УДК-323/324(470+571)+002:338.2

КОНТРОЛИРУЯ НЕКОНТРОЛИРУЕМОЕ: СТРАТЕГИЯ РОССИЙСКОГО ГОСУДАРСТВА В ИНТЕРНЕТЕ

***М.В. Котляров*[1]**

Статья посвящена российским практикам управления Интернетом в контексте адаптации государства к условиям "диджитализации" массовых социальных коммуникаций. Результаты исследования доказывают, что в России завершается период развития свободного Интернета. Государство видит в нем угрозу собственной безопасности и стремится его контролировать. Формируется система управления Интернетом на основе пяти элементов, включающих: анализ информационных угроз, управление публичной информационной повесткой в сети, ужесточение правовой ответственности за распространение информации в киберпространстве, национализацию ключевой инфраструктуры Интернета и личных данных пользователей. Государственная политика скажется на социальных функциях Интернета в России. Его роль как пространства свободного обмена информацией, выражения мнений, политической самоорганизации и мобилизации снизится, а потенциал государственного влияния на общество будет расти. Однако, по мнению автора, государство технически не способно контролировать весь рунет и, вероятно, двинется по пути создания Интернета «для себя».

Ключевые слова: Интернет; политический контроль; информационная безопасность; государственная информационная политика; социальные сети.

Первостепенная роль Интернета как технологического источника модернизации современного общества сегодня не нуждается в доказательстве. После событий «Арабской весны» и движения Occupy значительную актуальность приобрела тема политических изменений, обусловленных развитием киберкоммуникаций. Изучая тему, исследователи и эксперты все больше обращают внимания на проблему трансформации государственных политик управления Интернетом в меры по контролю над компьютерными сетями. Проведенные исследования выявили, что государственный контроль над Интернетом становится распространённой практикой, как в авторитарных, так и в конкурентных политических режимах [24].

[1] Котляров Максим Васильевич - доцент кафедры истории и теории журналистики Гуманитарного института Новосибирского национального исследовательского государственного университета. E-mail: mv_kotlyarov@mail.ru.

Российский опыт исследуется исключительно в контексте политического контроля над медиаполем [26]. Контроль над интернет-сервисами и интернет-инфраструктурой в целях слежки за гражданами пока больше интересует журналистов, а не ученых [16]. В литературе политика российского государства в отношении Интернета оценивается, как правило, в контексте борьбы власти с оппозицией и политизированным гражданским обществом. Между тем этот подход не учитывает объективной эволюции всемирной паутины, которая радикально повлияла на практику повседневной коммуникации и заставила государственные институты адаптироваться к изменениям в независимости от типа политического режима.

Теория политической адаптации обладает рядом методологических преимуществ в изучении этой темы [28]. Она концентрирует внимание на рисках, с которыми сталкивается политическая система в условиях динамичных изменений среды (социальной, культурной, информационной) и взаимосвязанную реакцию на них государственных структур. Кроме того, анализ механизмов адаптации государства к новым условиям и оценка успешности этого процесса даст возможность спрогнозировать его дальнейшие действия и их влияние на среду.

В статье под «государственным управлением Интернетом» подразумевается регулирование хранения, распространения и публикации информации с помощью технологий компьютерных сетей. «Государственный контроль над Интернетом» является частью системы управления им и включает нормы и практику цензурирования публикаций, доступа государственных служб к инфраструктуре Интернета и обращения с данными пользователей. В статье основное внимание уделено анализу контроля над Интернетом, поскольку предполагается, что он выступает в качестве основного механизма адаптации государства к новым социально-политическим условиям, формируемым Интернетом.

Политические риски Интернета

Политические скандалы вокруг хакерских атак в ходе выборов президента США в 2016 г. вновь выявили один из главных политических рисков интернет-коммуникации, заключающийся в слабой защищенности информации, передаваемой через массовые электронные сервисы. Их уязвимость для внешнего вторжения была хорошо известна задолго до этих событий и уже неоднократно использовалась в политических целях. В России от «взломов» электронной почты, личных аккаунтов в социальных сетях и последующей публикации материалов пострадали многие политики и чиновники. В течение 2012–2015 гг. хакерские атаки на публичных персон приобрели характер кампаний, в открытый доступ выкладывалась переписка, в том числе высокопоставленных чиновников правительства и администрации президента, что стало новой формой внутриэлитной борьбы [4].

Информационный шум вокруг хакерских атак между тем заслоняет другие политические риски, порождаемые Интернетом как субъектом и объектом информационного влияния.

Ко второй группе политических рисков относится культура электронной коммуникации. Интернет-сервисы привлекают пользователей объективными преимуществами: мобильностью, простотой и дружелюбием. Популярность киберуслуг заставляет государственные службы соответствовать новому стилю коммуникаций и организационным возможностям сети: быть доступными и оказывать государственные и муниципальные услуги через Интернет, учитывать мнение его пользователей при принятии решений, применять сетевые технологии для легитимации своего статуса. В качестве ответа на эти требования правительства развитых и ряда развивающихся стран, в том числе и России, с разной степенью успеха реализуют программы «электронного правительства» и «электронной демократии» [18].

