А.М. Кузьмин, кандидат экономических наук, ст. преподаватель кафедры Глобальных информационных процессов и ресурсов МГИМО;
e-mail: akuzmin82@mail.ru

КОНТРОЛЬ ИНФОРМАЦИОННЫХ ПОТОКОВ В МЕДИАСРЕДЕ КАК ВАЖНЕЙШАЯ ФУНКЦИЯ ИНФОРМАЦИОННО-УПРАВЛЯЮЩЕЙ СИСТЕМЫ

В статье исследуется проблема регулирования информационных потоков в медиасреде России. Автор обобщает и систематизирует существующий опыт зарубежных стран в решении данной проблемы и предлагает различные подходы и механизмы осуществления функции контроля в российской медиасреде и, в частности, сети Интернет. Данные механизмы тесно увязываются с другой важнейшей функцией — мотивацией. В статье также предлагаются возможные субъекты управления, которые могут осуществлять функцию контроля в российской медиасреде со стороны государственного и частного сектора.

Ключевые слова: *информационные потоки, контроль за информационными потоками, медиасреда, СМИ и Интернет, информационно-управляющая система.*

In this article the issue of information flows regulation in Russia's media-area is examined. The author does the research, summers up and systematizes the practice of foreign countries in solving this problem, and suggests various approaches and mechanisms of control function realization in foundation of mechanism to manage the information flows in form of information-managing system, that is to be the connecting-link through the various Russia's media-area and Russian sector of Internet. These mechanisms are tightly connected with another important function — motivation. Possible subjects of management are also offered, which could execute control function in Russia's media-area from public and private sector.

Key words: *information flows, information flows control, media-area, mass media & Internet, information-managing system.*

Для эффективной реализации мер по регулированию информационных потоков необходим системный подход к решению проблемы управления данными потоками. Связующим звеном между различными институтами российского общества, на наш взгляд, должна стать Информационно-управляющая система российской медиасреды, главной функцией которой является регулирование информационных потоков в медиасреде и обеспечение управляемости процесса сбора, обработки, подачи и хранения информации в соответствии с интересами общества.

Элементы информационно-управляющей системы должны выполнять основные функции управления, которые заключаются в:

— планировании;
— мотивации;
— организации;
— координации;
— контроле (обратная связь) [Латфуллин, 2004, с. 20].

В данной статье автор рассматривает одну из сложнейших и важных функций системы — контроль. Целью функции *контроля* является обеспечение так называемой "свободы от информации" граждан. На сегодняшний день механизм контроля в отечественной медиасреде развит недостаточно глубоко.

Особую сложность представляет собой выполнение функции контроля в сети Интернет. В развитых странах контроль за соблюдением вредности, непристойности или незаконности информации в сети Интернет осуществляется по принципу саморегулирования в результате сотрудничества провайдеров и создателей интернет-СМИ. И хотя решения, принятые подобными гражданскими институтами, носят рекомендательный характер, существенным мотивом к их исполнению служит угроза изоляции сообщества или сети, не соблюдающей "правила игры". Подобные организации или комитеты могут быть созданы в России в рамках Совета по реализации информационной политики.

При этом, учитывая культурные, исторические и политические особенности нашей страны, нельзя недооценивать роль государства в решении данного вопроса с учетом новых вызовов глобального информационного общества. И самым сложным вопросом управления информационными потоками в настоящее время является контроль или цензура в сети Интернет.

На сегодняшний день в мире сложились различные подходы к решению данной проблемы, которые могут быть полезны и в российской практике.

Существует несколько способов осуществления цензуры, и используются они в контрольных точках в рамках архитектуры Интернета.

Эти контрольные точки включают исходное сообщение, исходящего провайдера, конечного провайдера и конечное сообщение или конечного пользователя [Zittrain, 2003, p. 12].

Способы, применяемые для контроля этих параметров, включают:

— прямые указания по контенту: что можно отправлять и к чему может быть предоставлен доступ;

— требования по установке фильтров и других технических средств блокирования потоков данных.

Методы контроля за информационными потоками тесно связаны с функцией *мотивации*, которая подразумевает применение разли-

ченных стимулов. В мировой практике применяются различные режимы лицензирования форм выражения мнения, передачи и приема информации:

— режимы ответственности для источников сообщений и провайдеров;

— ответственность за оскорбление и клевету;

— режимы защиты авторского права и интеллектуальной собственности и пр.

