи. Либерализация Интернет-сектора представляет собой продолжение идей, рассмотренных в секторе электросвязи. См. Emanuele Giovannetti, «IT-революция, Интернет, и электросвязь: переход к конкурентоспособной индустрии в Европейском Союзе», в E. Giovannetti, M. Kagami и M. Tsuji, «Интернет-революция: глобальная перспектива (издательство Кембриджского университета, 2003 г.), стр. 124-142.

5.2 Цензура и свобода слова

Цензура со стороны правительства и частного сектора существует во всем мире. Как отмечалось ранее, вопрос состоит в сбалансированности местных интересов с международными нормами о введении небольшой или отсутствии цензуры в Интернете. Полное блокирование сайтов осуждается Интернет-сообществом. Наиболее практичным и приемлемым решением является какой-то элемент фильтрации со стороны пользователя. Фильтрующее программное обеспечение, установленное пользователем, является приемлемым. Но было установлено, что часто родители оказывались не столь сообразительны, как их дети в установке и использовании фильтров.

Добровольная самооценочная фильтрация

В 1999 году Фонд Бертельсмана (Bertelsmann) собрал группу для разработки системы фильтрации Интернет-контента, которая былы бы бесплатной, учитывала культурные особенности, а также не нарушала права на свободу слова. Данная команда включала исследователей, регуляторов, а так же защитников свободы слова. Заключительным этапом было формирование Ассоциации по оценке Интернет-контента (Internet Content Rating Association, ICRA).

Группа представляла себе идеальный результат: родитель кликнул бы на страну, в которой он или она находятся, затем кликнул на систему фильтрации (скажем, одну из установленных католической церковью), и затем сайты, которые считаются не соответствующими, будут отфильтрованы. Под действием системы фильтрации сайты маркировали бы себя по признакам языка, наличия насилия, обнаженных картинок и нежелательного (но легального) содержания, такого как алкоголь. В целом было примерно 40 ярлыков.

В конце концов, однако, ICRA не приблизилась к своей благородной цели. Во-первых, была оппозиция со стороны борцов за гражданские права, таких как Центр развития демократии и технологического прогресса в США.

Сайты новостей, которые первоначально согласились самомаркироваться, изменили свое мнение, когда они посчитали, что они будут восприниматься как уступающие режиму цензуры. Во-вторых, чтобы решить проблему свободы слова, вебсайты должны были самомаркироваться. Это препятствовало развитию критической массы сайтов, которые маркировали себя. Без той критической массы сайтов пользователи фильтра должны время от времени переставать пользоваться фильтрами так часто. В-третьих, фильтры работали бы лучше всего, если бы они были включены в браузеры. В то время, когда методика ICRA была готова к действию, война браузеров была закончена, из которой Microsoft вышел победителем. До тех пор и Netscape и Microsoft добавляли функции в свои браузеры. На самом деле, у браузера Microsoft в 2000 году была сырая система фильтрации. Наконец, как было испытано при другой подобной маркировке систем, как V-chip в США, которая, как предполагалось, фильтровала бы непотребное телевизионное содержание, никакого фактического спроса от потребителей не возникло, либо же потребители не действовали по своему устному соглашению о необходимости такой схемы фильтрации.

В 2007 году ICRA был преобразован в Институт семейной сетевой безопасности (Family Online Safety Institute).

Поскольку автор был непосредственно вовлечен в ICRA в качестве одного из членов Совета, вышеупомянутые подробности изложены впервые. В книге «Упорядочивание хаоса» изложены некоторые подробности о ICRA в главе под названием «Цензура и регулирование содержания Интернета».

Другой подход заключается в том, чтобы установить фильтры на серверном уровне, которые продаются в качестве специальной дополнительной услуги пользователям. Плата вносится для обновления и поддержания списка заблокированных сайтов. Такой фильтр обычному пользователю фактически невозможно обойти. Недостатком является то, что иногда срабатывала сверхблокировка, после чего трудно было «разблокировать» сайт, который был ошибочно заблокирован.

Практическое упражнение

1. Опишите меры регулирования контента, которые приняты в вашей стране, если таковые имеются.

2. Если правительство другой страны обратится с просьбой к правительству вашей страны заблокировать сайт с содержанием, нелегальным в данной стране, какие меры предпримет ваше правительство? Дайте свои рекомендации и обоснуйте их.

5.3 Диффамация

С гораздо большей свободой слова в Интернете появляется больше шансов для диффамации. В целом, решение вопроса об умышленном ложном сообщении требует сбалансированности конкурирующих интересов: интерес человека к собственной репутации и общественный интерес в деле поощрения большей свободы выражения мнений. В Интернете также существуют дополнительные сложности противоречивых культурных ценностей в нагрузку к личным и общественным интересам.

Один из самых поучительных случаев связан с Джозефом Гутником, предпринимателем из Мельбурна, Австралия. Журнал Barron's, принадлежащий компании Dow Jones, опорочил господина Гутника в статье. У журнала было 14 подписчиков в Австралии, пять из которых были из штата Виктория. Этого было достаточно для распространения юрисдикции Австралийского Верховного суда.[31] У журнала *Barron's* было 1700 онлайн-подписчиков, которые заплатили австралийской кредитной карточкой. И встал вопрос: если бы Гутник выиграл дело, означало ли бы это, что все печатные издания должны были следить за тем, что они издавали, используя в качестве критерия страну с самыми жесткими законами о диффамации? К счастью, Верховный суд постановил, что денежная компенсация, на которую г-н Гутник мог претендовать, будет ограничена в нанесении вреда его репутации только в Мельбурне, но не глобально.[32] Суд, как представляется, принял к сведению фактический ущерб, который клеветническая статья, возможно, могла нанести. Обычно суды Британского Содружества не склонны так делать.

