

# ГЛОБАЛЬНЫЕ ИНТЕРНЕТ-СЕРВИСЫ В СТРУКТУРЕ ИНСТРУМЕНТОВ АМЕРИКАНСКОЙ ВНЕШНЕЙ ПОЛИТИКИ

АЛЕКСАНДР СТИХИН

Арканзасский университет, Файетвилль, США

МГИМО(У) МИД России, Москва, Россия

---

## Резюме

Вопрос обеспечения безопасности информационного пространства стоит сегодня особенно остро. Развитие информационно-коммуникационных технологий и глобальной сети Интернет связано с регулярным возникновением новых вызовов национальной и международной безопасности. В условиях открытости и свободы всемирной сети на передний план, помимо технологических угроз, выходят угрозы содержательные. Попытку обратить внимание мирового сообщества на эти вызовы предприняла Россия, представив в 2012 г. проект конвенции ООН об обеспечении международной информационной безопасности. Однако появление этого документа обнаружило коренные противоречия Запада и Москвы по вопросам регулирования информационного пространства. Центральное противоречие связано с разницей в подходах к соотношению безопасности и свободы действий в информационной сфере. Западные страны настаивают на недопустимости цензурирования Интернет-контента. Россия и ряд стран ШОС указывают на угрозы злоупотребления свободой во всемирной сети в целях дестабилизации социально-политической ситуации в отдельных странах. Опасения российской стороны представляются оправданными или, как минимум, заслуживающими совместного обсуждения и исследования.

Вопрос использования возможностей Интернета для осуществления информационного влияния в интересах других стран и их политических элит наиболее уместно рассматривать в контексте информационной политики государств. Давно перестав носить сугубо внутривнутриполитический характер, она включает официальный и неофициальный компонент, различающиеся по используемым методам. На примере информационной политики США, осуществляемой через глобальные Интернет-сервисы, автор приходит к выводу о существовании двух потенциальных аспектов их использования в интересах конкретных стран. Прежде всего, речь идет о возможностях технологического манипулирования информационной повесткой дня, что вкупе с измеримостью поведения пользователей в Интернете создает широкие возможности по управлению внешней аудиторией. Вместе с тем ключевой проблемой остается подавляющее преобладание США в качестве основного источника информационной повестки дня и содержательного наполнения глобальных информационных площадок. Как следствие доминирования в информационном пространстве контента, которое отвечает интересам одной страны, создается информационный

---

Статья подготовлена при финансовой поддержке гранта РФФИ No.13-07-00022.

Для связи с автором / Corresponding author:

Email: aleksandr\_stikhin@gmail.com

дисбаланс. Без изменения соотношения информационного присутствия различных государств в Интернете сложно ожидать реформирования архитектуры регулирования мирового информационного пространства.

**Ключевые слова:**

информационная безопасность; кибербезопасность; Интернет-сервисы; социальные сети; режим; информационная политика; публичная дипломатия; Веб 2.0; США.

По мере неостановимого совершенствования информационных технологий все большую остроту приобретает проблема обеспечения национальной информационной безопасности и государственного суверенитета в этой области. Число пользователей сети Интернет во всем мире превышает 2,3 млрд. человек. Ее влияние на все стороны жизни общества и государства нарастает, что влечет за собой возникновение новых, типологически более разнообразных угроз. Интернет становится не только крупнейшим хранилищем информации, накопленной человечеством, но и местом концентрации критической инфраструктуры государственного и корпоративного управления, от которой зависит безопасность стран. Революционные события последних лет на Арабском Востоке, а также ряд скандальных разоблачений об использовании частной информации из глобальной сети в разведывательных и криминальных целях, привлекли дополнительно большое, порой даже непропорционально большое внимание к вопросам политической конкуренции в информационной сфере.

Наряду с громадными возможностями, которыми новейшие информационно-коммуникационные технологии (ИКТ) вооружают разнотипных субъектов мировых взаимодействий, все более очевидным становится факт наличия у комплексного лидера современного мира — США — подавляющего, в сравнении с другими участниками международной системы, превосходства в осуществлении широкого экстерриториального информационного воздействия. Подобное положение провоцирует рост озабоченности России и целого ряда других стран, включая ее партнеров по БРИКС и ШОС, состоянием защищенности национальных информационных пространств. Не случайна активизация попыток ряда

международных игроков, прежде всего Российской Федерации, добиться разработки глобальных правил, регулирующих функционирование сети Интернет.

Весомым вкладом в эту деятельность стала инициатива по заключению конвенции ООН об обеспечении международной информационной безопасности. Проект такого документа был предложен Россией ее международным партнерам в 2012 году. Вместе с тем выдвинутое предложение, основывавшееся на идее всестороннего регулирования информационной сферы, встретило резкое неприятие как США, так и ЕС. Ведущие развитые страны рассматривают в качестве предпочтительной основы международного регулирования в этой области Будапештскую конвенцию Совета Европы по борьбе с киберпреступностью, построенную на концептуально ином понимании угроз национальной безопасности.

