§3 ПОЛИТИЧЕСКИЕ КОММУНИКАЦИИ

Кульназарова А.В.

ОГРАНИЧЕНИЕ ДОСТУПА К КОНТЕНТУ В РУНЕТЕ: ТЕКУЩАЯ СИТУАЦИЯ И ПЕРСПЕКТИВЫ

Аннотация. *В данной статье представлены результаты мониторинга Единого реестра запрещенных сайтов: выявлена динамика внесения сайтов в реестр, определены основные категории (тематика) блокируемого контента, а также исследована законодательная база ограничений доступа к интернет-ресурсам. Произведен анализ популярности сервисов «обхода» блокировок, значительно снижающих эффективность и целесообразность существования Реестра. Выявляются основные проблемы и тенденции в ограничении доступа в Рунете, а также возможные сценарии дальнейшего государственного контроля над интернет-пространством. Целью исследования является выявление динамики, закономерностей и перспектив ограничения доступа к контенту в Рунете. Для достижения данной цели был осуществлен мониторинг Единого реестра запрещенных сайтов, классификация запрещенного контента, качественный и статистический анализ данных. Всего обработано 4132 сайтов за период 01.02.2014-30.06.2016. В результате проведенного исследования автор приходит к следующим выводам: тематика блокируемых сайтов совпадает с наиболее острыми общественно-политическими проблемами (терроризм, исламизм, проблемы Украины и Крыма и т.д.); подавляющая часть заблокированных сайтов принадлежит или посвящена деятельности запрещенных в России националистических, террористических и экстремистских организаций, тогда как на оппозиционные ресурсы приходится лишь 11% сайтов. С учетом существующих тенденций можно предположить дальнейшее усиление контроля над интернет-средой с подготовкой соответствующей законодательной базы и внедрением новых технологий, которые препятствовали бы несанкционированному доступу к запрещенным материалам.*

DOI: 10.7256/1812-8696.2016.8.19971

Ключевые слова: *Единый реестр, запрещенные сайты, ограничение доступа, интернет-контент, блокировка, интернет-технологии, государственное регулирование, экстремистские материалы, интернет-коммуникации, оппозиционные сайты.*

Abstract. *This article presents the results of monitoring of the Unified Register of the banned websites. The author determines the dynamics of placing websites on the register, defines the main categories (themes) of the blocked content, as well as examines the legislative base of restriction of access to the Internet sources. An analysis is conducted on the popularity of the services of circumventing of the blocks that significantly lower the efficiency and the point of existence of the Register. The author determines the main problems and trends in the limitation of the access in the Russian Internet, as well as the possible scenarios of further government control over the Internet. The goal of this research is to determine the dynamics, regularities, and prospects of restriction of access to the Runet content. In order to achieve the set goal, the author conducted monitoring of the Unified Register of banned websites, classification of the prohibited content, as well as qualitative and statistical analysis of the data. The conclusion is made that the theme of the blocked websites matches the most acute sociopolitical problems (terrorism, Islamism, Ukrainian and Crimean questions, etc.); the majority of the blocked websites belongs or dedicated to the activity of the prohibited in Russia nationalistic, terrorist, and extremist organizations, whole the portion of the oppositional resources comprises just 11% of the websites. Considering the existing trends, we can suggest the further strengthening of control over the Internet environment with preparation of the corresponding legislative base and implementation of new techniques, which would hinder the unauthorized access to the banned materials.*

Key words: *extremist materials, government regulation, Internet technologies, blocking, Internet content, restricting access, banned websites, Unified Register, Internet communication, oppositional websites.*

Массовые протесты в России и напряженность обстановки на международной арене стали важнейшим стимулом для активизации законотворческой деятельности в области регулирования Интернета. Законы, регулирующие интернет, принимались как отдельно, так и в пакете с другими законами – речь идет об антиэкстремистском и антитеррористическом законодательстве. Факт того, что законы, регулирующие интернет-пространство, принимаются наряду с законами, направленными на борьбу с терроризмом и экстремизмом, свидетельствует об осознании властями потенциальных угроз для общества, исходящих из неконтролируемой интернет-коммуникации.

По мере развития информационных технологий применение не предназначенной для регулирования этой области правовой базы становится все менее эффективным, что приводит к совершенствованию и расширению законодательства. Однако перманентно наблюдается устаревание законодательства и несоответствие его уровню технологического развития и новейшим реалиям, поскольку принятие и вступление закона в силу усложняется длительными бюрократическими процедурами, а технологический прогресс только ускоряется.