Третья группа рисков связана с появлением новых методов информационного манипулирования, потенциально имеющих глобальный охват за счет популярности поисковых сервисов. Исследование, выполненное в 2014 г. под руководством американского психолога Р. Эпстейна, выявило возможности поисковых машин, таких как «Гугл», манипулировать электоральными предпочтениями избирателей с помощью ранжирования выдачи страниц при поиске информации о кандидатах. Феномен получил название Search Engine Manipulation Effect (SEME), то есть «эффект манипулирования через поисковик» [21].

Российское государство отреагировало на рост информационного влияния поисковых систем. С 1 января 2017 г. вступил в силу закон, приравнивающий крупные новостные интернет-агрегаторы к СМИ. К ним, в первую очередь, относятся агрегаторы поисковых машин «Яндекс» и «Мэйл.Ру». Закон обязывает владельцев сервисов «проверять достоверность распространяемых общественно значимых сведений до их распространения и незамедлительно прекратить их распространение на основании предписания» Роскомнадзора [11].

Четвертая группа рисков возникла в результате социализации киберпространства. Согласно статистическим оценкам, численность пользователей социальных сетей в мире в 2016 г. составила около 2,22 млрд чел., а к 2019 г. их количество вырастет до 2,72 млрд [22]. На апрель 2016 г. в мире насчитывалась 21 социальная сеть с численностью активных пользователей более 100 млн чел. Безусловным лидером является «Фейсбук», активная аудитория которого составляет 1 млрд 590 млн чел. В топ социальных сетей входят два сервиса, созданных российскими разработчиками, – «Вконтакте» (100 млн) и «Телеграм» (100 млн) [22].

Главным общественно-политическим последствием распространения социальных сетей стало увеличение информационной связности между

людьми, что оказало прямое влияние на динамику политизации обществ. Возможности гражданской самоорганизации, мобилизации, а также международной презентации политической деятельности существенно упростились благодаря «Твиттеру», «Фейсбуку», «Ютьюбу» и другим сервисам, что наглядно продемонстрировали протестные выступления в различных странах, начиная с 2009 г.

Научная дискуссия о роли интернет-коммуникации в гражданских протестах продолжается. Исследователи уже отошли от однозначных выводов, содержащих восторженные оценки «Твиттера» и «Фейсбука» как непосредственных причин революций в Арабском мире, либо полное уничижение их роли в событиях такого рода. Все больше доводов находит точка зрения, что роль социальных сетей в протестных выступлениях заключается в консолидации и мобилизации протестных групп, то есть они являются не просто инструментом организации протеста, а его когнитивной средой. Важнейшее значение в этой среде имеет не рациональная критика политического режима или информирование о планируемых акциях, а эмоциональная заряженность аудитории. Лучшей метафорой этой среды стала *батарея*, аккумулирующая протестные эмоции и передающая их пользователям, тем самым становясь триггером гражданского движения [19].

Государство и Интернет: борьба за влияние

Первой активную позицию в использовании Интернета для решения общественно-политических задач заняла администрация президента США Б. Обамы. Помимо позиционирования главы государства среди Интернет-пользователей, американские чиновники стали отводить Интернету важную роль в вашингтонской внешнеполитической повестке. Публичная защита свободы распространения информации в Интернете стала одним из важных направлений деятельности Госсекретаря Х. Клинтон.

«Технофетишизм» внешнеполитического ведомства США имел неоднозначные последствия. По мнению одного из первых исследователей государственной политики в отношении социальных сетей Е. М. Морозова, защита свободы киберпространства со стороны Госдепартамента привела к обратному эффекту. Авторитарные и оппонирующие США правительства увидели реальную угрозу стабильности своих режимов. Интернет стал рассматриваться как незащищённый канал внешнеполитического влияния США [10, 50].

В России точка зрения на Интернет как на инструмент внешнего влияния стала звучать на государственном уровне с конца 2010 г. *После массовых беспорядков на Манежной площади в Москве, произошедших в декабре 2010 г.,* Генеральный секретарь *Организации Договора о коллективной безопасности (ОДКБ) Н. Н. Бордюжа заявил, что Интернет используется для дестабилизации общественно-политической ситуации*. По его словам, большую

роль Интернет сыграл в организации массовых беспорядков в Молдавии, Иране, Украине и Киргизии [1].