Расхождения сторон проявляются уже в различном понимании самого объекта регулирования. В этих условиях приходится констатировать: *хотя проблема формирования международного режима в сфере информационной безопасности остается предельно актуальной, пока она выглядит принципиально неразрешимой.*

1

Несмотря на глобальный характер информационных угроз, противодействие им блокируется концептуальными разногласиями ключевых игроков. Это проявляется уже в названиях регулирующих документов, которым следуют или предлагают следовать стороны. Россия совместно со своими партнерами по ШОС фокусируют внимание на информационной безопасности, в то время как США и ЕС — на кибербезопасности. Полезно сопоставить понятийные границы обоих подходов.

Российский проект конвенции ООН определяет **информационное пространство** как «сферу деятельности, связанную с формированием, созданием, преобразованием, передачей, использованием и хранением информации, оказывающей воздействие на индивидуальное и общественное сознание, информационную инфраструктуру и, собственно, информацию». **Информационная безопасность** — это состояние защищенности интересов личности, общества и государства от угроз деструктивных и иных негативных воздействий в информационном пространстве. **Киберпространство** — это электронная среда, в которой информация создается, передается, принимается, хранится, обрабатывается и уничтожается. **Кибербезопасность** — свойство киберпространства противостоять намеренным и/или ненамеренным угрозам, а также реагировать на них и восстанавливаться после воздействия этих угроз<sup>1</sup>.

Исходя из устоявшихся в международных документах определений видно, что информационное пространство представляет собой более широкое понятие по сравнению с часто употребляемым термином киберпространство, обозначая более широкую сферу деятельности, оказывающую воздействие не только на инфраструктуру, но и на индивидуальное и общественное сознание. Между тем основной ныне действующий акт, призванный создавать нормативные рамки обеспечения международной безопасности в сети Интернет, — принятая в 2001 г. Конвенция Совета Европы о киберпреступности<sup>2</sup> — нацелен на повышение защищенности в первую очередь самой электронной среды. Он не затрагивает проблемы и угрозы, связанные с влиянием информа-

ции на социальную и политическую обстановку в мире или в отдельных странах. Более конкретно: документ фокусируется на противодействии преступлениям, связанным с нарушениями конфиденциальности, целостности и доступности компьютерных данных и систем, правонарушениям с использованием компьютерных средств в мошеннических целях и нарушением авторских прав.

Список угроз в проекте конвенции ООН, подготовленном Россией, значительно шире. Его основная особенность — стремление распространить сферу международного регулирования на попытки оказания внешнего влияния на внутриполитические и социально-культурные процессы в отдельных странах. В качестве угроз информационной безопасности авторы документа обозначили «действия в информационном пространстве с целью подрыва политической, экономической и социальной систем другого государства, психологическую обработку населения, дестабилизирующую общество»; «трансграничное распространение информации, противоречащей принципам и нормам международного права, а также национальным законодательствам государств»; «манипулирование информационными потоками в информационном пространстве других государств, дезинформацию и сокрытие информации с целью искажения психологической и духовной среды общества, эрозии традиционных культурных, нравственных, этических и эстетических ценностей»<sup>3</sup>.

*Краеугольным камнем российского проекта становится принцип распространения разграничения национальных «территорий» на информационное пространство и предот-*

<sup>1</sup>Russia-U.S. bilateral on cybersecurity. Critical terminology foundations. Issue 1. 2011. P.20,31. [Электронный ресурс]. URL: [http://www.google.com/url?sa=t&rc=t&q=&esrc=s&source=web&cd=2&ved=OCDUQFJAB&url=http%3A%2F%2Fwww.ewi.info%2Fsystem%2Ffiles%2Freports%2FRussia-U%2520S%2520%2520bilateral%2520on%2520terminology%2520v76%2520%282%29.pdf&ei=MMtftUtPxOqTe2QW894GQBw&usq=AFQjCNfLyXkPIUk5XiOE9iJ3mtSJlBys5w&sig2=1R\\_-Ba5sct9VZNUYDvH4\\_A&bvm=bv.54176721,d.b2l](http://www.google.com/url?sa=t&rc=t&q=&esrc=s&source=web&cd=2&ved=OCDUQFJAB&url=http%3A%2F%2Fwww.ewi.info%2Fsystem%2Ffiles%2Freports%2FRussia-U%2520S%2520%2520bilateral%2520on%2520terminology%2520v76%2520%282%29.pdf&ei=MMtftUtPxOqTe2QW894GQBw&usq=AFQjCNfLyXkPIUk5XiOE9iJ3mtSJlBys5w&sig2=1R_-Ba5sct9VZNUYDvH4_A&bvm=bv.54176721,d.b2l)