Как и во многих других государствах, Интернет воспринимается как неподконтрольный источник нежелательной информации. В России к активному регулированию интернета государство приступило лишь в 2011-2012 гг. Стимулом к этому являются изменения общественных настроений и в увеличении роли интернет-коммуникаций в различных политических движениях, мероприятиях и агитации. В результате был принят ряд законов, устанавливающих порядок ограничения доступа к сайтам и удаления информации из поисковой выдачи, локализацию персональных данных, регистрацию блогеров, идентификацию пользователей в публичных сетях Wi-Fi, а также «антипиратские» законы.

Систематическая блокировка сайтов стала возможна с введением «Единого реестра запрещенных сайтов» Федеральным законом № 139-

DOI: 10.7256/1812-8696.2016.8.19971

ФЗ от 2012 г.[2] Первоначально основанием для блокировки являлось наличие на сайте социально вредного контента, с принятием Федерального закона № 398-ФЗ от 2013 г.[3] внесудебной блокировке подвергается и политический контент (призывы к участию в несанкционированных массовых мероприятиях, беспорядках, экстремистской деятельности). Ранее механизмом ограничения было внесение в список экстремистских материалов. Также последовали блокировки нескольких известных онлайн-СМИ, десятков блогов в ЖЖ, сообществ в социальных сетях. Однако ресурсы такого рода составляют меньшинство в списке запрещенных сайтов.

Процедуры блокировки различаются в зависимости от ведомства, принимающего решения о внесении материала в список запрещенных. В случае если это решение принимается Генпрокуратурой, то процедура блокировки – внесудебная, т.е. осуществляется без проведения экспертизы, после получения уведомления от федеральных или региональных госорганов, органов местного самоуправления, организаций и граждан. Далее решение о блокировке ресурса направляется в Роскомнадзор, по требованию которого операторы связи должны незамедлительно ограничить доступ к ресурсу. Данный закон не предусматривает обжалования блокировки. Однако, автор материала или владелец сайта может беспрепятственно дублировать контент на других ресурсах, а пользователи – применять технологии для получения доступа к блокированному контенту. На данный момент подобные действия не имеют правовых последствий.

Полный перечень запрещенных сайтов, формально являясь открытым, недоступен для ознакомления рядовыми пользователями. Государственный сайт Роскомнадзора [9] позволяет проверить, находится ли ресурс в реестре, но увидеть полную картину можно лишь при использовании программных средств, также полный и актуальный реестр предоставляется операторам связи. Безусловно, это создает благоприятную почву для злоупотреблений и манипуляций при добавлении Интернет-ресурса в реестр. В Рунете неофициальным источником информации о содержании реестра являются два проекта: «Роскомсвобода» и «Антизапрет. инфо». Проекты предоставляют статистическую информацию по блокировкам, извлеченную из официальных источников, и представленную в наглядном для пользователей виде. Для этого применяются программные решения с открытым исходным кодом, что позволяет перепроверить данные, полученные при помощи этих технологий.

Решение о незаконности Интернет-ресурса принимает компетентный государственный орган. Цель ограничения доступа к контенту или его удаления должна быть законной и служить интересам общества. В России данные в Реестр запрещенных сайтов вносятся следующими ведомствами:

– Роскомнадзор;
– Роспотребнадзор;
– Генпрокуратура;
– Федеральная налоговая служба;
– ФСКН;
– Суды (в т.ч. Мосгорсуд).

Весь блокируемый контент можно разделить на три крупные сферы:

– Социальная (материалы, содержащие социально вредную информацию, например, о способах суицида, наркотиках, порталы азартных игр и т.д.).
– Политическая (ресурсы оппозиционного, экстремистского характера);
– Экономическая (сайты, нарушающие права на интеллектуальную собственность).

Ресурсы с политическим контентом блокируются в основном по решению Генеральной прокуратуры, от общего числа ресурсов в Реестре они составляют ~ 5%. Среди них было выделено 5 тематических групп:

– Исламистские ресурсы;
– Проукраинские сайты;
– Оппозиционные ресурсы;
– Экстремистские, сепаратистские сайты.

Соотнесение сайта к той или иной тематике базируется на ключевых словах в URL сайта или в сниппете (кратком описании содержания) в поисковой выдаче. Таким образом удалось распознать 80% (3185) сайтов, внесенных в Реестр Генпрокуратурой по 30.06.2016. Часть заблокированных материалов распознать не представляется возможным ввиду отсутствия описаний