Недоверие по поводу независимости и безопасности всемирной паутины выразил лично президент В.В. Путин в апреле 2014 г. на медиафоруме в Санкт-Петербурге. Отвечая на один из вопросов журналистов, он сказал, что Интернет возник «как спецпроект ЦРУ США, так и развивается» и поддержал идею хранения данных крупных российских интернет-сервисов на территории страны [12]. Слова президента не были случайной оговоркой, а являлись отражением оценки политических рисков киберпространства со стороны органов, ответственных за государственную безопасность.

В новой «Доктрине информационной безопасности Российской Федерации», утвержденной 5 декабря 2016 г. зафиксированы эти угрозы: «Расширяются масштабы использования специальными службами отдельных государств средств оказания информационно-психологического воздействия, направленного на дестабилизацию внутриполитической и социальной ситуации в различных регионах мира и приводящего к подрыву суверенитета и нарушению территориальной целостности других государств» [3].

Политические протесты зимы 2011−2012 гг. в России ярко продемонстрировали возможности социальных сетей в целях консолидации и мобилизации народных выступлений [20]. Интенсивность протестного движения в городах заставила органы государственной власти на практике озаботиться вопросами регулирования распространения публичной информации в Интернете. Предпринятые меры складываются в полноценную систему государственного контроля над ним, включающую: анализ протестных трендов, распространение пропаганды, правовое регулирование и управление инфраструктурой Интернета.

В течение 2012−2014 гг. спецслужбы, правоохранительные органы, администрация президента, федеральные министерства, региональные и городские администрации начали активно применять программно-аппаратные комплексы, позволяющие собирать и анализировать публикации интернет-СМИ и социальных сетей практически в онлайн-режиме. Одной из функций наиболее высокоразвитых программно-аппаратных комплексов является автоматизированная оценка тональности сообщений, с целью улавливания эмоционального напряжения в сети как признака протестной мобилизации. В этом видится возможность на ранней стадии выявлять протестные поводы и, соответственно, оперативнее, чем прежде, на них реагировать [7].

В июне 2013 г. была создана организация численностью не менее 400 чел., специализирующаяся на онлайн-пропаганде. Она получала название «фабрика-троллей». В круг ее задач входит навязывание проправительственной повестки в общественно-политических дискуссиях и дискредитация оппозиции на популярных интернет-сайтах, форумах, блогах и в социальных

сетях. Онлайн-пропаганда дополняет систему государственной пропаганды, ведущуюся через государственное телевидение, радио, интернет-издания [2].

Юридической основой фильтрации контента в Интернете стали законы, налагающие ответственность за распространение экстремистских мнений и фактов в онлайн-пространстве. Антиэкстремистское законодательство в России действует с 2002 г., однако специфические нормы для Интернет-экстремизма были приняты еще в июне 2012 г. Правовые изменения предусматривали внесудебную блокировку сайтов с призывами к экстремистским действиям и массовым беспорядкам [17]. Они были дополнены поправками в законодательство, направленными на установление контроля за лидерами мнений в социальных сетях. С 1 августа 2014 г. деятельность блогеров, чья ежедневная аудитория превышает 3 тыс. чел., была приравнена к деятельности СМИ.

Одной из последних инициатив стал контроль над так называемой критической инфраструктурой Интернета, включающей национальные доменные зоны верхнего уровня (.ru, .рф) и элементы, обеспечивающие их функционирование – системы точек обмена трафиком, линии и средства связи. Совет Безопасности России впервые обратил внимание на защиту критической инфраструктуры в 2009 г., однако никаких конкретных действий не предпринималось до раскручивания в 2014 г. нового витка противостояния между Россией и Западом [8].

В конце июля 2014 г. в рамках исполнения поручения Совета Безопасности в Министерстве связи и массовых коммуникаций состоялись первые учения по моделированию инфраструктурных угроз Интернета. Помощник президента РФ И. О. Щеголев доложил президенту России В. В. Путину о результатах летних учений, подчеркнув, что российский сегмент Интернета скорее не устойчив к внешним воздействиям. Затем И.О. Щеголев призвал создать в России «ключевую инфраструктуру Интернета», включая национальные корневые серверы и национальную систему маршрутно-адресной информации [5]. В 2016 г. началась реализация этих предложений, был установлен контроль со стороны госструктур над некоммерческой организацией − Координационным центром национального домена, управляющего доменами .RU и РФ, что означает фактическую его национализацию [9].

Судить об эффективности проводимой политики позволяет ряд фактов. Как показало исследование Центра Беркмана при Гарвардском университете, в 2010 г. русскоязычная блогосфера была пространством в значительной степени свободным от государственного контроля. Существовавшие на тот момент проправительственные молодежные группы и блогеры были немногочисленны и не являлись центральными узлами в общественно-политических сообществах социальных сетей [20].