<sup>2</sup>Convention on Cybercrime. Council of Europe. Budapest, 23.XI.2001. [Электронный ресурс]. URL: <http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm>

<sup>3</sup>Конвенция об обеспечении международной информационной безопасности (концепция). [Электронный ресурс]. URL: <http://www.scrf.gov.ru/documents/6/112.html>

вращение размывания в этой сфере норм международного поведения, исходящих прежде всего из концепции государственного суверенитета. Отсюда — акцент на возрастающих угрозах социального, политического и экономического характера, связанных с содержанием зачастую неравноправных информационных обменов и влиянием иностранных игроков на национальное информационное пространство.

США и ЕС последовательно демонстрируют нежелание рассматривать вопросы угроз информационного содержания в более широком контексте национальной безопасности, а также признавать принцип государственного суверенитета в киберпространстве в ущерб трансграничному доступу и распространению данных [Сондерс 2013].

Беспокоящий Россию вопрос потенциально дестабилизирующего информационного влияния на социально-политическую сферу отдельных государств тесным образом связан с понятием информационной политики, посредством которой и осуществляется такое воздействие. *Информационная политика* государства, являясь составной частью внешней и внутренней политики, представляет собой «совокупность целей, отражающих национальные интересы этого государства в информационной сфере, стратегических направлений их достижения (задач), а также систему мер их реализующих»<sup>4</sup>. Ряд других, взаимодополняющих определений рассматривает информационную политику как: (а) государственное управление информационной сферой, состоянием общественного сознания, системой средств массовой информации и коммуникации [Попов 2001]; (б) способность и возможность субъектов политики воздействовать на сознание, психику людей, их поведение и деятельность с помощью информации в интересах государства и гражданского общества [Попов 2001]; (в) способ поддержания дискурса в сфере власти; совокупность взаимосвязан-

ных действий государства, направленных на создание условий получения гражданами необходимой информации [Петрунин 2007]; (г) политику государства в отношении субъектов информационной деятельности, а также информационных инструментов воздействия на социум, которыми пользуются в своих целях субъекты экономической и политической деятельности [Социальная информатиология 2007].

Общей понятийной основой перечисленных определений является идея воздействия государства на информационную сферу в интересах этого государства и его граждан. При этом воздействие может оказываться как официально самим государством, так и неофициально посредством иных субъектов. Это позволяет выделить *два типа и одновременно уровня государственной информационной политики — официальный и неофициальный*. Каждый из них определяется государственными интересами, наряду с задачами и мерами по их осуществлению. Говоря о государственном интересе в сфере внешней политики, стоит оговориться, что они воплощают в себе интересы властной элиты этого государства или — в случае с формальными (интеграционными группировками или союзы) и неформальными коалициями — элит сразу нескольких государств.

## 2

Одними из основных субъектов всемирной информационной сети являются глобальные Интернет-сервисы. При этом их вовлеченность в реализацию широко понимаемой информационной политики государств как посредством их официального присутствия, так и в неофициальном виде возрастает.

Государственная информационная политика претерпела радикальные изменения не только в результате распространения всемирной сети, но и после революционных перемен в самом Интернете, ознаменованных появлением так называемой

<sup>4</sup>Концепция государственной информационной политики Российской Федерации. [Электронный ресурс]. URL: <http://www.unesco.kz>.

Веб 2.0. Оно подтолкнуло развитие новых инструментов «публичной дипломатии» и росту представлений о возможности сознательного наращивания «мягкой силы» страны посредством этих инструментов.

Термин Веб 2.0 описывает переход всемирной паутины на новую стадию развития, которая характеризуется более динамичным обновлением контента за счет вовлечение пользователей в круг его производителей. Важнейшим элементом современного этапа развития Интернета стало распространение виртуальных социальных сетей. Для Веб 2.0 характерно: (1) использование современных подходов в оформлении интерфейса (веб-дизайн), включая шрифты, цвета, структуру и форматы взаимодействия с пользователем; (2) создание приложений, основанных на доступе в Интернет, в противовес приложениям изолированного (офф-лайнового) характера; (3) возникновение разнотипных Интернет-сервисов, позволяющих физическим и юридическим лицам взаимодействовать с широким кругом пользователей; (4) наличие у пользователя возможности выразить свое мнение в виртуальном общественном пространстве; (5) как следствие, создание психологического климата взаимосвязи и причастности при использовании таких приложений и веб-сайтов.