Практическое упражнение

Дайте совет Y, который является гражданином вашей страны, в следующих ситуациях:

Ситуация 1:
В блоге, принадлежащем W, в вашей стране оклеветали Y. Есть ли разница в зависимости от того, популярен данный блог или нет? Что делать, если там оказалось 200 сообщений, защищающих Y?

Ситуация 2:
Что делать, если организация онлайн-новостей в США оклеветала компанию, принадлежащую Y. Может ли это стать «глобальной ответственностью» за клевету в Интернете?

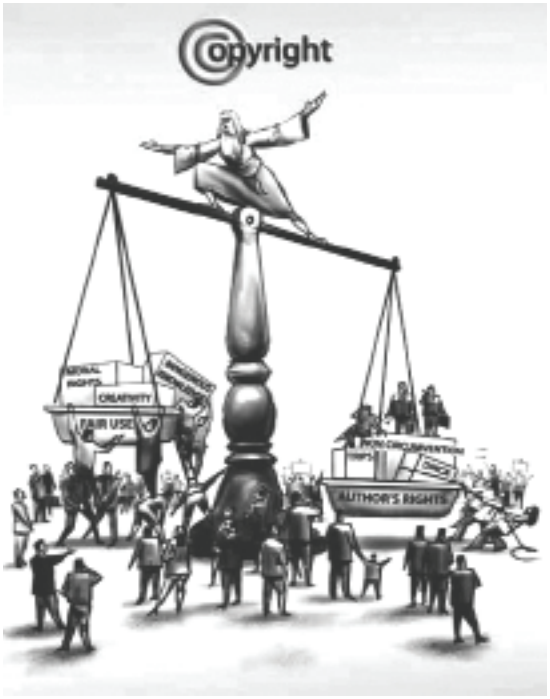
Интернет вынудил внести еще одно изменение в законы, регулирующие использование Интернета: необходимость для предоставления иммунитета для контента третьей стороны. Это означает, что владельцы вебсайта и форума не должны нести ответственность за содержание, размещенное другими, при условии «разумности» действий владельцев после уведомления о дискредитирующем содержании. В большинстве юрисдикций «действовать разумно» означает устранение дискредитирующего содержания в течение установленного срока.[33] Это положение также называют «уведомлением и устранением».

31 David Fickling and Stuart Millar, "How Diamond Joe's libel case could change the future of the internet," *The Guardian*, 11 December 2002, http://www.guardian.co.uk/technology/2002/dec/11/media.newmedia.
32 High Court of Australia, "Dow Jones and Company Inc v Gutnick [2002] HCA 56" (10 December 2002), http://www.austlii.edu.au/au/cases/cth/high_ct/2002/56.html.
33 See Ang (2005).

5.4 Авторское право и другие права интеллектуальной собственности

Рисунок 3. Уравновешивание в авторском праве

(Источник: DiploFoundation, http://textus.diplomacy.edu/textusbin/env/scripts/Pool/GetBin.asp?IDPool=1181)



Для авторского права необходимо обеспечение аналогичного положения иммунитета. Это означает, что владельцы вебсайта и форума не должны нести ответственность за содержание, размещенное другим лицом, которое может привести к нарушениям авторского права, при условии с правилами принимающей стороны «о разумности». Все чаще во многих странах стали принимать американское положение «Уведомление и устранение», предоставленное для обеспечения авторского права. Данные положения позволяют уведомлению быть оспоренным. Лицо, утверждающее о нарушении авторского права, может либо отступить и позволить информации остаться размещенной, либо же этот вопрос будет решен в судебном порядке.

Нужно ли доменные имена рассматривать в качестве товарных знаков - это спорная область в праве на интеллектуальную собственность. Для транснациональных компаний такое правило ослабило бы бремя необходимости регистрации своего имени в каждой стране. Это правило будет означать, что любой, кто использует название транснациональной компании в качестве своего доменного имени без соответствующего разрешения, нарушает правила прав на интеллектуальную собственность и должен будет отказаться от использования доменного имени этой компании.

Единые процедуры ICANN по урегулированию споров может разрешить этот вопрос на глобальном уровне. Но в каждой стране необходимы национальные правила для разъяснения прав относительно страновых доменных имен ccTLDs.

Вопросы для размышления

1. Должны ли считаться доменные имена в качестве товарных знаков? Почему да или почему нет?

2. Как бы вы расположили интересы своей страны и тех праводержателей, которые могут быть из более развитых стран?

5.5 Неприкосновенность частной жизни

Как было замечено ранее, сохраняются правила неприкосновенности частной жизни. Возникает вопрос: какая модель должна использоваться для регулирования неприкосновенности частной жизни? Существуют, в основном, две модели с разными парадигмами. В модели ЕС неприкосновенность частной жизни является одним из прав человека. Она не может быть куплена, продана или иметь какой-либо коммерческий характер, и это заслуживает всеобъемлющей законодательной поддержки. В американской модели неприкосновенность частной жизни является юридическим правом, которое может быть передано под контракт. Например, в обмен на предоставление адреса электронной почты можно иметь возможность читать некоторые документы или воспользоваться некоторой услугой. Законодательная поддержка в этом случае не является всеобъемлющей, а носит фрагментный характер.

Что касается Интернета, то обе парадигмы весьма схожи в действии и по результатам. Конечно, у европейской модели есть больше санкций, но она и обходится дороже.

Способ, который выбирает страна, зависит больше всего от влияния ее культуры и истории. Европейская модель, однако, имеет потенциал принятия во всем мире, если будет исполняться Директива о защите данных (Data Protection Directive).

Вопросы для размышления

1. Насколько требование пользователя в неприкосновенности личной жизни в законодательном порядке признается в вашей стране?