Эти способы могут использоваться вместе или по отдельности в зависимости от ситуации.

При использовании указанных выше способов потоки данных контролируются во имя соблюдения приличий, безопасности и морали. Фильтры могут быть поставлены на уровне провайдера получателя для блокировки доступа пользователя к информации, которая считается вредной. Людей можно заставить использовать фильтры в пределах Интернет-кафе или публичных библиотек. Желающие выразить свое мнение могут подпадать под действие законов о клевете, которые, как правило, требуют идентификации пользователя и, следовательно, некоторых форм лицензирования поставщиков интернет-услуг.

Лицензирование провайдеров может сделать их ответственными за контент, хостинг которого они осуществляют. И, наконец, от провайдеров могут потребовать удаления хостируемого контента и разглашения информации о человеке, поместившем конкретный вызывающий сомнение контент.

Многие, если не все, из этих мер можно применять на основании закона об охране интеллектуальной собственности.

Теперь возникает вопрос, кто именно должен осуществлять функцию контроля за информационными потоками?

В мировой практике органы, которым поручено осуществлять надзор за процессом регулирования, могут быть самыми разными: в одних странах это правительственные департаменты, в других — регулятивные органы, в третьих — независимые организации. Правительственные департаменты функционируют в Швейцарии (там полиция для блокировки контента, пропагандирующего расизм, направляет письма непосредственно провайдерам), в Италии (комитет национальной безопасности и министерство связи), в Лаосе (комитет, в состав которого входят несколько министерств, определяет порядок работы пользователей Интернет) и в Тунисе (Тунисское интернет-агентство, входящее в состав Министерства связи). Регулятивные органы отвечают за контент в Австралии (Австралийское управление вещания обладает правом издавать распоряжения о прекращении работы поставщиков интернет-услуг на территории Австралии), в Индии (Комиссия по связи Индии),

Южной Корее (Комитет по этике информационных коммуникаций имеет право удалять контент без решения суда) и Венгрии (Национальный совет по радио и телевидению) [Хосейн, 2008, с. 30].

В состав регулятивных органов могут входить члены правительства, а сами регулятивные органы могут контролироваться правительством. В числе стран с подобной моделью управления Великобритания, где действует Фонд контроля над Интернетом (Internet Watch Foundation, IWF) — организация, созданная изначально для противодействия регулированию; Венгрия, в которой существует Ассоциация контент провайдеров (Content Providers' Association), первоначально аналогичная IWF, но ставшая более проблематичной из за предложений по установке антипорнографических фильтров, удалению "вульгарных и агрессивных высказываний" и всего, что направлено против "хорошего вкуса", а также из-за рекомендаций в отношении потенциального нарушения авторского права. Однако здесь проблема в том, что все эти полномочия ограничены географическими границами.

При формировании элемента контроля информационно-управляющей системы необходимо ответить на вопрос, с какой целью он осуществляется.

Цели контроля или цензуры могут быть самыми разными. Цензура вводится во многих странах для:

— защиты интересов национальной безопасности (Китай, Сингапур);

— защиты "общественной нравственности" путем регулирования ошибочных или злонамеренных слухов или тревожных новостей, целью которых становится нарушение общественного спокойствия, вселение страха в людей или нанесение вреда государственным интересам (Египет)[1].

Среди других целей можно перечислить примеры Перу, где наложен запрет на информацию, которая "противоречит морали или добрым традициям". Законы Марокко использовались для ареста редакторов газет за нанесение оскорбления королю и публикацию коммюнике Исламской группы.

Австралия регулирует контент, который считается неподходящим для несовершеннолетних. Китай также фильтрует ряд порнографических сайтов. Индия цензурирует материалы, "носящие похотливый характер" или "вызывающие похотливые желания". Закрываются веб-сайты, пропагандирующие ненависть, клевету, оскорбления, азартные игры и расизм, насилие и терроризм, порнографию, включая детскую, и секс с элементами насилия.

[1] *Frankel G.* Egypt Muzzles Calls for Democracy // Washington Post. 2004. January 6. A01.

Помимо контента, описывающего инцест, педофилию, скотоложество и некрофилию, Сингапур регулирует пропаганду гомосексуализма.

