



ФОНД РАЗВИТИЯ
ГРАЖДАНСКОГО
ОБЩЕСТВА

Фильтрация контента в Интернете. Анализ мировой практики.

Фильтрация контента в Интернете. Анализ мировой практики.

На протяжении последних двух лет в российском обществе ведутся дискуссии о допустимых границах государственного регулирования контента в Интернете. Одним из последствий этих дискуссий стало принятие закона № 139-ФЗ от 28 июля 2012 года, в рамках которого появился «Единый реестр запрещенных сайтов», доступ к которым блокируется российскими операторами связи.

Во время дебатов по поводу этого закона и его сторонники, и противники, которые составляют большинство среди лидеров мнений российского сегмента Интернета, активно апеллировали к международному опыту регулирования Сети. При этом с обеих сторон зачастую имело место манипулирование информацией и использование различных штампов, имеющих весьма отдаленное отношение к реальности.

В этом докладе сделана попытка объективно рассмотреть опыт фильтрации нежелательного контента в разных странах мира, а также систематизировать полученную информацию. Основными источниками информации, представленной в докладе, стали публикации в зарубежных научных изданиях, а также специализированные доклады исследовательских организаций и общественных групп.

Вопреки устоявшемуся мнению, ограничения в области интернет-контента являются прерогативой не только авторитарных и тоталитарных политических режимов. На деле, и это описано в данном исследовании, практически все крупные страны мира в той или иной мере ограничивают доступ своих граждан к нежелательной, по мнению властей, информации в Сети – будь то социально-опасная информация, нелегальный контент или экстремистские материалы.

Этот доклад предназначен для широкого круга читателей, интересующихся данной темой. Поэтому некоторые его части, особенно связанные с технической стороной фильтрации контента, подверглись необходимым упрощениям без искажения смысла. Полагаем, что он будет интересен как представителям государственной власти, так и представителям интернет-индустрии, а также работающим в России некоммерческим организациям.

➤ Ключевые выводы доклада:

- На сегодняшний день большинство развитых стран мира прибегают к фильтрации интернет-контента и другим ограничениям свободы в Сети. Однако цели, задачи и конкретные механизмы реализации подобных ограничений существенно варьируются;

- Можно выделить следующие категории контента, которые подвергаются фильтрации в различных странах мира: политический контент; социально-опасная информация; контент, связанный с национальной безопасностью; сайты и сервисы, нарушающие экономические интересы; специализированные интернет-инструменты и социальные сервисы;

- Методы цензуры контента в Интернете можно разбить на две категории: нетехнические и технические. К категории нетехнических методов относятся законы, запрещающие публикацию того или иного контента, давление на интернет-провайдеров, владельцев сайтов и пользователей с целью заставить их убрать нежелательные материалы или изменить их и самоцензура. К категории технических методов относится блокирование интернет-ресурсов по IP-адресу, искажение DNS-записей, блокирование сайтов по URL, пакетная фильтрация, фильтрация через HTTP прокси-сервер, нарушение работы сети и фильтрация результатов поиска. Для повышения эффективности механизмов цензуры также активно используются различные методы сбора информации в Интернете. Из-за сложности и несовершенства технических инструментов обхода фильтров, к ним прибегают не более двух процентов пользователей даже в тех государствах, где фильтрации подвергается большое число интернет-ресурсов.