США первыми осознали преимущества нового этапа развития сети и роль, которую Веб 2.0 способен сыграть в государственной информационной политике. В ходе предвыборных кампаний Барака Обамы в 2008 и в 2012 годах его штаб активно использовал все сопряженные с данным феноменом технологии. В соответствии с новыми принципами, США реформировали свою публичную дипломатию и сконцентрировались на поддержке создания и популяризации глобальных Интернет-сервисов. По прогнозным оценкам координатора Государственного департамента

Алека Росса, для сохранения американского глобального экономического лидерства, количество американских Интернет-сервисов и компаний должно увеличиться в ближайшие 2–3 года в несколько раз<sup>5</sup>.

При осуществлении своей информационной политики государство (прежде всего его политический класс) исходит из конкретных интересов, задач и мер. Стратегические интересы Соединенных Штатов в информационной сфере обширны и многоплановы. При этом традиционно ключевым приоритетом для США остается задача сохранения и упрочения своего глобального лидерства и распространения демократии в мире<sup>6</sup>. С учетом этой цели необходимо рассматривать набор и эффективность применяемых Вашингтоном инструментов официальной и неофициальной информационной политики.

*Официальную информационную политику* США наиболее уместно рассматривать в контексте публичной дипломатии. Новое концептуальное звучание ей придали государственный секретарь Х. Клинтон, возглавлявшая американскую дипломатию в течение первого срока пребывания у власти Б. Обамы, ее заместитель по вопросам публичной дипломатии Дж. Макхейл и советник по инновационным технологиям А. Росс. Под влиянием сформулированных этими представителями американского внешнеполитического истеблишмента подходов, обновленное понимание публичной дипломатии оказалось тесно увязано с использованием инструментов Веб 2.0 во внешнеполитической практике США<sup>7</sup>. В круг ключевых задач такой деятельности были включены: усиление целенаправленного влияния на зарубежную аудиторию; формирование у зарубежной аудитории положительных взглядов на цели и ход реализации проводимой США внешней и внутренней политики, с целью *добровольного принятия соответствующих*

<sup>5</sup>[http://www.youtube.com/watch?v=bxFPW\\_Lf9ao](http://www.youtube.com/watch?v=bxFPW_Lf9ao)

<sup>6</sup>National security strategy 2010. [Электронный ресурс]. URL: [http://www.whitehouse.gov/sites/default/files/rss\\_viewer/national\\_security\\_strategy.pdf](http://www.whitehouse.gov/sites/default/files/rss_viewer/national_security_strategy.pdf)

<sup>7</sup>IT Strategic Plan: Fiscal Years 2011–2013–Digital Diplomacy. 2010. [Электронный ресурс]. URL: <http://www.state.gov/m/irm/rls/148572.htm>

установок; создание благоприятных условий и обеспечение поддержки общественным мнением зарубежных стран конкретных акций Соединенных Штатов на международной арене; строительство долгосрочных и доверительных отношений с зарубежной аудиторией; достижение лучшего понимания ценностей и институтов США за рубежом; расширение взаимодействия американских граждан и правительства с населением других стран мира; повышение привлекательности и улучшение имиджа государства.

Для достижения всех этих задач был налажен алгоритм взаимодействия американских дипломатов с зарубежной аудиторией посредством глобальных Интернет-сервисов, в том числе «Facebook», «Diplopedia», «Twitter», «LinkedIn», «Communities@State». По официальным сведениям, у Государственного департамента имеется свыше 200 официальных аккаунтов в социальных сетях, 100 из которых связаны с посольствами. Целый ряд отделов американского внешнеполитического ведомства занимается исключительно цифровой дипломатией, социальными сетями и сетевыми сообществами.

*Центр электронных коммуникаций* отвечает за поддержку нескольких собственных платформ социальных сетей ведомства, предназначенных для ведения официального представительства дипломатической службы, например – блог «DipNote», официальный твиттер-канал «@StateDept», а также официальная страница в «Facebook». Сотрудники этого подразделения поддерживают официальные твиттер-каналы на многих языках.

Персонал *Отдела быстрого реагирования* наблюдает за реакцией социальных сетей на процессы, которые потенциально могут иметь значение для национальных интересов США.

Сотрудники *Отдела по изучению аудитории* разрабатывают аналитические обзоры социальных сетей, включая визуализацию собранных данных. Эти обзоры вместе с анализом результатов публичной дипломатии, исследованиями аналитиков и данны-

ми опросов общественного мнения публикуются на сайтах программы «управления знаниями». Они же оценивают эффективность тех или иных мероприятий и инструментов в сфере внешней информационной политики.