DOI: 10.7256/1812-8696.2016.8.19971

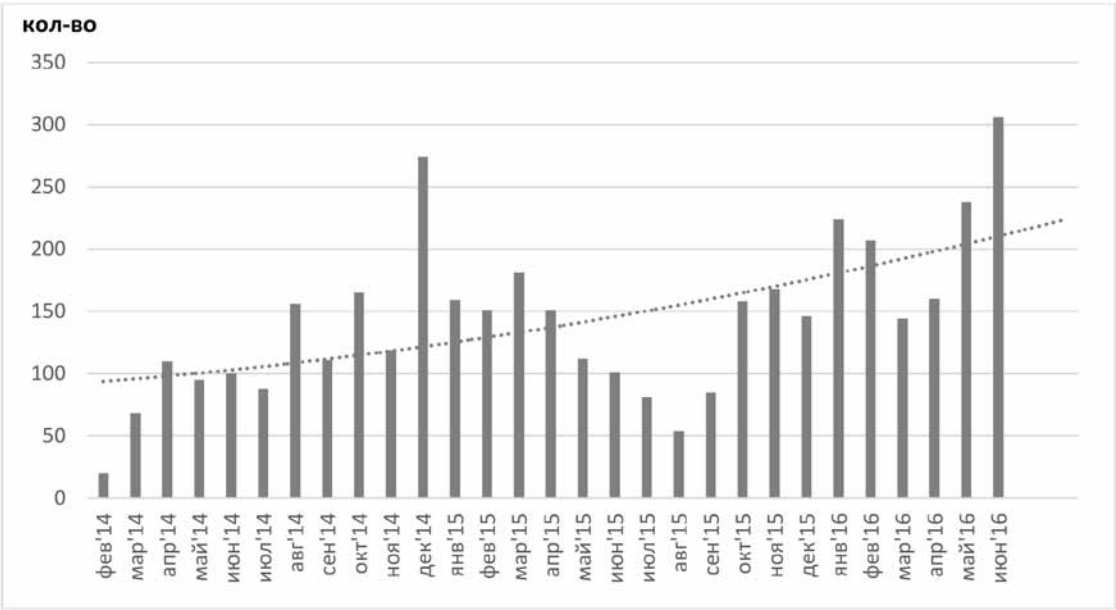

Рис. 1. Динамика блокировок интернет-сайтов

страниц в поисковой системе, кешированных копий, упоминаний в социальных сетях и ключевых слов в URL-адресах. Помимо собственно сайтов, блокируется видео и аудиоконтент Youtube и различных файлообменников.

– Перечень ключевых слов для URL по каждой из тематик следующий:
– Категория «исламизм» определяется следующими тегами (и их вариациями): hizb-ut-tahrir, islamdin, khilafa, golosislama, jihad, halifat, igil, islamic-world, hunafa (превалируют сайты, связанные с «Хизб ут тахрир»).
– Экстремизм, сепаратизм: kavkazcenter, freecaucasus, daymohk, sibpower, shturmnovosti, vdagestan, destroyrussia, ma nezhka (основной массив запрещенных материалов приходится на популярный портал «Кавказ центр»). И хотя проблематично провести четкую грань между категориями «исламизм» и «экстремизм/сепаратизм», ко второй относятся все ресурсы, распространяющие идеи против территориальной целостности Российской Федерации (в первую очередь, они связаны с Кавказом, но сюда же относятся сайты с требованиями федерализации Сибири и т.п.).
– В категорию «Оппозиционные издания, блоги» отнесены: grani.ru, navalny, kasparov, ej, golossgalerki, censoru.net, ros-boloto, также блоги в Живом Журнале, координирующие сайты оппозиционных массовых мероприятий, видеозаписи оппозиционных митингов.
– Ключевые слова «проукраинской» категории: ua, yarosh, azov, pravyj sektor, right sector, ps-zahid, sockraina, krym, sich, banderivec, unaunso. В эту же категорию отнесены публикации «Памятка потребителям при посещении территории Крыма», блоги украинских общественных деятелей и др.

Динамика блокировок выглядит следующим образом (рис. 1).

На данном графике видны несколько периодов резкого увеличения числа блокированных сайтов: декабрь 2014, январь-февраль 2016, май-июнь 2016. Снижение активности блокировок приходится на 3-й квартал 2015 года, однако общий тренд показывает устойчивое движение к усилению контроля над интернет-пространством.