- На основании общности задач и доводов, которые страны используют для обоснования вмешательства в Интернет, а также схожести инструментов, решающих данную задачу, можно выделить 5 культурно-страновых моделей фильтрации контента в Интернете: азиатская модель, ближневосточная модель, рестрикционная модель, континентальная модель и либеральная модель. Азиатская модель характеризуется расплывчатым определением в законах тех категорий контента, которые должны подвергаться блокировке, что дает правительствам стран широкие полномочия по фильтрации контента как из общественно-нравственных, так и из политических соображений. На фильтрацию контента в рамках ближневосточной модели основное влияние оказывает религиозный фактор – блокировке подвергаются ресурсы, противоречащие нормам ислама, включая некоторые категории правозащитных сайтов. Рестрикционная модель фильтрации распространена в странах с крайне нестабильной политической обстановкой и характеризуется блокированием ресурсов радикальной политической оппозиции, зачастую исламистского толка. Континентальная модель предполагает четкое законодательное обозначение тех категорий контента, которые подвергаются фильтрации. К данным категориям не могут относиться политические или правозащитные ресурсы, а исключительно социально-опасный контент и сайты, систематически нарушающие авторские права. Либеральная модель характеризуется отсутствием систематической фильтрации контента. Вместо этого власти стремятся закрывать нарушающие закон ресурсы и преследуют их владельцев. Россия в соответствии с данной классификацией относится к континентальной модели ограничений в Сети.

- Российский закон о «черных списках интернет-сайтов» основан на опыте британской системы фильтрации нежелательного контента под названием Cleanfeed. Данная система направлена на блокирование доступа интернет-пользователей к детской порнографии и сервисам, систематически нарушающим авторские права. Оператором реестра запрещенных сайтов в Великобритании выступает негосударственный фонд, а блокировка сайтов осуществляется при помощи двухэтапного механизма, что позволяет избежать избыточного блокирования сторонних сайтов.
-

- В качестве рекомендаций для России можно выделить как меры по устранению существенных недостатков действующего законодательства, связанного с регулированием Интернета, так и создание механизмов, не нарушающих функционирование крупных интернет-сервисов, но препятствующих провокациям, связанным с распространением призывов к насилию, в том числе, при помощи специально созданных для этого аккаунтов. От корректности и адекватности государственного подхода к регулированию Сети во многом зависит, сохранят ли российские интернет-компании лидирующие позиции в Рунете.
-

- Системным изучением состояния свободы слова в Интернете в различных странах мира занимаются организации правозащитного толка, зачастую ангажированные политически: Freedom House, «Репортеры без границ» и Open-Net Initiative. Наиболее масштабные исследования по этой теме проводит организация Freedom House, однако объективность этих исследований, особенно в части России и некоторых других стран, находится под вопросом;
-

- Роль социальных сетей и сервисов в событиях, получивших название «твиттер-революций», во многом переоценена. Использование социальных сервисов, прежде всего Twitter, являлось прерогативой узкой прослойки протестующих, значительную долю среди которых составляли журналисты и эмигранты. В то же время, интернет-сервисы стали оперативным источником фото- и видеоконтента с места событий, который подхватывался традиционными СМИ с большой аудиторией, создавая «эффект информационного бумеранга».

➤ Содержание доклада:

Стр. 1	Введение
Стр. 2	Ключевые выводы доклада
Стр. 5	Рейтинги свободы в Интернете: реальность и ее искажения
Стр. 11	Сферы применения фильтрации интернет-контента, декларируемые цели и задачи
Стр. 17	Средства и методы фильтрации контента в Интернете
Стр. 27	Модели цензуры в Интернете
Стр. 34	Способы обхода интернет-фильтрации
Стр. 37	Пример: США
Стр. 39	Пример: Великобритания
Стр. 43	Пример: Китай
Стр. 52	Пример: Иран
Стр. 56	Социальные медиа и кризисы политической легитимности. Возможные меры реагирования со стороны властей.
Стр. 65	Рекомендации для России.

➤ В работе над докладом принимали участие:

- Станислав Апетьян
- Андрей Ковалев
- Александр Файб

Рейтинги свободы в Интернете: реальность и ее искажения

Увеличение числа интернет-пользователей по всему миру и неуклонный рост экономического и политического значения Интернета привели к тому, что начиная с середины 90-х годов XX века государства стали искать оптимальные механизмы регулирования формирующегося коммуникационного пространства, принципиально отличного по своей структуре от традиционных средств связи и информации.