Многие страны континентальной Европы запрещают контент, пропагандирующий расизм или ксенофобию. Совет Европы продвигает принятие гармонизирующих мер, призванных обеспечить признание всеми государствами—членами ЕС преступного характера подобных выступлений и предписывает удалять их с веб-сайтов государств—членов ЕС. Эти государства также разработали четкие законодательные нормы в отношении клеветы и оскорблений.

Пока правительство США, находясь под контролем Конституции и практики ее применения, более ограничено в вопросах регулирования свободы слова, возникают новые формы цензуры. Например, потребителей ограничивают "Условиями оказания услуг", которые принимают провайдеры, фактически ограничивая конституционные права пользователей: они разрешают им какие-то высказывания и действия, но при этом ограничивают свободу слова и доступа, которые на основании других документов являются абсолютно законными[2].

Таким образом, субъекты производства и частного сектора оказываются вовлеченными в процесс контроля за потоками данных.

Государственный сектор для эффективного осуществления функции контроля за информационными потоками должен тесно взаимодействовать с частным сектором.

Для защиты авторского права и интеллектуальной собственности в различных странах принимаются законы и утверждается практика.

В Бельгии в 2000 г. впервые в мире было введено отслеживание пользователей, работающих с приложениями "точка-точка": на основании "джентльменского соглашения" провайдеры стали предоставлять имена своих пользователей представителям музыкальной индустрии.

Гораздо дальше пошел закон об авторском праве в США. На основании "Закона об авторском праве в цифровом тысячелетии" (Digital Millenium Copyright Act, DMCA) от 1998 г. публикация информации о средствах, позволяющих обойти механизмы защиты авторского права, подлежит судебному преследованию. Закон предусматривает ответственность даже в том случае, когда люди, опубликовавшие подобный материал, находятся за пределами США. Так, в 2001 г. Дмитрий Скляров, российский программист, написавший программу, позволяющую обойти этот закон при пользовании Adobe eBooks, был арестован на собрании хакеров

[2] Committee to Protect Journalists. CPJ Delegation Meets with Moroccan Ambassador: Calls for Immediate Release of Jailed Editors. N.Y., 2003. P. 4.

в Лас-Вегасе, на котором он выступал с докладом о своем изобретении. История закончилась тем, что ему лично обвинение предъявлено не было, но оно было предъявлено московской компании "Элкомсофт", сотрудником которой он являлся. Суд присяжных оправдал "Элкомсофт", частично потому, что написание программ не является в России противозаконным делом.

Другой пример: 16 летний студент из Норвегии Йон Йоханссон написал программу DeCSS для обхода системы, защищающей коммерческие DVD, и был подвергнут штрафу со стороны Ассоциации американского кино опять же на основании вышеуказанного закона. Однако Ассоциация на этом не остановилась: она стала возбуждать дела против каждого, кто просто выходил по ссылке на эту программу. В числе пострадавших оказался и Эрик Корлей, редактор "2600: the Hacker Quarterly", который (наряду со многими другими пользователями Интернета) подключился к DeCSS с веб-сайта своего журнала.

Отдельные граждане и группы также могут иметь право на цензуру поведения других людей в отношении клеветы и оскорблений.

В ходе одного из исследований в Великобритании Правовая комиссия обнаружила, что некоторые поставщики интернет-услуг получали более сотни жалоб в год от адвокатов и рядовых граждан на якобы оскорбительные материалы, размещаемые или распространяемые через этих провайдеров. Большая часть писем приходила от адвокатов и содержала жалобы на веб-сайты, созданные недовольными потребителями. Комиссия была вынуждена признать, что лучшим решением для получателей этих писем было "удалить материал вне зависимости от общественных интересов и соответствия действительности". Такое решение было принято по причине неясного юридического статуса поставщиков интернет-услуг по британскому законодательству. Правовая комиссия выразила озабоченность тем, что группы граждан, организующие подобные кампании, являются первой "пострадавшей стороной" в подобной ситуации[3]. Этот правовой режим слишком близок к замораживанию свободы политического слова.

До тех пор пока поставщики интернет-услуг воспринимаются как "вторичные издатели" или как организации, отвечающие в определенной степени за хостируемый контент, они, скорее всего, могут быть привлечены к ответственности. Правовая комиссия считает, что одним из выходов из создавшейся ситуации является полное освобождение провайдеров от ответственности, как это сделано в США.

[3] Law Commission. Law Commission Report on Defamation and the Internet: A Preliminary Investigation. London: Law Commission of England and Wales, 2002. P. 25.