2. По какой из моделей регулирования неприкосновенности частной жизни, ЕС или США, вероятнее всего последует ваша страна? Объясните вашу точку зрения.

Заключение

Процесс регулирования должен быть прозрачным, демократичным и вовлекать как можно больше сторон. То есть, данный процесс должен носить консультативный характер с участием всех заинтересованных сторон. Следует также изучить все четыре способа регулирования — с помощью рынка, социальных норм, структурно и через государственное регулирование (в том числе саморегуляцию, так как для повышения эффективности саморегуляция требует делегирования полномочий от правительства).

Проверьте себя

1. Какова значимость конкурентной политики для доступа в Интернет?
2. До какой степени может быть допустима или дозволена цензура в Интернете, если такое вообще может быть?
3. Может ли пользователь Интернета оклеветать кого-либо в онлайне и остаться безнаказанным?
4. Должен ли быть изменен закон о диффамации с учетом Интернета?
5. Какие существуют основные спорные вопросы, касающиеся авторских и других прав интеллектуальной собственности в Интернете?
6. Какие существуют 2 модели обеспечения неприкосновенности частной жизни и защиты данных? Как они отличаются?

6. АСПЕКТЫ РАЗВИТИЯ: ЦИФРОВОЕ НЕРАВЕНСТВО

Данный раздел описывает, каким образом Интернет может быть использован для социально-экономического развития, а также какие существуют ограничения ИКТР.

Национальное развитие было одним из мотивов для ВВУИО, который, в конечном итоге, привел к дискуссии по вопросам управления использованием Интернета. Тем не менее, развитие представляет собой большую тему, решение которой займет многие десятилетия. Надежда на ИКТ, в том числе Интернет, состоит в том, что они будут способствовать ускорению процесса развития.

6.1 ИКТ в целях развития

Для эффективности ИКТР должен охватить следующее: (1) управление и расширение прав и возможностей, (2) инфраструктура, (3) экономическое развитие, и (4) социальное развитие. Без надлежащего управления финансовые средства могут быть растрачены впустую. Без полномочий пользователи не считают, что они могут изменить свое положение. Без такой инфраструктуры как электричество или телекоммуникационные линии невозможно обеспечить жизнеспособность Интернета.

ВВУИО помогла учредить Фонд цифровой солидарности. ЦРТ представляют собой хорошее руководство по тому, каким образом Фонд должен быть израсходован. ЦРТ являются:

1. Ликвидация крайней нищеты и голода
2. Обеспечение всеобщего начального образования
3. Содействие равенству мужчин и женщин, а также расширение прав и возможностей женщин
4. Сокращение детской смертности
5. Улучшение охраны материнства
6. Борьба с ВИЧ/СПИДом, малярией и другими заболеваниями
7. Обеспечение экологической устойчивости
8. Формирование глобального партнерства в целях развития.

В модуле 1 из серии Академии ИКТ для лидеров государственного управления обсуждается взаимосвязь между ИКТ и ЦРТ.

Интернет для деревни

Будучи мощной и современной технологией, Интернет обладает потенциалом для расширения неравенства в доходах между теми, кто использует его, и теми, кто этого не делает. Одна из самых драматических иллюстраций различий может быть найдена в Индии. Там можно обнаружить присутствие новейших современных технологий — в больших городах. Но в сельских районах Индии есть места, которые сами индийцы называют «медиа темными» — где не имеется телевидение.

Для распространения использования Интернета и решения ряда социальных проблем правительство Индии в 2007 году запустило национальный проект по электронному управлению под названием «Сеть центров общественных услуг» (ЦОУ), согласно которому в 600 000 деревнях в Индии будет размещено 100 000 центров. В сущности, это так называемые Интернет-киоски.

Прежние Интернет-киоски не имели особого успеха. Фактически, у первой волны таких киосков норма успеха составляла только 3 процента, причем успех в данном случае измерялся устойчивостью через год. Приняв во внимание опыт первой волны, у второй волны норма успеха составила 30 процентов. Это десятикратное увеличение, но это все еще означало 70-процентную норму отказа. Сеть ЦОУ была бы третьей волной. Это было бы реализовано на основе результатов последнего исследования о том, какие приложения будут полезными для сельских жителей, а также преобразующими их жизни.

Например, правительство Индии предоставит доступ к базе данных о праве собственности на землю, потому что в деревнях коррумпированные чиновники иногда обманывают сельских жителей с их землями. Запись на компакт-диски и печать цифровых фотографий, как выяснилось, также являются источниками доходов. В городе Ченай (Chennai) по частной инициативе было установлено, что выставление экзаменационных работ в онлайне способствует преобразованию: обычно у сельских жителей низкий показатель сдачи основных экзаменов. Но когда они занимаются с экзаменационными работами, доступными в онлайне, их показатели резко улучшаются. Уверенность, которая приходит после успешной сдачи экзамена, является расширением прав и возможностей.

Сеть ЦОУ представляет собой творческую идею. Помимо использования Интернета для решения социальных проблем (таких, как незаконный захват земли) и сокращения цифрового разрыва, она также направлена на обеспечение некоторой занятости. Операторы Интернет-киосков в деревнях должны быть частными предпринимателями. В теории это означает, что затраты национального правительства будут низкими, в то время как правительства штатов, как ожидается, будут содействовать финансами или другими видами поддержки, и вклад частного сектора может быть в виде финансовых издержек.

Сеть в настоящее время развернута. За результатами стоит понаблюдать.

Для получения дополнительной информации см. Департамент информационных технологий, «Сеть ЦОУ», правительство Индии, http://www.csc-india.org.