Динамика блокирования сайтов по отдельным тематикам представлена на рис. 2. На графике заметно существенное увеличение числа заблокированных сайтов исламистской тематики во второй половине 2015 года с одновременным снижением количества по оппозиционной тематике. Предполагается, что связано это с актуализацией проблем Ближнего Востока (сентябрьская спецоперация в Сирии) и терро-

DOI: 10.7256/1812-8696.2016.8.19971

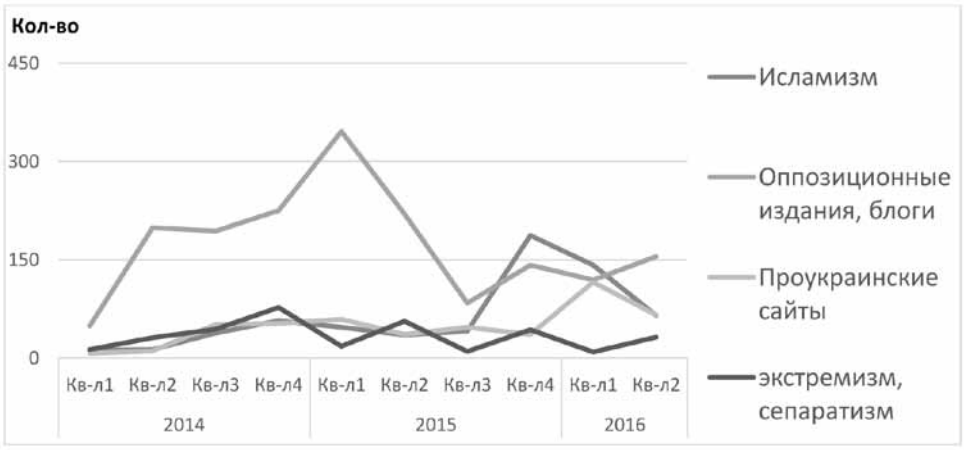

Рис. 2. Динамика блокировок отдельных тематик (поквартальная)

ристическими угрозами (события конца 2015 года, ответственность за которые взяла на себя группировка ИГИЛ). Пик блокировок оппозиционных ресурсов хронологически совпадает с убийством Б. Немцова и соответственно увеличением числа оппозиционных публикаций.

Количественное распределение по категориям показывает, что основной массив – 42% составляют оппозиционные сайты. Как уже было сказано, значительную часть в реестре составляют копии одних и тех же интернет-ресурсов. Однако, вычленив из массива данных неповторяющиеся значения, мы получаем иное процентное соотношение: оппозиционные ресурсы составляют лишь 11% заблокированных материалов, а наибольшее внимание уделяется исламистским и проукраинским материалам (39% и 22% соответственно).

Таблица 1

Количественное распределение по категориям

Категория	Весь реестр	Без «зеркал»
Unknown	23%	19%
Исламизм	20%	39%
Оппозиционные издания, блоги	42%	11%
Проукраинские сайты	12%	22%
Экстремизм, сепаратизм	3%	8%

Блокировки направлены в основном против распространения идей, угрожающих территориальной целостности РФ и противоречащие официальной внешнеполитической позиции – запрещены сотни различных сайтов подобной направленности. Тогда как среди оппозиционных лишь несколько наиболее известных ресурсов («Грани.ру», «Каспаров.ру», «Еж.ру», некоторые блоги ЖЖ, в том числе блог А. Навального) подвергаются систематическим блокировкам. В проанализированном перечне сайтов более 70% составляют так называемые «зеркала» и практически идентичные сайты. Значительный массив заблокированных сайтов (более 600) составляют копии издания Грани.ру. Периодически проводится мониторинг и блокировка «зеркал», целесообразность которой сомнительна, т.к. успешно функционирует ряд аналогичных ресурсов и страниц в соц. сетях. Чаще всего блокированию подвергаются сайты исламистской тематики, а также ресурсы о независимости северокавказских республик. Ограничивается доступ и к украинским новостным и националистическим сайтам.

Соотношение блокировок доменов и отдельных страниц составляет 54% доменов к 46% страниц (с учетом сайтов-зеркал) и 19% доменов к 71% страниц – без учета «зеркал». Блокировка страниц требует «точечной» работы: в Реестре имеется множество сайтов с десятками заблокированных страниц, но работающим доменом. Это свидетельствует о некоторой степени гибкости в ограничении доступа к интернет-ресурсам. С другой стороны, имеются случаи блокировки и домена, и нескольких страниц на нем уже после внесения всего ресурса в Реестр, что не может не вызывать вопросов о целесообразности этой деятельности. Пример

DOI: 10.7256/1812-8696.2016.8.19971

таких блокировок – портал kavkazcenter.com. По оппозиционной категории имеется лишь 11 полностью заблокированных доменов, остальное – отдельные публикации, которые, однако, с легкостью копируются на другие сайты, что вызывает необходимость вносить в Реестр новую запись.

С использованием корреляционного анализа были выявлены некоторые зависимости между блокировкой сайтов по тематике. Например, между категориями «Исламизм» и «Проукраинские ресурсы», коэффициент корреляции равен 0,43; это связано с тем, что обе темы (терроризм, конфликт в Украине) практически одновременно внесены в общественную повестку дня. Между «Оппозиционные издания, блоги» и «Проукраинские сайты» коэффициент корреляции составляет 0,39. Данную зависимость можно объяснить тем, что многие оппозиционные издания занимали проукраинскую позицию, отличающуюся от позиции официальной власти. Тем не менее, эти значения коэффициента считаются слабыми и объясняются: а) одновременностью нескольких происходящих политических процессов; б) многонаправленностью работы Роскомнадзора и других контролирующих органов.