По прошествии пяти лет структура политизированного сегмента русскоязычной блогосферы заметно изменилась. Рейтинги наиболее популярных

русскоязычных блогов, которые публикует одна из ведущих компаний на рынке анализа и мониторинга социальных сетей Brand analytics, показывают возросшее влияние проправительственных авторов. С января 2015 г. по июнь 2016 г. в Топ-10 русскоязычных блогов по количеству цитирования обычно входило четыре – шесть авторов, которые транслировали провластную позицию, и только два – оппозиционных. По общему количеству цитирования в последние полтора года провластные ресурсы также, как правило, заметно опережали оппозиционные [16].

Одновременно важным фактором снижения радикальности и оппозиционности рунета стало применение правоохранительными органами антиэкстремистского законодательства. По данным мониторинга информационно-аналитического центра «Сова», усиливается преследование пользователей Интернета за публикации. В 2007 г. было зафиксировано три приговора за публичные высказывания в Интернете из 28 приговоров по антиэкстремистским статьям уголовного кодекса, в 2008 г. – 14 из 45, в 2009 г. – 17 из 56, в 2010 г. – 26 из 72, в 2011 г. – 52 из 78, в 2012 г. – 65 из 89. В 2013 г. таких приговоров уже насчитывалось 103 из 133, в 2014 г. – 138 из 165. В 2015 г. из 232 приговоров за публичные высказывания, которые были отнесены к экстремистским, 194 было вынесено за высказывания онлайн [17]. Новой тенденцией 2014–2015 гг. стало то, что в рамках борьбы с экстремизмом государство усилило давление на самые разные категории граждан – от радикальных националистов, исламистов, до оппозиционеров, людей и организаций, просто случайно оказавшихся в поле зрения борцов с экстремизмом [17].

Статистика правоприменительной практики в отношении «антиэкстремистских» высказываний в сети, кроме того, выявила важную особенность – чаще всего в поле зрения правоохранительных органов попадают пользователи российской социальной сети «ВКонтакте». В 2015 г., по http://www.sova-center.ru/racism-xenophobia/publications/2016/06/d34913/-_ftnref14 данным центра «Сова», за посты и репосты в «ВКонтакте» к уголовной ответственности привлекли 119 чел., в то время как за пост на «Фейсбуке» преследовали одного человека, а в «Одноклассниках» − троих.

Причина такой практики обусловлена как спецификой аудитории социальной сети, так и возможностями доступа к ее данным. «Вконтакте» − «молодежная» социальная сеть, согласно исследованию компании Mail.Ru Group, проведенному в марте 2014 г., 59% аудитории «ВКонтакте» составляют пользователи до 34 лет. В этой социальной сети чаще всего создают сообщества и публикуют сообщения молодёжь с радикальными общественно-политическими взглядами.

Кроме того, пользователей этой сети легко обнаружить. «ВКонтакте», по сравнению с другими социальными сетями, не имеет ограничений для скачивания публичной информации пользователей. Самая популярная рос-

сийская социальная сеть очень удобна для автоматизированного парсинга с целью поиска сообщений и авторов по определенным объектам и темам.

Идентифицировать пользователя «ВКонтакте» также проще, чем пользователя других социальных сетей. При регистрации в этой социальной сети вводятся контактные данные и номера телефонов владельцев страниц, администраторы сети предоставляют эти сведения сотрудникам правоохранительных органов, в то время как администрация зарубежных сетей отказывает в предоставлении информации.

Ограниченность возможностей спецслужб и правоохранительных органов по поиску и идентификации пользователей социальных сетей указывает на серьезные препятствия по организации оперативной слежки в Интернете. Российские спецслужбы и правоохранительные структуры в условиях большого разнообразия независимых коммуникационных интернет-сервисов технически не способны организовать поиск и анализ противоправного контента не только во всем рунете, но даже во всех русскоязычных социальных медиа. С этим препятствием связаны последние законодательные инициативы, нацеленные на хранение личных данных пользователей и расширение доступа государства к ним.

Государство и Интернет: борьба за данные

Первые шаги по контролю за личными данными пользователей рунета государство предприняло в 2014 г., когда был принят закон, налагающий на физических и юридических лиц, «организующих распространение информации и (или) обмен данными между пользователями», обязанность уведомлять Роскомнадзор о начале своей деятельности, а также хранить данные обо всех действиях пользователей в течение полугода после окончания своей деятельности и предоставлять их правоохранительным органам в случаях, предусмотренных законодательством. За невыполнение этих обязательств вводились административные санкции в виде штрафов. Принятие этого закона не вызвало большого резонанса в Интернет-сообществе, поскольку его нормы были приемлемыми.

В апреле 2016 г. на рассмотрение Государственной думы поступил «Антитеррористический пакет» законов или «пакет Яровой», по фамилии одного из четырех парламентариев, внесших его в нижнюю палату Федерального собрания. Самое резонансное обсуждение вызвали изменения в федеральный закон «О связи», касающиеся хранения на территории Российской Федерации личных данных пользователей на срок до шести месяцев. Точный «порядок, сроки и объем хранения информации», согласно закону, должен быть установлен правительством Российской Федерации и вступит в силу 1 января 2018 г. Законопроект был одобрен обеими палатами Федерального собрания, и 7 июля 2016 г. его подписал президент.