6.2 Ограничения и барьеры

На данном этапе следует иметь в виду, что существуют ограничения в отношении полезности ИКТР. Например, использование ИКТР предполагает, что «качественная информация соответствует лучшим решениям», а это не обязательно так. Кроме того, многие приложения ИКТ являются средством для обеспечения или обработки информации, а не средством коммуникации, когда связь часто дает более надежные результаты в области развития. Существуют также препятствия, лежащие вне контроля любого человека. Языковые проблемы могут быть барьером. Коррупция также является препятствием.

Стоимость по-прежнему представляет собой одну из основных тем для рассмотрения. Тем не менее, затраты могут быть уменьшены. Во-первых, возрастает доступность более дешевых устройств. Во-вторых, существует доступность программного обеспечения под эгидой ПО с открытым кодом (free and open source software, FOSS). Следует отметить, что прикладные программы FOSS не могут быть дешевыми, потому что они требуют технического обслуживания, и иногда некоторых компонентов программы (для соединения, скажем, с принтером), которых возможно, нет в наличии, должны быть специально написаны.

6.3 Применение ИКТР

Существует много известных и хорошо проверенных применений ИКТР. Как уже отмечалось, большинство из них находится в форме доставки информации. Такие приложения могут быть найдены в сельском хозяйстве, образовании, здравоохранении и туризме. Зачастую правда то, что более точная информация в этих секторах приводит к лучшему результату. Например, информация, что лучше сажать и когда, будет полезна для фермеров.

Помимо обеспечения информацией коммуникации могут принести еще больше пользы. Например, после посадки было бы полезно знать, как бороться с вредителями, которые напали на растения. ИКТР имеют наибольшие перспективы именно в обеспечении лучшей коммуникации.

Особенно перспективным является развитие и продвижение услуг электронного правительства. Примеры услуг электронного правительства включают в себя обработку виз, подачу налогов, регистрацию прав собственности на землю, подачу и выдачу водительских прав и даже просто обеспечение возможности заполнить формы заявок в онлайне. Для начала все государственные учреждения должны быть компьютеризированы. Результатом компьютеризации является повышение эффективности государственного управления. Так, например, проведение процедур государственных закупок в онлайне, как показывает опыт, экономит финансовые средства. При компьютеризации процессы становятся более прозрачными, что снижает коррупцию. Компьютеризация также способствует созданию ИТ-экономики, где становится возможной карьера в области ИТ для технического персонала и программистов. Компьютеризация в сочетании с использованием Интернета предоставляет возможность для более широких консультаций граждан по важным государственным вопросам. Это, в свою очередь, приводит к расширению прав граждан, что является началом благотворного цикла развития (*В модуле 3 из серии Академии ИКТ для лидеров государственного управления обсуждается применение электронного правительства*).

Большая прозрачность, обеспечиваемая услугами электронного правительства, как часто говорят, приводит к большей демократии. Это не обязательно так. На самом деле, услуги электронного правительства предоставляют возможность усиления контроля со стороны центрального правительства. Это облегчает для центрального правительства получение данных о том, что происходит в конечной точке предоставления государственной услуги. Это вынуждает руководство государственной службы на местном уровне быть более отзывчивым, и тем самым снижается коррупция.[34]

Заключение

Развитие было одним из мотивов для ВВУИО, который привел к формированию РГУИ. Но теме развития не уделили достаточного внимания в итоговом отчете РГУИ, и она часто упускается в дискуссиях по управлению использованием Интернета. Международное сообщество может, конечно, многое сделать через финансирование проектов ИКТР. Государственно-частное партнерство является наиболее устойчивым способом, поскольку при этом происходит разделение расходов финансирования, и при структурном осуществлении проектов наблюдается больше шансов на успех. (*Применение ГЧП для финансирования проектов по ИКТ рассматривается в Модуле 8 Академии ИКТ для лидеров государственного управления*). Но есть многое из того, что национальные правительства могут и должны сделать, чтобы использовать ИКТР. Стоимость доступа должна быть ниже. Например, затраты на регистрацию доменного имени могут быть снижены. Затем следует проявить политическую волю для укрепления правовой среды, которая является благоприятной для ИКТР. Использование ИКТР, в частности, в качестве инструмента для коммуникации никогда не было более обнадеживающим.

Проверьте себя

1. Как может быть использован Интернет для содействия достижению целей в области развития?
2. Какие существуют ограничения и барьеры на пути использования Интернета для достижения целей в области развития?

34 R. Kluver, The Architecture of Control: a Chinese Strategy for e-Governance, in “The Internet and Governance: The Global Context,” *The Journal of Public Policy*, 25, 1 (2005): 75-97.

7. УПРАВЛЕНИЕ ИНТЕРНЕТОМ: ВЗГЛЯД В БУДУЩЕЕ

В данном разделе перечислены нерешенные вопросы управления использованием Интернета, которые Форум по управлению Интернетом не может и не будет решать, и которые требуют внимания правительств.

Пятилетний мандат Форума по управлению использованием Интернета заканчивается в 2010 году. Многое из запланированного для Форума вошло в пленарные заседания. Выгоды наличия Форума очевидны. Концептуально он предоставил возможность для обсуждения важных вопросов, а также позволил небольшим странам поднимать свои проблемы. На практике, было привлечено внимание вопросам управления Интернетом и улучшено понимание важности процесса в управлении использованием Интернета.

По иронии судьбы, большая часть реальных действий по управлению Интернетом теперь происходит в параллельных сессиях, где планирование носит децентрализованный характер для сторон, предлагающих темы заседаний. Некоторые из динамических коалиций, в частности, принимали активное участие в реализации интересов своих соответствующих групп. Например, параллельная сессия по спаму была очень активной в организации совещаний по урегулированию данного вопроса.