*Отдел сетевой активности* отвечает за управление несколькими платформами социальных сетей, включая четыре страницы Государственного департамента в «Facebook» с аудиторией, превышающей миллион пользователей. К числу платформ относятся «Электронный журнал о США» (Ejournal USA), «Вызовы демократии» (Democracy Challenge), «Глобальные дискуссии о климате» (Global Conversations: Climate) и проект «CO.NX», предоставляющий возможности проведения интерактивных мероприятий ведомства. Отдел разрабатывает для этих страниц мобильные приложения и обеспечивает трансляцию в социальных сетях. Под его управлением находятся сайты на различных языках, включая арабский, китайский, фарси, французский, русский и испанский, созданные для улучшения образа Соединенных Штатов в различных регионах мира.

*Отдел по электронной информационно-просветительской работе*, располагающийся в Центре стратегической коммуникации по предотвращению терроризма, основное внимание уделяет противодействию экстремизму и дезинформации о США в Интернете. Одна из задач отдела – создание видеоряда, представляющего экстремистов в невыгодном свете.

Официальная миссия *Отдела политики, планирования и ресурсов* – контроль над реализацией задач публичной дипломатии, осуществляемой через социальные сети, с целью предотвращения утечки важной информации. Отдел также служит связующим звеном между государством и различными узлами публичной дипломатии в рамках общей программы.

Стоит заметить, что подобные структуры созданы не только в Государственном департаменте, но и в Центральном разведывательном управлении, Пентагоне, а также в Агентстве международного разви-

тия США. Они заняты анализом международных и национальных социальных сетей, блогов, чатов, а также транслируют позитивную информацию о Соединенных Штатах в Интернете. Однако если Государственный департамент в основном сконцентрирован на официальной дипломатии в Интернете, деятельность последних структур, по всей видимости, имеет более неофициальный характер. В структуре ЦРУ был создан отдел Центр открытой информации, осуществляющий мониторинг зарубежных Интернет-СМИ и оперативно реагирующий на негативную информацию о США через блоггеров и неофициальных партнеров в социальных сетях.

Тем не менее, говоря о *неофициальной информационной политике*, представляется уместным рассматривать иные, более автономные от правительственных структур организации. Неофициальный трек информационной политики в интересах государства и ее властной элиты в основном осуществляется негосударственными субъектами, например, самими Интернет-сервисами.

### 3

В начале 2000-х годов традиционный для Вашингтона с 1970-х годов курс на распространение демократических ценностей и поддержку институтов гражданского общества в зарубежных государствах и противодействие репрессивным политическим режимам, трансформировался к концепцию «смены режимов» — смену политической власти на более демократичную (или более лояльную по отношению к тем, кто выступает в качестве лидера демократизации). Элементы ненасильственной смены режимов, по мнению экспертов, применялись и в ходе «арабской весны» [Филимонов 2012]. Один из теоретиков ненасильственного свержения власти является глава Института А. Эйнштейна — профессор Дж. Шарп. Ряд сформулированных им критериев может быть использован при определении методов реализации информационной политики в интересах внешнего государства.

Дж. Шарп выделил ряд объектов, подлежащих дискредитации и блокированию с целью «мягкого» свержения власти: (а) авторитет власти (уверенность народа в том, что власть легитимна и что его моральный долг — ей подчиняться); (б) человеческие ресурсы — число и значение лиц и групп, которые выполняют указания, сотрудничают или предоставляют помощь своему правительству; (в) умения и знания, необходимые режиму для выполнения конкретных действий; (г) нематериальные факторы — психологические и идеологические стереотипы, обеспечивающие лояльность населения; (д) материальные ресурсы — степень контроля или доступа правительства к имуществу, природным и финансовым ресурсам, экономической системе, а также к средствам связи и транспорта; (е) санкции — необходимые для существования режима и проведения его политики наказания, грозящие или применяемые против неповинующихся или отказывающихся сотрудничать [Sharp 2003].

По мнению других американских исследователей, существует и более компактный алгоритм действий, способных привести к падению режима. Для этого вполне достаточно разрушения монополии государства на власть, формирования открытого общества и сетевых содружеств людей, объединенных схожими идеями, а также налаженная посредством социальных сетей связь со сторонниками из стран «свободного мира». Вполне очевидно, что в обоих случаях перечисленные меры возможно реализовать главным образом с помощью спланированной информационной политики, где Интернет-сервисам отводится одна из ключевых ролей. Этому способствуют не только их возможности по координации и формированию протестных сообществ, но и всё большая мультифункциональность этих площадок, порой замещающих традиционные средства массовой информации в странах, где журналистская деятельность контролируется государством.