Подводя итог, отметим, что регулирование интернета имеет несколько направлений, по каждому из которых государство проявляет большую или меньшую степень вмешательства. Приоритетом в регулировании интернет-среды является обеспечение государственной безопасности (об этом свидетельствует принятие законов в «антитеррористическом» пакете, борьба с экстремизмом, противодействие информационным угрозам и т.д.).

И хотя наблюдается явная тенденция усиления контроля над интернетом, современные технологии позволяют «обходить» блокировки, а ограничение доступа влияет лишь на пользователей с низким уровнем компьютерной грамотности. Также распространено дублирование контента на сторонних ресурсах, что снижает эффективность законодательных мер и вынуждает власть искать новые способы ограничения информации. Поэтому эффективность предпринимаемых мер остается невысокой. Существует множество средств «обхода» блокировок, и они постепенно набирают популярность среди интернет-пользователей: по данным сервиса «Яндекс.Wordstat» [11], если в 2014 году количество запросов, содержащих ключевые слова «обход блокировки сайта», составляло ~7000 в месяц, то в 2016 это количество составляет более 70 000 запросов в месяц.

Таким образом, можно выделить две существенные трудности в области контроля со стороны государства: с одной стороны, это простота дублирования информации, с другой стороны, применение технических средств, позволяющих обходить фильтрацию, блокировку контента и скрывать активность пользователя в интернете.

К этим средствам относятся:

– Использование альтернативных доменных имен для получения доступа к блокированной информации;
– Использование стороннего веб-сайта для доступа к заблокированной информации (RSS-агрегаторы, онлайн-переводчики, фильтры сжимания контента и т.д.) – формально пользователь подключается к третьему сайту, доступ к которому разрешен провайдером; а к заблокированному ресурсу подключается уже сторонний сервер, действия которого провайдер отслеживать не может. Таким образом, контент становится доступным конечному пользователю.
– Использование шлюзов электронной почты, с целью получения блокированных веб-страниц через электронную почту.
– Использование анонимайзеров (программное обеспечение туннелирования и шифрования трафика, подключение через прокси-сервера, например, браузер Tor).

Кроме того, крупные интернет-ресурсы внедряют все более совершенные технологии шифрования и передачи данных, что затрудняет применение ограничительных мер. Постоянная модернизация технических средств и упрощение их использования приводят к нивелированию усилий по ограничению доступа к информации. И хотя не существует статистических данных о том, какое количество пользователей получают доступ непосредственно к указанным типам запрещенных сайтов, судить можно по растущей популярности всевозможных анонимайзеров

DOI: 10.7256/1812-8696.2016.8.19971

(по данным Google Trends, после введения запретов имеет место явный всплеск пользовательского интереса к такого рода инструментам [10]). Также по данным этого сервиса, с 2012 года наблюдается резкое усиление интереса к анонимному браузеру TOR (функционирующему еще с 2001 года).

Блокировки сайтов сопровождаются ограничением доступа к соответствующему контенту в социальных сетях. Однако такие ограничения не отражены ни в Реестре, ни в перечне экстремистских материалов. Социальные сети по причине их доступности, простоты подачи информации и широкому охвату аудитории разных возрастов и категорий, способны оказывать мощное влияние на общественное сознание, могут применяться для прямого коммуникационного воздействия на пользователей. Поэтому вполне логично, что блокировки веб-сайтов сопровождаются ограничением к страницам в социальных сетях, но, тем не менее, и эти ограничения легко обойти при помощи новых технологий и использования новых коммуникационных платформ. Например, мессенджеры позволяют создавать паблик-чаты и осуществлять прямую коммуникацию, при этом используя новейшие технологии шифрования данных. Помимо ограничения доступа к сайтам по закону, практикуется и «самоцензура» в социальных сетях – администрация социальных сетей блокирует аккаунты по своему усмотрению, без официального запроса властей. Подобная практика встречается в социальной сети Facebook. Учащение блокировок (в первую очередь, оппозиционно настроенных пользователей и сообществ) отмечено с декабря 2014 года [6]; недовольство этой ситуацией высказали известные общественные деятели и блогеры в петиции [12], опубликованной на ресурсе Change.org.

Подобную «антиоппозиционную» модерацию можно объяснить тем, что руководству социальной сети выгоднее сотрудничать с властями государств, поддерживая их политику, чем провоцировать местные власти на блокировку ресурса (как в Китае, Иране и др. странах), что приводит к потере национальных рынков.