Темы, поднятые в итоговом отчете РГУИ, являются сложными и не ведут к легким путям решения. Например, политический вопрос международного надзора над ICANN и DNS был забюрократизирован. Администрация США может заявить о «победе» в том смысле, что ICANN все еще находится в их руках. На заднем плане раздается ропот, так как, несмотря даже на то, что страновые ccTLDs находятся в руках национальных правительств, правительству США ничто не мешает физически прекратить в одностороннем порядке контроль любой страны над своей ccTLD. Существуют практические ограничения, но нет физического ограничения. Это означает, что возможность все еще существует, хотя и гипотетическая, что страну могут отключить от Интернета.

Другие важные блоки вопросов — использование Интернета, вопросы, связанные с Интернетом, но с более широким воздействием, а также аспекты развития Интернета — не поддаются легкому разрешению. Что может сделать Форум по управлению Интернетом, так это помочь осветить передовой опыт для их решения. Усиление потенциала для управления Интернетом будет также постоянной проблемой, которой должны заняться все правительства.

Обсуждение, которое привело к итоговому отчету РГИУ, вызвало осознание важности вопросов управления Интернетом. Поскольку на решение проблем уйдет время, правительства должны повысить свой потенциал для решения данных вопросов и принять участие в международных обсуждениях по ним. Такое укрепление потенциала является необходимым, поскольку управление Интернетом является не только вопросом международного сообщества. Многие из этих вопросов по управлению Интернетом должны решаться на местном уровне. Вопросы ИКТР являются наиболее важными для местных органов власти. По этой причине местные органы власти и национальные правительства должны играть ключевую роль в управлении использованием Интернета.

ЗАКЛЮЧЕНИЕ

В данном модуле по управлению использованием Интернета рассматривается следующее:

1. Вопрос управления Интернетом касается больше управления, чем самого Интернета. Он охватывает ряд политических вопросов, касающихся международной политики в отношении Интернета, использование и злоупотребление Интернетом, а также развертывание Интернета в целях содействия достижению социального и экономического развития.

2. Несмотря на бытующее неверное представление, Интернет имеет центральный контрольный пункт в области, называемой системой корневой зоны. Данная система корневой зоны находится под контролем организации под названием ICANN, за которым стоит правительство США.

3. РГУИ (Рабочая группа по управлению использованием Интернет) была создана под эгидой ООН для урегулирования напряженности вокруг политического аспекта управления Интернетом. В процессе бурных обсуждений и компромиссов после отчета РГУИ было принято решение о том, что будет проводиться легковесный Форум по управлению использованием Интернет, но система корневой зоны будет все еще находиться в руках ICANN с условием, что только национальные правительства могут управлять и использовать свои соответствующие страновые домены верхнего уровня ccTLDs.

4. Управление Интернетом должно быть многосторонним и мультисекторальным. Это означает, что ни одна из стран или организаций не должна иметь решающий голос в управлении Интернетом. Вместо этого процесс на национальном или международном уровне должен быть демократичным. На международном уровне в управлении Интернетом должны принимать участие все страны; на всех уровнях в управлении должны участвовать представители частного сектора и гражданского общества.

5. Как и в реальной жизни, Интернет может управляться четырьмя способами: закон, социальные нормы, рыночные механизмы и архитектура. Поскольку соблюдение закона не всегда является жизнеспособным в Интернете, правительства должны проявлять творческий подход в вопросах регулирования в Интернете.

6. Саморегуляция является формой делегированного государственного регулирования. Она часто рекомендуется в качестве предпочтительной формы регулирования Интернета, но существуют ограничения и издержки для ее применения.

7. Была предложена «дорожная карта» регулирования Интернета в целях поощрения его распространения наряду с возможностью получения вреда.

8. Интернет дал новую жизнь ряду старых преступлений, а также породил новые правонарушения. Одной из трудностей в соблюдении правопорядка является определение преступления.

    а. Двумя областями, где существует практически всеобщее согласие, являются детская порнография и обман потребителей. Правоохранительные органы сотрудничают для преследования таких преступлений.

    б. Спам, мошенничество, вредоносные программы и фишинг являются общепринятыми преступлениями, но не все страны имеют законы, направленные против них.

    в. Существует еще больший разрыв в правилах и противодействиях в отношении киберзапугивания, киберпреследования, кражи личных данных и Интернет-зависимости.

г. Форум по управлению Интернетом инициировал создание «активных объединений», где могут встретиться группы, заинтересованные в решении конкретных задач, для обсуждения передовой практики и общих мер.

9. Точно так же, как нормативные документы должны быть креативными, санкции в Интернете тоже должны быть творческими.

10. В конце концов, международное сотрудничество имеет важное значение для победы над преступным поведением в Интернете.

11. Вопросы управления Интернетом распространяются на офлайновый мир. Примеры включают политику в области конкуренции, цензуру и свободу выражения мнений, диффамацию, авторское право и права на интеллектуальную собственность, а также неприкосновенность частной жизни.