Новые изменения напрямую обязывают сотовых операторов и провай-

деров хранить содержание переговоров, переписки и другие типы файлов, пересылаемые абонентами за шесть месяцев. Исполнение новых норм предполагает затраты на создание инфраструктуры хранения, которые, по оценкам экспертов, составят сотни миллиардов рублей и, соответственно, могут уничтожить бизнес многих участников рынка.

Оппозиционные организации, в свою очередь, обеспокоились угрозой тотальной слежки за гражданами со стороны государства. Против «Пакета Яровой» были организованы самые крупные общественно-политические митинги и «народные сходы» 2016 г. В Новосибирске, Екатеринбурге, Уфе, Кургане, Казани, Санкт-Петербурге 26 июля прошли протестные акции. В Москве митинг состоялся 9 августа. В общей сложности в протестах приняли участие около 4 тыс. чел.

Несмотря на негодования бизнеса и протесты оппозиции, государство нацеливается на исполнение «Антитеррористического пакета», не собираясь идти на существенные уступки. Реализация «Антитеррористического пакета» может стать началом создания в России «китайской» модели Интернета. Об этом говорит заявление советника президента по вопросам развития Интернета Г. С. Клименко, которое он произнес 26 января 2017 г. в Военной академии Генерального штаба ВС РФ: «Путь один – это китайский вариант. Безусловно, контроль нужен, потому что не существует ни одной возможности это предотвратить. Китай менее щепетилен к мнению общества, они оценили угрозу и ограничили Интернет. Теперь у них таких проблем нет». Он подчеркнул, что если иностранные мессенджеры и социальные сети не будут сотрудничать с правоохранительными органами «любое уважающее себя государство должно их выкинуть» [14].

Выводы и прогнозы

Политику российского государства в отношении киберпространства в 2012–2016 гг. определяло два мотива. Глобальный Интернет рассматривается государством как инструмент внешнеполитического влияния США, который угрожает политическому суверенитету. Второй мотив заключается в понимании консолидирующей и мобилизующей роли массовых социальных сетей в современных гражданских протестах. В совокупности эти риски были признаны угрожающими национальной безопасности, поэтому инициатива по установлению контроля над Интернетом в настоящее время принадлежит спецслужбам, а не «гражданским» ведомствам.

Борьба с этими угрозами ведется в информационной и политико-юридической сферах. Автоматизированный анализ сообщений социальных сетей, блогов и интернет-изданий, распространение онлайн-пропаганды и правовая база для привлечения пользователей к уголовной ответственности за «экстремистские публикации» служит выявлению и пресечению опасного для политического режима контента. Следующими шагами в процессе уста-

новления контроля над Интернетом становится национализация его инфраструктуры и получение полного доступа государства к личным данным пользователей.

Период свободного Интернета в России, таким образом, завершается. «Национальный» Интернет в России формируется не с целью усиления экономического и культурного присутствия страны в глобальном информационном пространстве, а в виде спИнтернета (*от английского глагола to spin – крутить*) – разновидности всемирной паутины, в которой функция свободного обмена информацией и выражения взглядов приходит в упадок, а развитие получает манипуляция общественным мнением и слежка со стороны государства за пользователями.

Проводимая политика, таким образом, гораздо шире задач противодействия терроризму в киберпространстве, а также распространенных авторитарных практик, включающих блокирование сайтов и распространение пропаганды. В российской стратегии видны амбиции великодержавности. Адаптируясь к новой информационной среде, государственная власть не только защищается от информационных угроз Интернета, но и стремится с его помощью стать сильнее и влиятельнее.

Важнейший вывод состоит в том, что формирующаяся в России модель контроля над Интернетом является одним из признаков имперской трансформации политического режима, стремящегося быть единственным игроком на политическом поле «русского мира» не только «офлайн», но и «онлайн». Для российского государства киберпространство – среда, которой необходимо управлять также как реальной территорией, используя ее ресурсы для решения актуальных задач.

Экспансионистская государственная политика для рунета будет иметь негативный характер. С помощью предпринимаемых мер властям, безусловно, удастся добиться повышения уровня самоцензуры в Интернете. Пользователи, напуганные новостями о полном доступе спецслужб к их личным данным, будут более осторожно действовать в Интернете, особенно в его публичной сфере.

Воплощение «Антитеррористического пакета» приведет к национализации данных пользователей услуг связи, т.е. в распоряжении государства окажутся не только телефонные разговоры, фото, аудио и видео рядовых пользователей, посылаемые своим родственникам, друзьям и знакомым, но и деловые файлы корпоративного мира. С экономической точки зрения это означает, что в деловых отношениях появляется еще один агент – государство, которое может непредсказуемо вмешаться в бизнес-процесс, обладая данными его участников, т.е. надежность деловых отношений подрывается.