Итак, по результатам проведенного анализа можно прийти к следующим выводам:

1. Имеется тенденция к усилению контроля над интернет-средой: об этом говорит, с одной стороны, постепенное увеличение количества блокированных сайтов, с другой – вновь появляющиеся законодательные инициативы в этой области. Однако стоит отметить, что политический контент составляет незначительную часть материалов, внесенных в реестр.
2. В реестре большую часть составляют «зеркала», т.е. отслеживается в основном ограниченное количество популярных ресурсов (возможно, автоматически) – только четверть из всех запрещенных сайтов являются уникальными ресурсами, остальное – копии (т.е. борьба с ветряными мельницами).
3. Тематика блокируемых сайтов совпадает с наиболее острыми общественно-политическими проблемами (терроризм – группировки и идеология, исламизм, проблемы Украины и Крыма – темы, освещаемые и в других СМИ; оппозиционные движения, сепаратизм – темы, не находящие существенного освещения в традиционных СМИ).
4. Подавляющая часть заблокированных сайтов принадлежит или посвящена деятельности запрещенных в России националистических, террористических и экстремистских организаций (Хизб ут Тахрир, ИГИЛ, Правый сектор, УНА-УНСО, Всеукраинская организация «Тризуб» имени Степана Бандеры). Ограничение такого рода необходимо не только для недопущения распространения социально опасных идей, но и для ограничения возможностей вербовки новых членов в эти организации.
5. На оппозиционные ресурсы приходится 11% заблокированных сайтов (не считая копий). Однако наибольший резонанс в Сети вызывают именно блокировки материалов этой категории. Чаще подвергаются блокировке материалы, представляющие большую идеологическую опасность – вышеуказанные экстремистские и исламистские ресурсы.
6. Существенной проблемой является то, что на применяемые методы контроля доступа находятся технические средства, позволяющие обходить фильтрацию, блокировку кон-

DOI: 10.7256/1812-8696.2016.8.19971

тента и скрывать активность пользователя в интернете. Все большее количество пользователей применяют средства обхода ограничений доступа (об этом свидетельствует статистика поисковых запросов), что сводит на нет работу ведомств по борьбе с распространением запрещенной информации.

Таким образом, с учетом существующих тенденций можно предположить дальнейшее усиление контроля над интернет-средой с подготовкой соответствующей законодательной базы и внедрением новых технологий, которые препятствовали бы несанкционированному доступу к запрещенным материалам. Возможные сценарии развития государственного контроля в Интернете, по нашему мнению, таковы:

1. Усиление контроля по китайскому примеру: постепенное вытеснение нежелательных ресурсов из доменных зон .ru и .рф; внедрение единой государственной поисковой системы; установка глобальной системы фильтрации контента в отечественном сегменте Интернета. Однако подобные меры, во-первых, потребуют значительных финансовых, материальных и временных затрат, во-вторых, могут вызвать негативную реакцию со стороны общественности в силу сформированных потребительских и пользовательских привычек. Предпосылками к возможной реализации данного сценария являются нововведения в информационном законодательстве:
– ограничения по хранению и обработке данных (например, сервера иностранных ресурсов должны быть локализованы в России, данные о действиях интернет-пользователей должны храниться операторами связи и хостинг-провайдерами в течение полугода) [1];
– ограничение анонимности (введение персонализированного доступа в Интернет через публичные сети Wi-Fi [5]; обязательная регистрация в качестве СМИ блогеров с аудиторией более 3 тысяч подписчиков [4]);
– воздействие на поисковые системы (введение процедуры удаления результатов поисковой выдачи);
– создание списка запрещенных сайтов, внесение ресурса в который может осуществляться и без достаточных правовых оснований;
– сотрудничество государственных органов (ведомств, связанных с государственной безопасностью) с администрациями социальных сетей, вследствие чего упрощается доступ к данным пользовательской активности.
2. «Бюрократический» путь развития: дальнейшее ведение реестра запрещенных (или разрешенных) сайтов, которое, однако, не решает вышеуказанных проблем дублирования контента и обхода блокировок. Также к недостаткам этого сценария можно отнести затраты на обслуживание реестра и формализацию процесса блокирования (т.е. существует риск внесения сайтов в реестр без четких на то оснований, с целью предоставления отчетов и соблюдения показателей эффективности деятельности соответствующих государственных органов). Однако существование реестра может быть оправдано при условии технологического совершенствования ограничения доступа к контенту, а также при сочетании блокировки сайтов с оффлайн-воздействием (напр., административным) на распространителей этой информации, особенно той, которая касается социально опасных явлений. На данный момент имеется ряд прецедентов возбуждения уголовных дел по экстремистским статьям за публикации в социальных сетях: по данным центра «Сова» в 2015 году выросло количество и доля людей, получивших приговоры, связанные с реальным лишением свободы; 16 человек были приговорены к лишению свободы только «за слова», без совершения других преступных действий [7]. Наиболее распространенная мера наказания – штрафы в размере от 6 до 250 тысяч рублей.
3. Либерализация: отказ от идеологического и политического контроля в интернет-пространстве, но с внедрением законодательных механизмов защиты экономических интересов (напр., правообладателей) и прав человека (напр., защита персональных данных). Недостатком такого подхода является неподконтрольность коммуникаций и, следовательно, непредсказуемость их влияния на общественное мнение. Однако с учетом