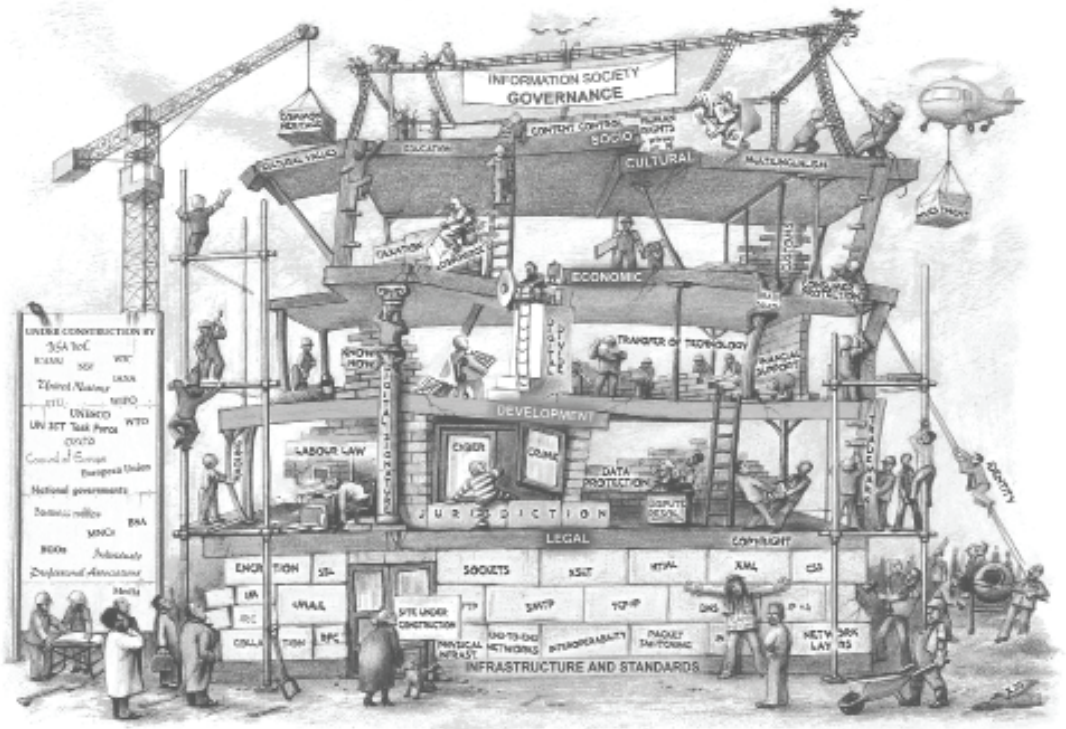
12. Одним из мотивов для изучения управления Интернетом была обеспокоенность тем, что развивающиеся страны будут оставлены вне информационной экономики. Таким образом, использование ИКТР является важной составной частью управления Интернетом.

    а. Существуют ограничения и преграды на пути использования ИКТР.

    б. Существуют также истории успеха, которые могут воспроизведены.

    в. ИКТР, например, может помочь улучшить управление реальным миром за счет улучшения прозрачности управления.

13. Политическая напряженность в управлении Интернетом не была урегулирована, и создание возможностей для управления использованием Интернета остается постоянной проблемой, которой должны заняться все правительства.



Источник: DiploFoundation, http://textus.diplomacy.edu/textusbin/env/scripts/Pool/GetBin.asp?IDPool=1190.

ПРИЛОЖЕНИЕ

Дополнительная литература

Ang, Peng Hwa. 2005. *Ordering Chaos: Regulating the Internet*. Singapore: Thomson.

Butt, Danny, ed. 2005. *Internet Governance: Asia-Pacific Perspectives*. Bangkok: UNDP-APDIP. http://www.apdip.net/publications/ict4d/igovperspectives.pdf.

Cukier, Kenneth Neil. 2005. Who Will Control the Internet? *Foreign Affairs* November/December. http://www.foreignaffairs.org/20051101facomment84602/kenneth-neil-cukier/who-will-control-the-internet.html.

Drissel, David. 2006. Internet Governance in a Multipolar World: Challenging American Hegemony. *Cambridge Review of International Affairs* 19(1), March, 105-120.

Kapur, Akash. 2005. *Internet Governance: A Prime*r. Bangkok: UNDP-APDIP. http://www.apdip.net/publications/iespprimers/eprimer-igov.pdf.

Working Group on Internet Governance. 2005. *Report of the Working Group on Internet Governance*. http://www.wgig.org.

Wu, Tim, Esther Dyson, A. Michael Froomkin and David A. Gross. On the Future of Internet Governance. *American Society of International Law Proceedings of the Annual Meeting*, Vol. 101. http://ssrn.com/abstract=992805.

Глоссарий

IP адрес	Адрес Интернет-Протокола: уникальный идентификатор, соответствующий каждому компьютеру или устройству в IP сети. В настоящее время активно используются два типа IP адресов. IP версия 4 (IPv4) и IP версия 6 (IPv6). IPv4 (которая использует 32 битную нумерацию) используется с 1983 года и все еще является наиболее широко используемой версией. Развертывание протокола IPv6 началось в 1999 году. Адреса IPv6 - 128-битовые числа.
Регистратор	Лицо, санкционированное (аккредитованное) системным реестром для продажи/регистрации доменных имен от своего лица.
Регистратура, Регистрационное бюро	Регистрационное бюро - компания или организация, которая обслуживает централизованную базу данных системного реестра для доменов верхнего уровня (TLD) или для блоков IP адресов (например, RIR — смотрите ниже). Некоторые Регистрационные бюро действуют без регистраторов вообще, а некоторые работают с регистраторами, но также позволяют и прямую регистрацию через системный реестр.
RIR	Региональные системные реестры Интернета. Это некоммерческие организации ответственные за распределение IP адресов на региональном уровне Провайдерам услуг Интернета и местным регистрационным бюро.
Корневые сервера	Серверы, которые содержат ссылки (указатели) на официальные (авторизированные) серверы имен для всех TLDs доменов верхнего уровня. В дополнение к «оригинальным» 13 корневым серверам, несущим файл корневой зоны, управляемым Комитетом по цифровым адресам в Интернете (Internet Assigned Numbers Authority), в настоящее время существует большое количество Anycast серверов, которые предоставляют идентичную информацию и которые были развернуты по всему миру некоторыми из оригинальных 12 операторов.
Файл корневой зоны	Основной файл, содержащий ссылки (указатели) на серверы имен для всех TLDs доменов верхнего уровня.
WHOIS	WHOIS - это протокол транзакций (запрос/ответ), который широко используется для предоставления информационных услуг интернет-пользователям. В то время как первоначально, данный протокол использовался большинством (но не всеми) операторов, регистрирующих TLD домены верхнего уровня для предоставления услуги «белые страницы» («white pages») и информации о зарегистрированных доменных именах, текущее использование охватывает намного более широкий диапазон информационных услуг, включая RIR WHOIS поиски для получения информации распределения IP адресов.