Одновременно с этим стали формироваться и центры исследований вопросов, связанных с Интернетом. В частности, на базе крупнейших университетов мира появились специализированные лаборатории, занимающиеся изучением различных аспектов функционирования Сети – Berkman Center for Internet & Society при Гарвардском университете, Oxford Internet Institute и другие.

Однако системное изучение вопросов государственного регулирования Сети взяли на себя некоммерческие организации правозащитного толка, что естественным образом повлияло на характер подобных исследований. В настоящее время три организации на постоянной основе занимаются составлением рейтингов «интернет-свободы»:

- Freedom House
- «Репортеры без границ»
- OpenNet Initiative

Каждая из этих международных организаций готовит ежегодные исследования, которые, в том числе, содержат карту свободы слова в Интернете и подразделяют все исследуемые страны на несколько категорий в зависимости от наличия и «уровня» инструментов, ограничивающих свободу высказывания и получения информации в Сети.

➤ Freedom House

Наиболее известным и самым цитируемым в средствах массовой информации по всему миру исследованием подобного рода является ежегодный доклад Freedom on the Net организации Freedom House, финансируемой преимущественно правительством США. Последний, второй по счету, доклад вышел в сентябре 2012 года.

Само появление подобного ежегодного исследования стало следствием выступления госсекретаря США Хиллари Клинтон о значимости свободы Интернета, которая была произнесена в январе 2010 года¹. В этом выступлении Клинтон, в частности, заявила:

«Берлинская стена стала символом разделенного мира и определила целую эпоху. Сегодня остатки этой стены выставлены в этом музее - где им и место. А новой знаковой инфраструктурой нашего времени стал интернет. Вместо того чтобы разделять, он призван соединять. Но одновременно с распространением сетей по всему миру, на замену видимым стенам приходят виртуальные. Некоторые страны возвели электронные барьеры, которые преграждают их народу доступ к отдельным частям мировых сетей. Они исключают отдельные слова, имена и фразы из результатов поиска. Они вторгаются в личное пространство граждан, выступающих с ненасильственной политической речью. Подобные действия противоречат Всеобщей декларации прав человека, которая гласит, что все люди имеют право "искать, получать и распространять информацию и идеи любыми средствами и независимо от государственных границ". С распространением таких ограничительных мер во многих странах мира опускается новый, информационный занавес. По ту сторону барьера распространяемые в интернете видеоклипы и посты в блогах превращаются в самиздат наших дней. <...>

Я горда тем, что уже сейчас Государственный департамент более чем в 40 странах помогает людям, которым затыкают рот деспотические правительства. Мы поднимаем этот вопрос как приоритетный также в ООН, включив пункт о свободе интернета в первую резолюцию, внесенной нами на рассмотрение Совета по правам человека ООН после нашего возвращения в этот орган.

Мы также поддерживаем разработку новых инструментов, помогающих гражданам осуществлять свое право на свободу самовыражения в обход политической цензуры. Мы предоставляем финансовую помощь группам во всем мире, чтобы открыть доступ к этим инструментам на местных языках тем, кто в них нуждается, и научить их, как без риска для себя подключаться к интернету. Соединенные Штаты уже некоторое время работают в этом направлении, стремясь внедрять указанные программы с максимальной эффективностью. Американский народ и страны, подвергающие цензуре интернет, должны знать, что наше правительство твердо намерено защищать свободу интернета. <...>

Ни одна страна, ни одна группа людей, ни один человек не должен оставаться погребенным под развалинами угнетения. Мы не можем безучастно смотреть на то, как стены цензуры отгораживают людей от общей человеческой семьи. И мы не можем молчать об этих проблемах только потому, что нам не слышны крики о помощи. Давайте же преисполнимся новой решимости сражаться за это дело. Давайте превратим эти технологии в реальную силу прогресса по всему миру и будем и дальше отстаивать эти свободы ради нашего времени и ради нашей молодежи, которая заслуживает всех возможностей, которые мы можем им дать».