Широко известно, что подавляющее большинство глобальных Интернет-серви-

сов создаются американскими компаниями и действуют в соответствии с законодательством США<sup>8</sup>. При этом в национальных сегментах сети Интернет в большинстве стран они продолжают укреплять свои позиции и уже в ближайшие годы американские сервисы, такие, как *Facebook*, *Twitter*, *Google*, *Youtube*, *Wikipedia* могут занять лидерские позиции и там, где до недавнего времени преобладали местные игроки. Закономерно, что в «Международной стратегии США в киберпространстве» содержится призыв Соединенных Штатов к гражданам всего мира «использовать медиа-системы для самовыражения, обмена информацией, наблюдением за выборами», а также для «разоблачения коррупции, создания социальных и политических движений»<sup>9</sup>. Одним из примеров новой и набирающей популярность Интернет-площадки может считаться «Change.org» — онлайн-сервис подачи петиций национальным правительствам по всему миру. При всей открытости и пользе подобных платформ, действительно способных приводить к позитивным изменениям в жизни граждан и повышению эффективности функционирования государства, нельзя с полной уверенностью рассматривать их в качестве объективных информационных площадок.

Появление Веб 2.0, со свойственной ему открытостью и равным участием пользователей в различных процессах, расширило и возможности по манипулированию этими пользователями. Несмотря на то что на современном этапе развития сети Интернет власть позиционирует себя как равного субъекта информационного пространства, открытого для диалога и влияния простых граждан на политическую и общественную жизнь, она тем не менее «продолжает осуществлять контроль и вертикальную убеж-

дающую коммуникацию, однако контроль теперь маскируется под отсутствие контроля, а вертикальная коммуникация — под горизонтальную». Интерактивность и свобода выражения допускаются лишь в определенных пределах и подвергаются модерации, чтобы «выводить к необходимому результату в оффлайне»<sup>10</sup>.

Существенным аргументом, подкрепляющим данное объяснение, является использование пользовательских данных американскими Интернет-сервисами. Помимо того, что весьма вероятным становится факт получения этой информации американскими спецслужбами (подтверждением такого сотрудничества служит оглашение Э. Сноуденом данных о секретной программе «Prism»), уже само обладание иностранными компаниями масштабным объемом данных о внешней аудитории не может не настораживать. Благодаря тотальной измеримости социальных медиа, фиксируется каждое нажатие кнопки «like» и «share», каждый переход по ссылке и посещение новой страницы. Это позволяет собрать и учесть практически неограниченное количество информации о пользователях, включая адреса электронной почты, истории поведения в поисковых системах и социальных сетях, предпочтения и мнения по самому широкому спектру вопросов, а также данные об оффлайн активности благодаря геолокации. За счет сбора данных о миллионах пользователей и соответствующей обработки можно не только узнавать предпочтения и настроения широких масс, но и предсказывать их реакцию и действия, направляя их в нужное политическое русло<sup>11</sup>.

Одновременно популярные американские Интернет-сервисы не могут не учитывать интересов государства, с которым они официально сотрудничают по целому ряду других вопросов и, более того, в

<sup>8</sup>Доклад Фонда развития гражданского общества «Рунет сегодня: исследование российского интернета». [Электронный ресурс]. URL: <http://civilfund.ru/mat/1>

<sup>9</sup>International Strategy for Cyberspace. 2011. [Электронный ресурс]. URL: [http://www.whitehouse.gov/sites/default/files/rss\\_viewer/international\\_strategy\\_for\\_cyberspace.pdf](http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf)

<sup>10</sup>Доклад Фонда открытой новой демократии «Власть и контроль в мире социальных сетей. Предвыборные кампании в интернете: опыт Европы и США. М.2013. С.7.

<sup>11</sup>Там же. С.13.



юрисдикции которого осуществляют свою деятельность.

Подтверждением того, что укрепление позиций американских Интернет-сервисов в глобальном информационном пространстве способствует реализации политических интересов США, становится и наблюдаемая неравномерность его содержательного наполнения. В условиях практически неограниченного разнообразия контента, размещенного в сети Интернет, во многих случаях, наиболее доступной оказывается информация, соответствующая приоритетам Соединенных Штатов. В значительной степени США продолжают задавать повестку дня глобальных информационных ресурсов.

Такой «перекос» происходит не столько по технологическим причинам, в результате сознательной модерации или благодаря использованию персональных данных, а в силу отсутствия противовеса в виде конкурентоспособной информационной политики со стороны других государств. Стоит отметить, что большинство правительств слабо владеют принципами Веб 2.0 и не действуют в полной мере современные инструменты медиа-влияния на аудиторию. В качестве примера — включение американских дипломатов в диалог с аудиторией посредством «Twitter» способствует донесению их позиции. В то же время пресс-службы других стран стремятся использовать этот сервис в более традиционном для них виде изложения официального мнения, в формате монолога, что оказывается неэффективным. В последнем случае контент зачастую никак не адаптируется с учетом интересов и привычного стиля общения соответствующей аудитории.