Заметки для инструктора

Как отмечено в разделе, озаглавленном «О серии модулей», этот и другие модули серии предназначены для того, чтобы донести знания различной аудитории в разнообразных и изменяющихся национальных условиях. Настоящие модули также могут быть представлены полностью или по частям, разными способами, в аудитории или через Интернет. Эти модули могут изучаться отдельными лицами и группами в учебных заведениях, а также в государственных организациях. Уровень участников, а также продолжительность учебных занятий будет определяться степенью детализации представления информации.

Данные заметки предлагают тренерам некоторые идеи и предложения для представления содержания модуля наиболее эффективно. Дальнейшие указания по учебным подходам и стратегиям представлены в справочнике по разработке учебных программ, разработанного в качестве сопутствующего материала для серии модулей Академии *ИКТ для лидеров государственного управления*. Руководство доступно по адресу: http://www.unapcict.org/academy.

Применение модуля

Каждый раздел данного модуля начинается с изложения целей обучения и заканчивается комплексом вопросов «Проверьте себя». Читатели могут использовать задачи и вопросы в качестве основы для оценки процесса изучения. Каждый раздел также содержит вопросы для обсуждения и практические упражнения, которые могут быть выполнены самими читателями или использоваться инструкторами. Эти вопросы и упражнения разработаны для того, чтобы дать возможность читателям, опираясь на собственный опыт, оценить содержание и подумать над заданными вопросами.

Тематические исследования являются важной частью содержания модуля. Они предназначены для обсуждения и анализа, особенно с точки зрения того, насколько ключевые концепции и принципы, представленные в модуле, работают в примерах из реального мира. В случае с управлением Интернета вопросы рассматриваются одновременно на международном и национальном или местном уровнях. Много работы выполняется на местном и национальном уровнях, особенно в области использования ИКТ, включая Интернет, в целях развития. Инструктор может побудить участников сослаться на другие примеры и случаи из собственного опыта, подтверждающие темы обсуждений модуля.

Структурирование занятий

В зависимости от аудитории, доступного времени, местной обстановки и условий содержание модуля может быть представлено в различных вариантах по длительности. Могут быть высшие правительственные должностные лица, которым нужно представить некоторые обновления и информацию об управлении Интернетом. Поэтому учебная программа должна быть построена в виде кратких сессий на час или два. Полная программа обучения занимает минимум полтора дня. Первые три раздела данного модуля включают обширное описание и теорию, а остальные разделы содержат практические вопросы.

Для занятий продолжительностью 60-120 минут

Уплотните разделы 1 и 2, уделив особое внимание вопросам, а также результатам, достигнутым в ВВУИО и РГУИ. Включите тему ИКТР из раздела 6.

Для занятия продолжительностью 3 часа

Уплотните разделы 1 и 2, как указано выше. В зависимости от участников, объедините разделы 3, 4, 5 и 6 с целью рассмотреть вопросы —

- Разработки правовой базы – в этом случае уделите внимание разделам 4 и 5;
- Использования ИКТР – в этом случае рассмотрите разделы 5 и 6.

Для занятий продолжительностью один день (6 часов)

Рассмотрите разделы 1, 2 и 3 в первой половине дня. Во второй половине дня обсудите разделы 4, 5 и 6, используя упражнения и вопросы для обсуждений. Это должно сохранить высокий уровень активности после обеда. Завершите занятие разделом 7.

Для занятий продолжительностью полтора дня

Хотя есть семь разделов, они имеют различную длительность. Вы должны оценить интересы группы — то есть, что они надеются получить от данного обучения. Разделы 1 и 2 не просты для изучения. Если группа не заинтересована в содержании, а только в результатах, то и уделите внимание рассмотрению этих результатов. В целом, более вероятно, что участники захотят изучить больше практических навыков. Обсуждения и обмен информацией должны быть полезными в усилении обучения.

Для занятий продолжительностью три дня

Обсудите разделы 1 и 2 в первый день. В зависимости от того, как группа отвечает, можно перейти к разделу 3. На второй день охватите разделы 3, 4 и 5. На третий день обсудите разделы 6 и 7. Стимуляция имеет важное значение. Участникам следует предложить поделиться собственным опытом в классе. В частности, участников следует поощрять к использованию содержания раздела 6 в вопросах по преодолению «цифрового неравенства» в своих соответствующих странах. Раздел 7 дает возможность подвести итог всего занятия.

Об авторе

Анг Пенг Хва (Ang Peng Hwa), профессор и директор сингапурского Интернет-исследовательского центра при колледже Ви Ким Ви по коммуникации и информации, технологический университет Nanyang, Сингапур. Юрист по образованию, он преподает право и политику о средствах массовой информации. Он проводит исследования в области управления Интернетом. В своей книге «Вызов хаоса: регулирование Интернета», изданной в 2005 году, он утверждает, что Интернет может быть, должен быть и уже регулируется.

В 2004 году он был назначен от имени Генерального секретаря ООН в Рабочую группу по управлению Интернетом для подготовки доклада к заседанию Всемирной встречи на высшем уровне по вопросам информационного общества, которая прошла в 2005 году. Позже он помог совместно создать академическую сеть по вопросам глобального Интернет-управления, где он был избран в качестве первого председателя.

В настоящее время он выступает в качестве председателя информационно-коммуникационного центра группы азиатских СМИ. Он также входит в состав управляющего совета института связи Мудра, Ахмедабад, Индия. С июля 2008 года он взял годичный отпуск с поста декана для руководства и помощи по запуску деятельности Института исследований Мудра в области связи.