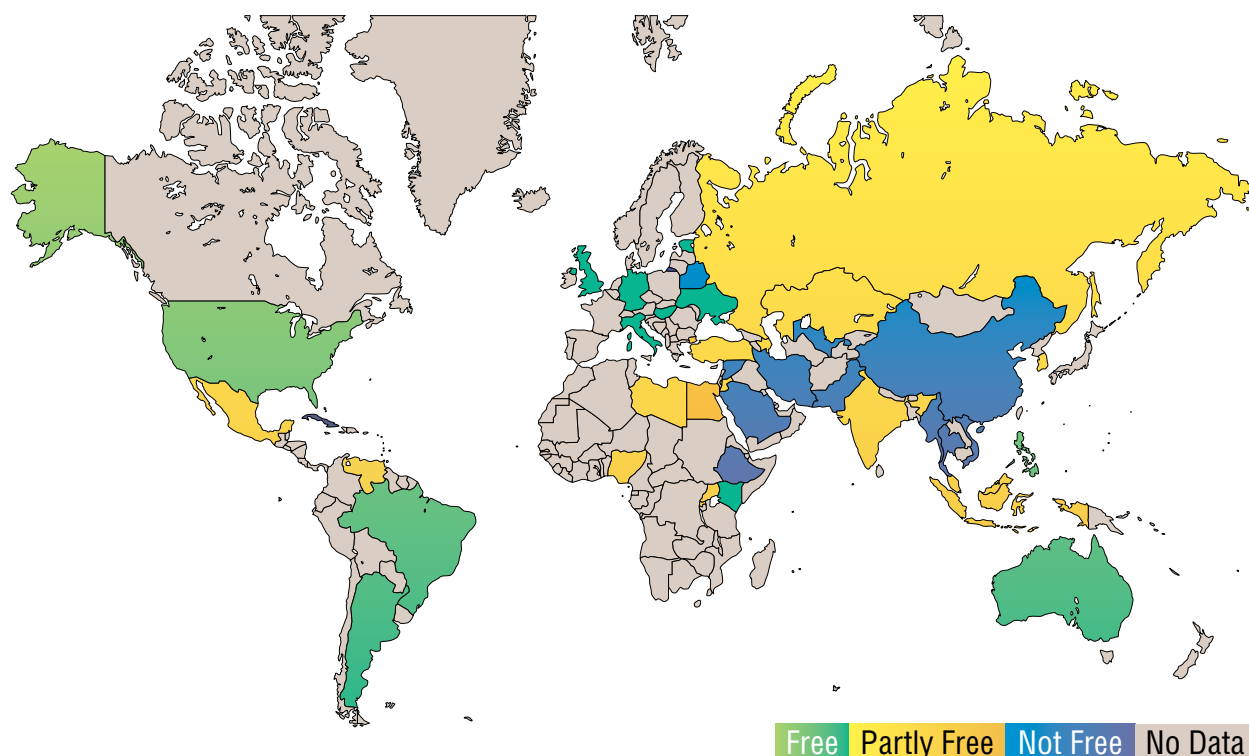
Первый доклад Freedom House 2011 года анализировал свободу Интернета в 37 странах мира. На следующий год объектами анализа экспертов организации стали уже 47 стран, а объем доклада возрос до 657 страниц. Данный материал является наиболее обширным источником информации по вопросам государственного регулирования Сети в различных частях земного шара. Впрочем, он содержит в себе целый ряд существенных недостатков и искажений, о которых пойдет речь ниже.

1. Clinton, H.R. (2010). Remarks on Internet Freedom.

Методология составления рейтинга выглядит следующим образом. Каждой из исследуемых стран были присвоены баллы по трем категориям: «препятствия для доступа к Сети» (от 0 до 25 баллов), «ограничения контента» (от 0 до 35 баллов), «нарушения прав пользователей» (от 0 до 40 баллов). Чем больше баллов получает страна – тем меньше в ней свободы по данному критерию. В конце полученные баллы суммировались, а страна получала итоговую оценку от 0 до 100 баллов. Исходя из этой оценки, страны были разделены на три категории: «свободные» (от 0 до 30 баллов, 14 стран), «частично свободные» (от 31 до 60 баллов, 20 стран) и «несвободные» (от 61 до 100 баллов, 13 стран). В таблице ниже отражено распределение исследованных стран по данным категориям.