В этом отношении стратегия государства в киберпространстве не имеет отличий от политики управления «стратегическими» отраслями, такими как атомная энергетика, добыча нефти и газа, ВПК, которые пронизаны государ-

ственным контролем. Жесткий государственный контроль над рунетом приведет к монополизации отрасли и сделает его менее привлекательным для инвестиций и создания бизнеса.

Однако реальный контроль над инфраструктурой Интернета, хранение и тем более оперативный анализ данных пользователей являются сложно выполнимыми задачами, которые могут быть решены лишь частично, либо не решены вовсе. Естественными ограничениями реализуемой стратегии выступает высокий уровень проникновения зарубежных коммуникационных сервисов в России и техническая сложность реализации этой задачи. В настоящее время Россия не располагает промышленными технологиями для изготовления серверов, чтобы обеспечить безопасное хранение и обращение с данными рунета на территории страны.

Авторы проводимой политики, кроме того, исходят из неверной посылки о том, что Интернет можно контролировать как любую другую систему, завладев ее центром управления и инфраструктурой. Технология компьютерных сетей изначально создавалась и функционирует как децентрализованная система узлов и связей, она не имеет единого органа управления и инфраструктуры. Кроме того, приватный и публичный контент в Интернете создается миллионами пользователей, а не ограниченным числом организаций.

Еще одним серьезным ограничением является антиинновационный характер проводимой государственной политики в отношении Интернета. Профильному бизнесу, научным организациям и обществу в целом не предлагается создание новых полезных и экономически выгодных инструментов. По этой причине законодательство по контролю за данными пользователей не вызывает какого-либо энтузиазма среди представителей телекоммуникационной отрасли и интернет-сообщества, без активного привлечения которых невозможно ни заручиться доверием к проводимой политике, ни решить сложные технические задачи в ходе ее выполнения.

Кроме того, расширение государственного контроля над сетью создает запрос на ее развитие в сторону защиты анонимности и автономности пользователей. Потенциально Интернет-индустрия может ответить на возникший вызов с помощью шифрования данных (что уже происходит), максимального закрытия программных «окон» и «дыр», позволяющих следить за пользователями, а также новой инфраструктуры Интернета, независимой от оптоволоконных кабелей.

В завершение ответим на один важный вопрос – возможен ли в текущих условиях компромисс между стремлениями государства к жесткому контролю над сетью и правом граждан и бизнеса защищать свою информацию? Наиболее приемлемым решением является введение особых норм и внедрение специальных Интернет-сервисов, в первую очередь, электронной почты, социальных сетей, мессенджеров и аналитической системы, анализи-

рующей информационные потоки, непосредственно для органов государственной власти, и обеспечивающих их функционирование организаций. Создание не государственного Интернета, а «Интернета для государства» вполне реализуемо уведет политический режим от конфликта с Интернет-компаниями и гражданами, отстаивающими личную свободу, а также снизит риски информационных утечек, инсайдов и повысит информационную безопасность госсектора.

Библиографический список

1. «Бордюжа сравнил интернет с оружием, имея в виду беспорядки в Москве и Минске» // Интерфакс. 21.12.2010. [Электронный ресурс]. URL: http://www.interfax.by/news/belarus/1085142 [Bordyuzha compared the Internet with a weapon, meaning riots in Moscow and Minsk // Interfax. 21.12.2010. Available at: http://www.interfax.by/news/belarus/1085142].
2. «Где живут тролли? И кто их кормит?» // Новая газета. 2013. 7 сент. [Электронный ресурс]. URL: http://www.novayagazeta.ru/politics/59889.html; «Я хочу закрыть эту фабрику лжи» // Новая газета. 2015. 1 июня. [Электронный ресурс]. URL: http://www.novayagazeta.ru/politics/68627.html; «Главпаутина» // Новая газета. 2016. 17 авг. [Электронный ресурс]. URL: http://www.novayagazeta.ru/society/74216.html [«Where trolls live. And who feeds them» // Novaya Gazeta. 07.09.2013. Available at: http://www.novayagazeta.ru/politics/59889.html; «I want to close this factory of lies» // Novaya Gazeta. 01.06.2015. Available at: http://www.novayagazeta.ru/society/74216.html; «Headweb» // Novaya Gazeta. 17.08.2016. Available at: http://www.novayagazeta.ru/society/74216.html].
3. «Доктрина информационной безопасности Российской Федерации». [Электронный ресурс]. URL: http://www.scrf.gov.ru/documents/6/5.html [Information Security Doctrine of the Russian Federation. Available at: http://www.scrf.gov.ru/documents/6/5.html].
4. «Звездные войны» «Шалтая-Болтая» // Gazeta.ru. 2015. 7 апр. [Электронный ресурс]. URL: https://www.gazeta.ru/politics/2015/04/15_a_6640401.shtml [«Star wars» of «Humpty Dumpty» // Gazeta.ru. 07.04.2015. Available at: https://www.gazeta.ru/politics/2015/04/15_a_6640401.shtml].
5. «И. Щёголев: «Учения подтвердили недостаточную устойчивость Рунета при недружественных «целенаправленных действиях» // Экспертный центр электронного государства (сайт). 17.10.2014. [Электронный ресурс]. URL: http://d-russia.ru/ucheniya-podtverdili-nedostatochnuyu-ustojchivost-runeta-pri-nedruzhestvennyx-celenapravlennyx-dejstviyax.html