АТУЦ ИКТР

Азиатско-Тихоокеанский учебный центр информационных и коммуникационных технологий для развития при ООН является вспомогательным органом Экономической и социальной комиссии ООН для Азии и Тихого океана (ЭСКАТО). Целью АТУЦ ИКТР является активизация усилий стран-членов ЭСКАТО по использованию ИКТ в их социально-экономическом развитии на основе создания человеческого и институционального потенциала. Работа АТУЦ ИКТР сосредоточена на трех основных компонентах:

1. Обучение. Для повышения знаний и навыков в области ИКТ разработчиков политики и ИКТ-специалистов, а также укрепление потенциала инструкторов и учебных заведений в области ИКТ;
2. Исследование. Для проведения аналитических исследований, связанных с развитием человеческих ресурсов в области ИКТ;
3. Консультации. Для оказания консультационных услуг по программам развития человеческих ресурсов для членов и ассоциированных членов ЭСКАТО.

АТУЦ ИКТР находится в г. Инчон, Республика Корея.

http://www.unapcict.org

ЭСКАТО

ЭСКАТО является региональным подразделением Организации Объединенных Наций и выступает в качестве главного центра ООН экономического и социального развития в Азиатско-Тихоокеанском регионе. Ее задача заключается в укреплении сотрудничества между ее 53 членами и 9 ассоциированными членами. ЭСКАТО обеспечивает стратегическую связь между глобальными и программами и проблемами на национальном уровне. Она оказывает поддержку правительствам стран региона в деле укрепления региональных позиций и защищает региональные подходы в решении уникальных социально-экономических проблем в условиях глобализации в мире. ЭСКАТО находится в Бангкоке, Таиланд.

http://www.unescap.org

Серия модулей Академии ИКТ для лидеров государственного управления

http://www.unapcict.org/academy

Академия представляет собой всеобъемлющую учебную программу в области ИКТР, состоящую из восьми модулей, основная цель которых оснастить разработчиков политики необходимыми знаниями и навыками по использованию в полной мере возможностями ИКТ для достижения целей национального развития и преодоления «цифрового разрыва».

Модуль 1 – Взаимосвязь между ИКТ и полноценным развитием

Освещаются ключевые вопросы и решения от этапов создания политики до реализации в области использования ИКТ для достижения Целей развития тысячелетия.

Модуль 2 –Политика, процессы и управление ИКТ в целях развития

Основное внимание уделяется вопросам создания политики и управления ИКТР, а также предлагается важная информация об аспектах национальной политики, стратегий и рамочных структур, способствующих ИКТР.

Модуль 3 – Применение электронного правительства

Изучаются концепции электронного правительства, принципы и виды приложений. Здесь также рассматриваются вопросы построения систем электронного правительства и определения соображений процесса проектирования.

Модуль 4 – Тенденции развития ИКТ

Содержится анализ современных тенденций в области ИКТ и будущих направлений развития. Здесь также рассматриваются основные технические и политические соображения при принятии решений в области ИКТР.

Модуль 5 – Управление использованием Интернета

Рассматривается дальнейшее развитие международной политики и процедур, которые регулируют использование и эксплуатацию сети Интернет.

Модуль 6 – Обеспечение информационно-сетевой безопасности и неприкосновенности частной жизни

Рассматриваются вопросы и тенденции в области информационной безопасности, а также процесс разработки стратегии по обеспечению информационной безопасности.

Модуль 7 – Управление проектами в области ИКТ в теории и на практике

Представляются концепции управления проектами, имеющими отношение к проектам в области ИКТР, в том числе широко используемые методы, процессы и порядки в области управления проектами.

Модуль 8 – Варианты финансирования ИКТ в целях развития

Изучаются варианты финансирования проектов в области ИКТР и электронного правительства. Освещается государственно-частное партнерство, как особо полезного варианта финансирования в развивающихся странах.

В настоящее время данные модули дополнены местными тематическими исследованиями национальными партнерами Академии для обеспечения значимости модулей и удовлетворения потребностей разработчиков политики в разных странах. Эти модули также переведены на разные языки. Кроме того, данные модули будут регулярно обновляться в целях обеспечения их актуальности для разработчиков политики, а также для разработки новых модулей, направленных на ИКТР 21-го века.

Виртуальная академия АТУЦ ИКТР (AVA – http://ava.unapcict.org)

- Интернет-платформа дистанционного обучения для *Академии*.
- Разработана для обеспечения доступности в режиме онлайн всех модулей Академии, включая виртуальные лекции, презентации и тематические исследования.
- Предоставляет возможность обучающимся лицам изучать материалы по своему усмотрению.

Электронный центр ИКТР для совместной работы (e-Co Hub – http://www.unapcict.org/ecohub)

- Ресурсный и сетевой портал для обмена знаниями в области ИКТР.
- Предоставляет удобный доступ к содержанию модулей.
- Пользователи могут участвовать в дискуссиях в режиме онлайн и стать частью Интернет-собщества практиков e-Co Hub, которая служит для обмена опытом и расширения базы знаний в области ИКТР.

Чтобы в полной мере воспользоваться услугами, предоставляемыми AVA и e-Co Hub, зарегистрируйтесь по следующему адресу: http://www.unapcict.org/join_form

Серия модулей Академии ИКТ для лидеров государственного управления

Анг Пенг Хва

Модуль 5: Управление использованием Интернета

Перевод с английского
под редакцией А.С. Бакенова

Бумага офсетная. Гарнитура Arial
7,91 печ. л. Тираж: 200 экз.

Верстка осуществлена М. Усубалиевой

Дизайн и разметка: Scandinavian Publishing Co., Ltd and studio triangle

Отпечатано в Национальном центре информационных технологий Кыргызской Республики и ОсОО ИК «Zest-Asia»