DOI: 10.7256/1812-8696.2016.8.19971

текущей обстановки, реализация этого сценария в России маловероятна.

4. Маркетинговый подход: продвижение мнений, выгодных официальной власти, при помощи PR-технологий. В первую очередь, речь идет о создании контента, обладающего характеристиками «вирусного». В сети имеется множество способов рационального и эмоционального воздействия на пользователей при помощи фотографий, мемов, видеороликов, текстов различного содержания. Это необходимо делать целью формирования необходимого общественного мнения и нейтрализации негативных тенденций в нем Таким образом, достигается мягкое воздействие на общественное мнение. Такой подход требует создания соответствующей централизованной структуры и высокой степени профессионализма от специалистов, задействованных в этой деятельности. Стоит отметить, что в России предпринимались попытки подобного воздействия через коммуникационную работу в социальных сетях (например, организация работы «Агентства интернет-исследований», в чьи задачи входило размещение заказных комментариев и постов в социальных сетях) [8].

Наиболее вероятным сценарием развития представляется сочетание бюрократического и маркетингового подходов, поскольку они позволяют добиться относительного контроля, при этом не вызывая резко негативной критики со стороны общества. Необходимо беспрерывно улучшать технологическую и законодательную базу регулирования интернет-среды и совершенствовать применяемые социальные технологии. Однако, по нашему мнению, ограничению должна подлежать лишь социально-опасная информация, а не оппозиционные материалы, т.к. это противоречит нормам демократического общества и свободе слова.

БИБЛИОГРАФИЯ

1. Закон Российской Федерации «О внесении изменений в отдельные законодательные акты Российской Федерации в части уточнения порядка обработки персональных данных в информационно-телекоммуникационных сетях» от 21 июля 2014 № 242 // Российская газета. 2014 г. № 6435 (163).
2. Закон Российской Федерации «О внесении изменений в Федеральный закон «О защите детей от информации, причиняющей вред их здоровью и развитию» и отдельные законодательные акты Российской Федерации» от 11 июля 2012 года № 139 // Российская газета. 2012 г. № 5845 (172).
3. Закон Российской Федерации «О внесении изменений в Федеральный закон «Об информации, информационных технологиях и о защите информации»» от 20 декабря 2013 года № 398 // Российская газета. 2013 г. № 6271 (295).
4. Закон Российской Федерации «О внесении изменений в Федеральный закон «Об информации, информационных технологиях и о защите информации» и отдельные законодательные акты Российской Федерации по вопросам упорядочения обмена информацией с использованием информационно-телекоммуникационных сетей» от 5 мая 2014 № 97 // Российская газета. 7 мая 2014 г. № 6373 (101).
5. Постановление правительства Российской Федерации «О внесении изменений в некоторые акты Правительства Российской Федерации в связи с принятием Федерального закона «О внесении изменений в Федеральный закон «Об информации, информационных технологиях и о защите информации» и отдельные законодательные акты Российской Федерации по вопросам упорядочения обмена информацией с использованием информационно-телекоммуникационных сетей « от 31 июля 2014 г. № 758 // Собрание законодательства Российской Федерации. 11 августа 2014 г. № 32. Ст. 4525
6. Активисты России и Украины требуют от Facebook прекратить политические блокировки // Газета.ру URL: http://www.gazeta.ru/tech/news/2015/06/17/n_7296201.shtml (дата обращения: 01.07.2016)
7. Антиэкстремизм в виртуальной России в 2014–2015 годы //Аналитический центр СОВА. URL: http://www.sova-center.ru/racism-xenophobia/publications/2016/06/d34913 (дата обращения: 11.07.2016)
8. Где живут тролли. Как работают интернет-провокаторы в Санкт-Петербурге и кто ими заправляет // Новая газета URL: http://www.novayagazeta.ru/society/59903.html (дата обращения: 20.06.2016).
9. Единый реестр доменных имен, указателей страниц сайтов в сети «Интернет» и сетевых адресов, позволяющих идентифицировать сайты в сети «Интернет», содержащие информацию, распространение которой в Российской Федерации запрещено. URL: https://eais.rkn.gov.ru