«Свободные» страны	«Частично свободные» страны	«Несвободные» страны
Эстония (10 баллов), США (12), Германия (15), Австралия (18), Венгрия (19), Италия (23), Филиппины (23), Великобритания (25), Аргентина (26), Южная Африка (26), Бразилия (27), Украина (27), Кения (29), Грузия (30)	Нигерия (33), Южная Корея (34), Уганда (34), Киргизстан (35), Мексика (37), Индия (39), Индонезия (42), Ливия (43), Малайзия (43), Иордания (45), Тунис (46), Турция (46), Венесуэла (48), Азербайджан (50), Руанда (51), Россия (52), Зимбабве (54), Шри-Ланка (55), Казахстан (59), Египет (59)	Таиланд (61), Пакистан (63), Беларусь (69), Бахрейн (71), Саудовская Аравия (71), Вьетнам (73), Мьянма (75), Эфиопия (75), Узбекистан (77), Сирия (83), Китай (85), Куба (86), Иран (90)

В результате, карта «интернет-свободы» по версии Freedom House выглядит следующим образом:



Составление рейтинга Freedom House, как и большинства подобных исследований, опирается на экспертные интервью. Каждый из экспертов (по одному на каждую страну) отвечает на вопросы по специальному опросному листу. Примечателен тот факт, что Freedom House не приводит имен исследователей, которые отвечали на вопросы по России и еще нескольким странам, отмечая, что они «пожелали остаться анонимными», в то время как по большинству

других рассматриваемых в докладе государств имена экспертов приводятся. Подобная позиция не позволяет сделать вывод о качестве экспертизы, которая использовалась для крайне негативной оценки уровня свободы в Рунете.

Более того, некоторые факты свидетельствуют о явно предвзятой оценке ситуации в России со стороны Freedom House. Так, даже в наименее дискуссионной и политизированной категории «препятствия для доступа к Сети» Россия получила 11 баллов из 25, а, к примеру, Великобритания и США – 1, и 4 балла соответственно. При этом из мотивировочной части исследования следует, что ситуация со свободой получения доступа к Сети в России является в целом благоприятной и ничем принципиально не отличается от ситуации в США и Великобритании, а конфигурация рынка широкополосного доступа во всех трех странах практически идентична. Цены и качество предоставляемых услуг также находятся примерно на одном уровне.