[I. Shchegolev: «The training showed insufficient stability of the Runet in case of unfriendly «focused actions» // Expert e-government center (website). 17.10.2014. Available at: http://d-russia.ru/ucheniya-podtverdili-nedostatochnuyu-ustojchivost-runeta-pri-nedruzhestvennyx-celenapravlennyx-dejstviyax.html].

6. Интернет и идеологические движения в России / сост. Г. Никипорец-Такигава, Э. Паин. М., 2016. С. 442–443. [The Internet and the ideological movements in Russia. Comp. by G. Nikiporets-Takigawa, E. Pain. Moscow, 2016. P. 442−443].
7. «Как власти читают ваши блоги» // Forbes. 16.08.2012. [Электронный ресурс]. URL: http://www.forbes.ru/sobytiya/vlast/92590-kak-vlasti-chitayut-vashi-blogi-rassledovanie-forbes [«How the authorities read your blogs»// Forbes. 16.05.2012. Available at: http://www.forbes.ru/sobytiya/vlast/92590-kak-vlasti-chitayut-vashi-blogi-rassledovanie-forbes].
8. *Колесников А.В.* Красная кнопка интернета // Индекс Безопасности, №4 (115), 2015 г. С. 40. [Электронный ресурс]. URL: http://www.pircenter.org/media/content/files/13/14513433110.pdf [*Kolesnikov A.V.* Red button of the Internet // Security Index. No. 4 (115), 2015, P. 40. Available at:: http://www.pircenter.org/media/content/files/13/14513433110.pdf].
9. «Мир вашему домену. Координационный центр .RU/.РФ готовят к национализации» // КоммерсантЪ. 17.08.2016. [Электронный ресурс]. URL: http://www.kommersant.ru/doc/3066171 [«Peace to your domain». The .RU/.RF Coordination Center is being prepared for nationalization // Kommersant. 17.08.2016. Available at: http://www.kommersant.ru/doc/3066171].
10. *Морозов Е. М.* Интернет как иллюзия. Обратная сторона сети. М., 2014. [*Morozov E.M.* The Internet as an illusion. The reverse side of the network. Moscow, 2014].
11. «Путин подписал закон, приравнивающий новостные агрегаторы к СМИ» // ТАСС. 2016. 23 июня. [Электронный ресурс]. URL: http://tass.ru/ekonomika/3395954 [«Putin signed the law equating news aggregators with the mass media» // TASS. 23.06.2016. Available at: http://tass.ru/ekonomika/3395954].
12. «Путин считает важным размещать в РФ серверы крупных национальных интернет-ресурсов» //ТАСС. 2014. 24 апр. [Электронный ресурс]. URL: http://tass.ru/politika/1144396 [«Putin considers it important to deploy servers of large national Internet resources in Russia» // TASS. 04.24.2014. Available at: http://tass.ru/politika/1144396].
13. «Рейтинг блогов.» [Электронный ресурс]. URL: https://br-analytics.ru/mediatrends/blog/ [The rating of blogs. Available at: https://br-analytics.ru/mediatrends/blog/].