DOI: 10.7256/1812-8696.2016.8.19971

10. Сервис Google Trends. URL: https://www.google.ru/trends/
11. Статистика поисковых запросов «Яндекс.Вордстат». URL: https://wordstat.yandex.ru
12. Stop political blocking on Facebook // Change.org URL: https://www.change.org/p/facebook-stop-political-blocking-on-facebook (дата обращения: 01.07.2016)

REFERENCES (TRANSLITERATED)

1. Zakon Rossiiskoi Federatsii «O vnesenii izmenenii v otdel'nye zakonodatel'nye akty Rossiiskoi Federatsii v chasti utochneniya poryadka obrabotki personal'nykh dannykh v informatsionno-telekommunikatsionnykh setyakh» ot 21 iyulya 2014 № 242 // Rossiiskaya gazeta. 2014 g. № 6435 (163).
2. Zakon Rossiiskoi Federatsii «O vnesenii izmenenii v Federal'nyi zakon «O zashchite detei ot informatsii, prichinyayushchei vred ikh zdorov'yu i razvitiyu» i otdel'nye zakonodatel'nye akty Rossiiskoi Federatsii» ot 11 iyulya 2012 goda № 139 // Rossiiskaya gazeta. 2012 g. № 5845 (172).
3. Zakon Rossiiskoi Federatsii «O vnesenii izmenenii v Federal'nyi zakon «Ob informatsii, informatsionnykh tekhnologiyakh i o zashchite informatsii»» ot 20 dekabrya 2013 goda № 398 // Rossiiskaya gazeta. 2013 g. № 6271 (295).
4. Zakon Rossiiskoi Federatsii «O vnesenii izmenenii v Federal'nyi zakon «Ob informatsii, informatsionnykh tekhnologiyakh i o zashchite informatsii» i otdel'nye zakonodatel'nye akty Rossiiskoi Federatsii po voprosam uporyadocheniya obmena informatsiei s ispol'zovaniem informatsionno-telekommunikatsionnykh setei» ot 5 maya 2014 № 97 // Rossiiskaya gazeta. 7 maya 2014 g. № 6373 (101).
5. Postanovlenie pravitel'stva Rossiiskoi Federatsii «O vnesenii izmenenii v nekotorye akty Pravitel'stva Rossiiskoi Federatsii v svyazi s prinyatiem Federal'nogo zakona «O vnesenii izmenenii v Federal'nyi zakon «Ob informatsii, informatsionnykh tekhnologiyakh i o zashchite informatsii» i otdel'nye zakonodatel'nye akty Rossiiskoi Federatsii po voprosam uporyadocheniya obmena informatsiei s ispol'zovaniem informatsionno-telekommunikatsionnykh setei « ot 31 iyulya 2014 g. № 758 // Sobranie zakonodatel'stva Rossiiskoi Federatsii. 11 avgusta 2014 g. № 32. St. 4525
6. Aktivisty Rossii i Ukrainy trebuyut ot Facebook prekratit' politicheskie blokirovki // Gazeta.ru URL: http://www.gazeta.ru/tech/news/2015/06/17/n_7296201.shtml (data obrashcheniya: 01.07.2016)
7. Antiekstremizm v virtual'noi Rossii v 2014–2015 gody //Analiticheskii tsentr SOVA. URL: http://www.sova-center.ru/racism-xenophobia/publications/2016/06/d34913 (data obrashcheniya: 11.07.2016)
8. Gde zhivut trolli. Kak rabotayut internet-provokatory v Sankt-Peterburge i kto imi zapravlyaet // Novaya gazeta URL: http://www.novayagazeta.ru/society/59903.html (data obrashcheniya: 20.06.2016).
9. Edinyi reestr domennykh imen, ukazatelei stranits saitov v seti «Internet» i setevykh adresov, pozvolyayushchikh identifitsirovat' saity v seti «Internet», soderzhashchie informatsiyu, rasprostranenie kotoroi v Rossiiskoi Federatsii zapreshcheno. URL: https://eais.rkn.gov.ru
10. Servis Google Trends. URL: https://www.google.ru/trends/
11. Statistika poiskovykh zaprosov «Yandeks.Vordstat». URL: https://wordstat.yandex.ru
12. Stop political blocking on Facebook // Change.org URL: https://www.change.org/p/facebook-stop-political-blocking-on-facebook (data obrashcheniya: 01.07.2016)

DOI: 10.7256/1812-8696.2016.8.19971