В качестве альтернативы следует подготовить более четкие инструкции по статусу поставщиков интернет-услуг как издателей, архивариусов или просто каналов передачи информации и ее носителей.

В делах, связанных с клеветой и оскорблениями, следует уделять больше внимания вопросам юрисдикции. Все чаще контент-провайдеры и поставщики интернет-услуг в разных странах мира подвергаются риску быть признанными юридически ответственными за клевету и оскорбления.

Такой случай произошел в Австралии, когда суды этой страны признали, что дело о клевете против компании "Доу Джоунс" (Dow Jones), расположенной в Нью-Йорке, находится в их юрисдикции. Это дело стало прецедентом для канадского суда, который недавно принял аналогичное решение. Постановление гласило, что статья, опубликованная в Washington Post (в то время как человек жил и работал в Кении), может быть предметом слушаний в канадском суде несколько лет спустя, поскольку газета должна была "предусмотреть, что эта история будет следовать за истцом, независимо от места его проживания"[4].

Европейский Союз, работающий над разрешением коллизионного права в сфере оскорблений, считает, что любой человек, помещающий информацию в Интернете, будет отвечать по закону о клевете, принятому каждым государством—членом ЕС[5].

Другой суд в Канаде признал, что анонимная клевета "носит более рискованный характер, так как в нее легче поверить", и, следовательно, тот, кто клевещет на других с использованием Интернета, должен нести большую ответственность за причиненный ущерб[6].

Недостаточно корректное рассмотрение данной ситуации может привести к тому, что цензура будет введена как орудие правового устрашения. Это может произойти в результате запугивания поставщиков интернет-услуг или отдельных людей, лимитируя их право на свободу слова.

Законы о клевете используются также и правительствами. В некоторых странах клевета является преступлением. Правительство Сингапура боролось со своими оппонентами, подавая на них в суд за клевету.

Закон о клевете в штате Джорджия используется как щит против расследований СМИ и имеет в своем распоряжении граждан-

---

[4] *Geist M.* Web Decision extends long arm of Ontario law // The Toronto Star. 2004. February 16. P. 25.

[5] Article 19. Press Release: ARTICLE 19 concerned that proposed Rome II regulations pose threat to Internet publishers' freedom of expression. January 14, 2004. P. 3.

[6] *Brethour P.* Net Libel Open to Higher Damages: Judge says anonymous Web postings can magnify impact of defamatory comments // Globe and Mail. 2004. February 11. P. 15.

ские и уголовные наказания, а правительство предлагает ввести более продолжительные сроки наказания за клевету на государственных официальных лиц.

Согласно статье 19 Глобальной кампании за свободу выражения мнений:

— клевета должна быть исключена из числа уголовно наказуемых преступлений;

— государственным органам, включая органы законодательной, исполнительной или судебной власти, должно быть запрещено подавать иски о клевете;

— высказывание мнения, в отличие от фактических обвинений, не должно служить основанием для обвинений в клевете;

— провайдеры интернет-услуг и другие организации, выполняющие аналогичные функции, должны быть ограждены от ответственности;

— должны быть предусмотрены меры защиты обоснованных публикаций;

— наказание должно быть адекватно нанесенному ущербу, а за нанесение нематериального ущерба должен быть установлен верхний предел наказания[7].

Таким образом, в мире сложилась достаточно обширная практика применения мер по контролю за информационными потоками в медиасреде и, в частности, в сети Интернет. При формировании контроля как элемента информационно-управляющей системы должна быть использована лучшая практика в первую очередь развитых стран, вплотную столкнувшихся с данной проблемой на ранних стадиях формирования информационного общества, которое в России находится на начальном этапе становления. При этом необходимо подчеркнуть тесную взаимосвязь функции контроля с функцией мотивации (положительной и отрицательной), которые должны быть тесно взаимосвязаны в информационно-управляющей системе.

Список литературы

Хосейн Г. Ограничение и сдерживание глобальных потоков данных. М.: МЦБС, 2008.

Организационное поведение: Учебник для вузов / Под ред. Г.Р. Латфуллина, О.Н. Громовой. СПб.: Питер, 2004.

Zittrain J. Internet Points of Control // Boston College Law Review 43. 2003. N 1.

Поступила в редакцию
14.01.2010

[7] Article 19. Harsh Georgian Defamation Laws Must Be Amended. London: The Global Campaign for Free Expression, 2004. P. 12.