Именно от конкурентоспособности содержания, его приспособленности к особенностям потребителя, зависит эффективность использования глобальных Интернет-сервисов в информационной политике государства. От наличия альтернативных источников такой качественной

информации зависит характер освещения актуальной политической проблематики на виртуальных социальных площадках, который может быть как сбалансированным, так и предвзятым. Технологические барьеры и особенности регулирования в данном случае имеют второстепенное значение. Тем не менее о сбалансированности говорить не приходится.

Между тем вполне вероятно, что достижение содержательного баланса в информационном пространстве могло бы содействовать продвижению стран в диалоге о формировании глобального информационного режима. Пока же национальный контент не окажется конкурентоспособным в сравнении с ресурсами информационного влияния США, информационное пространство будет заполнено неравномерно, и у Соединенных Штатов будут сохраняться достаточные стимулы блокировать любые международные договоренности.

Подобное мнение о роли контента в структурировании информационного пространства разделяют и американские официальные представители. Обращаясь к проблеме появления деструктивной информации на общественных Интернет-площадках госсекретарь Х. Клинтон заявила: «История показывает, что наилучшим ответом на порочащие высказывания является не их запрещение и блокировка, а подавление за счет преобладающего осуждения. Переводя проблему в плоскость дискуссий, правда будет только усиливаться, а слабые и ложные мнения и высказывания окажутся дискредитированы, пусть не сразу, но в конечном счете»<sup>12</sup>. Подобное высказывание наглядно демонстрирует подход самих США к регулированию негативных проявлений свободы самовыражения в интернете, пусть он, возможно, и не единственный. В качестве основного средства противодействия негативного для нее контента Америка использует интенсивное заполнение пространства информацией противоположного характера.

<sup>12</sup>Clinton H. Internet Rights and Wrongs: Choices & Challenges in a Networked World. Feb.15, 2011. [Электронный ресурс]. URL: <http://www.state.gov/secretary/rm/2011/02/156619.htm>

\* \* \*

Сегодня формирование международно-го режима информационной безопасности практически блокировано. Причины этого заключаются в принципиальных расхождениях двух групп государств, представленных США и ЕС, с одной стороны, и Россией и рядом стран ШОС — с другой. Узловым аспектом противоречий является характер и социально-политические последствия информационного воздействия на внутреннюю ситуацию в суверенных государствах.

Несмотря на постоянное увеличение количества субъектов информационного пространства, интересы государств и их властных элит продолжает оставаться определяющими. При этом многообразие форм реализации национальной информационной политики в современных условиях возрастает — она может проводиться как по официальным, так и по неофициальным каналам. В обоих случаях преследуются общие, государственные интересы.

Принципиальное значение для реализации информационной политики имеет способность учитывать тенденции разви-

тия самого Интернета. В современных реалиях принципы Веб 2.0 и возникающие сегодня все новые медиа-технологии определяют уровень конкурентоспособности и эффективности государства в информационной сфере. Расширение влияния американских Интернет-сервисов в глобальном масштабе создает дополнительные преимущества для Соединенных Штатов в этой области. Они обладают существенными возможностями формального и неформального воздействия на такие площадки.

Но существующая несбалансированность глобального информационного пространства в первую очередь определяется не этим. Она становится результатом разрыва в обладании компетенциями по подготовке информационного контента и его адаптации с учетом особенностей Веб 2.0 и современной диверсифицированной аудитории. Без достижения паритета в информационной сфере или хотя бы существенного снижения преобладания Соединенных Штатов, перспективы укрепления международного регулирования информационной безопасности просматриваются слабо.

### Список литературы

- Доклад Фонда открытой новой демократии. Власть и контроль в мире социальных сетей. Предвыборные кампании в интернете: опыт Европы и США. М.: 2013. 227 с.
- Петрунин А.Н. Государственная информационная политика: общий подход // Вестник информационного обеспечения Вооруженных Сил Российской Федерации. — 2007. — №2. С.15–22.
- Попов В.Д. Информациология и информационная политика. М.: 2001. 120 с.
- Сондерс Д. Как избежать эскалации конфликтов в киберпространстве? // Индекс безопасности. — 2013. — №104. Сс. 11–16
- Социальная информациология. Словарь. М.: 2007. 172 с.
- Филимонов Г.Ю. Культурно-информационные механизмы внешней политики США. М. 2012. С. 274.
- Clinton H. Internet Rights and Wrongs: Choices & Challenges in a Networked World. Feb.15, 2011. [Электронный ресурс]. URL: <http://www.state.gov/secretary/rm/2011/02/156619.htm>
- International Strategy for Cyberspace. 2011. [Электронный ресурс]. URL: [http://www.whitehouse.gov/sites/default/files/rss\\_viewer/international\\_strategy\\_for\\_cyberspace.pdf](http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf)
- IT Strategic Plan: Fiscal Years 2011–2013–Digital Diplomacy. 2010. [Электронный ресурс]. URL: <http://www.state.gov/m/irm/rls/148572.htm>
- Potter W. Media Literacy. Thousand Oaks. 2013. 424 p.
- Russia–U.S. bilateral on cybersecurity. Critical terminology foundations / ed. by K.F. Rauscher, V. Yaschenko. Issue 1. 2011. 48 p.
- Sharp G. From Dictatorship to Democracy. Boston, 2003. [Электронный ресурс]. URL: <http://www.aeinstein.org/organizations/org/FDTD.pdf>