14. «Советник президента Клименко предложил ограничить в России Интернет» // Интерфакс. 2017. 26 янв. [Электронный ресурс]. URL: http://www.interfax.ru/russia/547163 [«Presidential Adviser Klimenko suggested limiting the Internet in Russia» // Interfax. 26.01.2017. Available at: http://www.interfax.ru/russia/547163].
15. *Солдатов А., Бороган И.* Битва за Рунет: Как власть манипулирует информацией и следит за каждым из нас. М., 2017. [*Soldatov A., Borogan I.* Battle for Runet: How the authority manipulates information and spies on everyone of us. Moscow, 2017].
16. *Этлинг Б. , Алексанян К., Келли Д., Фарис Р., Палфри Д. и Гассер У.* Публичный дискурс в российской блогосфере: анализ политики и мобилизации в Рунете // Исследования Центра Беркмана № 2010−11. 2010. 19 окт. [Электронный ресурс]. URL: http://cyber.law.harvard.edu/sites/cyber.law.harvard.edu/files/Public_Discourse_in_the_Russian_Blogosphere-RUSSIAN.pdf [*Etling B., Alexanyan K., Kelly J., Faris R., Palfrey J. and Gasser U.* Public Discourse in the Russian Blogosphere: Mapping RuNet Politics and Mobilization // Berkman Center Research Publication No. 2010-11. 19.10.2010. Available at:: http://cyber.law.harvard.edu/sites/cyber.law.harvard.edu/files/Public_Discourse_in_the_Russian_Blogosphere-RUSSIAN.pdf].
17. *Юдина Н.* Антиэкстремизм в виртуальной России в 2014–2015 гг. Доклад информационно-аналитического центра «Сова». 28.06.2016. [Электронный ресурс]. URL: http://www.sova-center.ru/racism-xenophobia/publications/2016/06/d34913/#_ftn1 [*Yudina N.* Anti-extremism in virtual Russia in 2014−2015. Report of the information-analytical center «Sova». 28.06.2016. Available at: http://www.sova-center.ru/racism-xenophobia/publications/2016/06/d34913/#_ftn1].
18. *Baum S., Mahizhnan A.* E-Governance and Social Inclusion: Concepts and Cases. USA, 2014. 356 p.
19. *Castells M.* Networks of Outrage and Hope. Social movements in the Internet Age. Cambridge, 2015. P. 14–15.
20. *Enikolopov R., Makarin A., Petrova M.* Social Media and Protest Participation: Evidence from Russia. 07.04. 2016. Available at: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2696236.
21. *Epstein R., Robertson R.E.* The search engine manipulation effect (SEME) and its possible impact on the outcomes of elections // Proceedings of the National Academy of Sciences of the United States of America (PNAS). Published online 04.08.2015. Available at: http://www.pnas.org/content/112/33/E4512.full.
22. Leading social networks worldwide as of April 2016, ranked by number of active users (in millions). Available at:

http://www.statista.com/statistics/272014/global-social-networks-ranked-by-number-of-users/ (accessed 28.06.2016).
23. *Morozov, E.* The net delusion: The dark side of Internet freedom. New York, 2012. 432 p.; Yangyue Liu. Competitive Political Regime and Internet Control: Case Studies of Malaysia, Thailand and Indonesia. Cambridge Scholars Publishing. 2014. 220 p.
24. Number of social network users worldwide from 2010 to 2019 (in billions). Available at: http://www.statista.com/statistics/278414/number-of-worldwide-social-network-users/.
25. *Ognyanova K.* Careful What You Say: Media Control in Putin's Russia – Implications for Online Content // International Journal of E-Politics (IJEP) 1(2).2010. Available at: http://www.igi-global.com/article/careful-you-say/43597; Tselikov A. The Tightening Web of Russian Internet Regulation // The Berkman Center for Internet & Society Research Publication Series. Available at: http://cyber.law.harvard.edu/publications/2014/runet_regulation; *Качкаева А. Фоссато Ф.* Медиамашина зрелого авторитаризма: корпоративная консолидация и технологии политической мобилизации // Политическое развитие России. 2014−2016: Институты и практики авторитарной консолидации. М., 2016. С. 196-213 [*Kachkaeva A. Fossato F.* Mediamachine of the mature authoritarianism: corporate consolidation and technologies of political mobilization // Political development of Russia. 2014−2016: Institutions and practices of authoritarian consolidation. Moscow, 2016. P. 196−213.].
26. Revealed: US spy operation that manipulates social media // The Guardian. 17.03.2011. Available at: http://www.theguardian.com/technology/2011/mar/17/us-spy-operation-social-networks.
27. *Rosenau J.N.* The Study of Political Adaptation. L.; N.Y., 1981. 235 p.

CONTROLLING THE UNCONTROLLABLE: THE STRATEGY OF THE RUSSIAN AUTHORITIES IN THE INTERNET

M.V. Kotlyarov
Associate Professor, Department of History and Theory of Journalism,
Institute for the Humanities, Novosibirsk State University

The paper is devoted to the Russian practices of the Internet governance in the context of the state adaptation to the "digitalization" of mass social communications. The research results demonstrate that the period of the free Internet development is coming to the end in Russia. The state considers it as a threat to its own security and tends to control it. The system of the Internet governance is based on five elements: analysis of information threats, management of public information agenda

on the web, tightening of legal responsibility for the dissemination of information in cyberspace, and nationalization of the main Internet infrastructure and personal data of the users. The author states that the state policy will affect the social functions of the Internet. Its role as a space for free information exchange, expression of opinions, and political self-organization and mobilization will be reduced, and the state influence on the society will be growing. However, according to the author, the authorities are not technically able to control the entire Russian cyberspace and therefore will likely move towards the creation of the Internet "for themselves".

Keywords: Internet; political control; information security; public information policy; social networks.