# GLOBAL INTERNET SERVICES AS A US FOREIGN POLICY TOOL

ALEXANDER STIKHIN

University of Arkansas in Fayetteville, 72701, USA

Moscow State Institute of International Relations (MGIMO University),

Moscow, 119454, Russian Federation

## Abstract

Nowadays the problem of informational security has become crucial. The development of informational communications and the World Wide Web constantly creates new global challenges. The environment of Internet openness and freedom reveals not only technological threats, but also those related to content. Russia made an attempt to draw attention of the international community to this issue by announcing the draft UN convention on international information security in 2012. However, this proposal disclosed deep contradictions between the Western and Russian approaches to the regulation of the informational space. The tradeoff between freedom of information and protection from destructive information that could negatively affect states and societies appeared to be the primary stumbling block in the dialog between the two sides. While Western countries are trying to avoid Internet censorship, Russia, along with several SCO states, points out the potential risks of an uncontrolled informational space, emphasizing the factor of foreign informational interference and its influence on the social and political situation in different states. These worries are quite reasonable and require a joint resolution.

This issue is closely related with the informational policy of states. Taking as an example the U.S.' informational policy in Internet services, the author comes up with two aspects of the potential benefit that America receives from the proliferation of global Internet services. The technologies themselves and the full spectrum observance of social media activity are thought of as allowing the U.S. to gain wide control over its target audiences. However, what is more important is the U.S.' domination in producing content for global information exchanges. By intensively filling the informational space with favorable content, it creates an unbalanced environment that could turn Internet services into a tool of information influence. Without fill this gap in the production of information resources applicable to the Web 2.0 context between the U.S. and other states, it is difficult to expect progress in negotiating a new architecture of information regulation.

## Keywords:

Informational security; cyber security; social media; Web 2.0; regimen; informational policy; public diplomacy; USA.

## References

- (2007) *Socialnaya Informaciologiya. Slovar* [Social information science. The Dictionary.]. Moscow. 172 p.
- (2010) *IT Strategic Plan: Fiscal Years 2011–2013–Digital Diplomacy*. Available at: URL: <http://www.state.gov/m/irm/rls/148572.htm> (date of access: 10.10.2013)
- (2011) *International Strategy for Cyberspace*. Available at: URL: [http://www.whitehouse.gov/sites/default/files/rss\\_viewer/international\\_strategy\\_for\\_cyberspace.pdf](http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf) (date of access: 10.10.2013)
- (2013) *Doklad fonda otkritoy novoy demokratii. Vlast i kontrol v mire socialnikh setey. Predvibornie kampanii v Internete: opit Evropi i Soedinennikh Shtatov Ameriki* [Report of the Foundation for Open New Democracy. Power and Control in the World of Social Networks. Election campaigns in the Internet: record of Europe and the U.S.]. Moscow. 227 p.
- Clinton H. (2011) *Internet Rights and Wrongs: Choices & Challenges in a Networked World*. Feb. 15, 2011. Available at: URL: <http://www.state.gov/secretary/rm/2011/02/156619.htm> (date of access: 10.10.2013)
- Filimonov G. (2012) *Kulturno-informacionnie mekhanizmi vneshney politiki Soedinennikh Shtatov Ameriki* [Cultural and Information Mechanisms of the U.S. Foreign Policy]. M. 274 p.

- Pereturin A.N. (2007) Gosudarstvennaya informtsionnaya politika: obschij podkhod [State Information Policy: General Approach]. *Vestnik informatsionnogo obespecheniya vooruzhennykh sil Rossijskoj Federatsii*. No. 2. Pp.15–22.
- Popov V.D. (2001). *Informatsiologiya i informatsinnaya politika* [Information science and information policy]. Moscow. 120 p.
- Potter W. (2013) *Media Literacy*. Thousand Oaks. 424 p.
- Rauscher K.F., Yaschenko V. (2011) *Russia–U.S. bilateral on cybersecurity. Critical terminology foundations*. Issue 1. 48 p.
- Sharp G. (2003) *From Dictatorship to Democracy*. Boston: Albert Einstein Institution. 79 p.
- Sonders D. (2013) Kak Izbezhat Eskalacii Konfliktov v Kiberprostranstve? [How to Avoid Escalation of Conflicts in Cyberspace] *Index Bezopasnosti*. №104. Pp. 11–16.