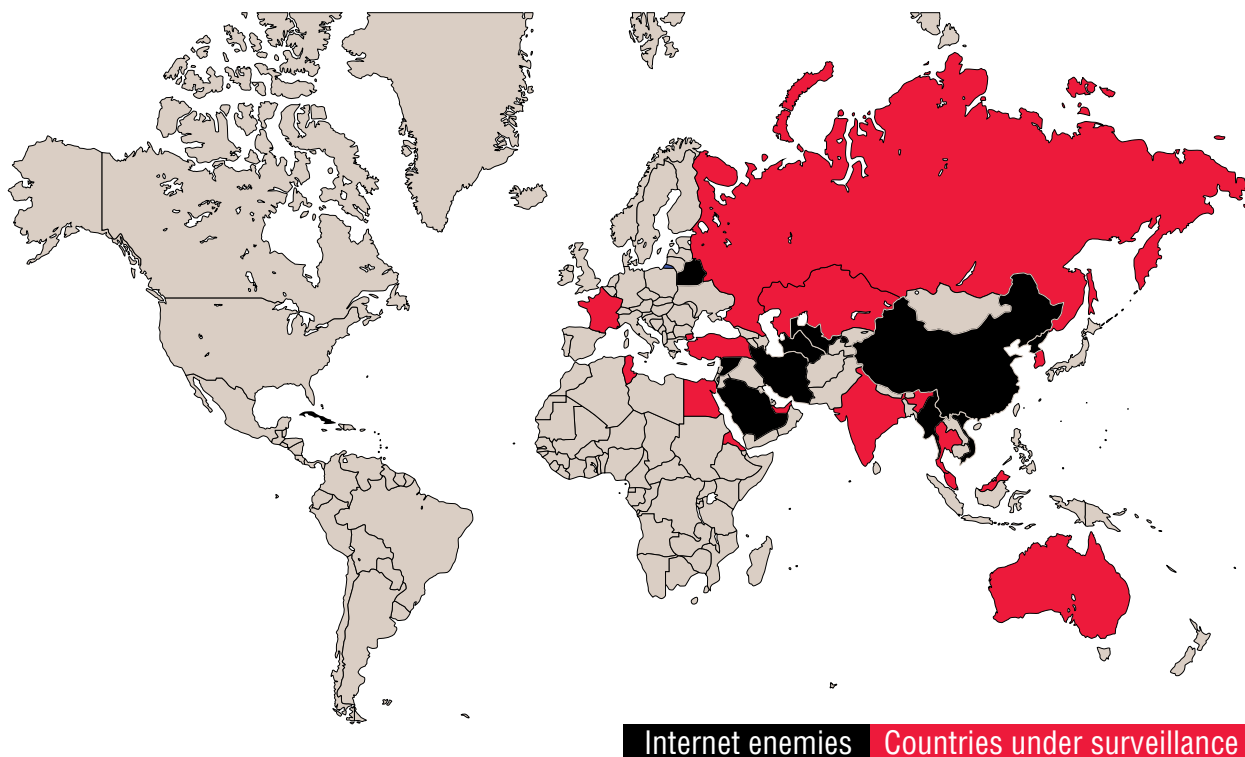
Уровень аргументации, используемый Freedom House для того, чтобы поставить России относительно низкий балл в данной категории, можно оценить по этой цитате из доклада: *«В России отсутствуют законодательные ограничения на предоставление услуг доступа в Интернет, однако нечестная конкуренция, распространенная коррупция и другие подобные препятствия не являются редкостью в этой стране»*. По остальным категориям («ограничения контента» и «нарушения прав пользователей») уровень аргументации аналогичен. В качестве обоснования низкой оценки России приводится не систематическое и законодательно оформленное «притеснение свободы слова в Сети» со стороны государства, а различные ситуативные политические конфликты, а также публикации оппозиционно настроенных СМИ.

➤ «Репортеры без границ»

С 2009 года международная организация «Репортеры без границ» публикует ежегодные аналитические доклады, посвященные «врагам Интернета». Последний подобный отчет был опубликован в марте 2012 года. В нем организация разделила все страны на три категории: «враги Интернета», «страны под наблюдением» и свободные страны. К числу «врагов», существенным образом ограничивающих свободу интернет-пользователей, по итогам исследования были отнесены Бахрейн, Беларусь, Мьянма, Китай, Куба, Иран, Северная Корея, Саудовская Аравия, Сирия, Туркменистан, Узбекистан и Вьетнам.

В категорию «стран под наблюдением» попали те государства, в которых исследователи нашли признаки определенных ограничений, масштаб которых, однако, не позволяет отнести их к категории «врагов Интернета». В перечень «наблюдаемых» стран вошли: Австралия, Египет, Эритрея, Франция, Индия, Казахстан, Малайзия, Россия, Южная Корея, Шри-Ланка, Таиланд, Тунис, Турция и Объединенные Арабские Эмираты. Остальные страны, по мнению экспертов «Репортеров без границ», могут считаться свободными.

Претензии экспертов организации в отношении России заключаются главным образом в наличии законодательства, направленного на противодействие экстремизму. Также эксперты выражают обеспокоенность судебным преследованием нескольких блогеров, чьи имена слабо известны в России, и кибератаками на оппозиционные ресурсы. Стоит отметить, что это исследование вышло еще до принятия закона №139-ФЗ и появления «единого реестра запрещенных сайтов».

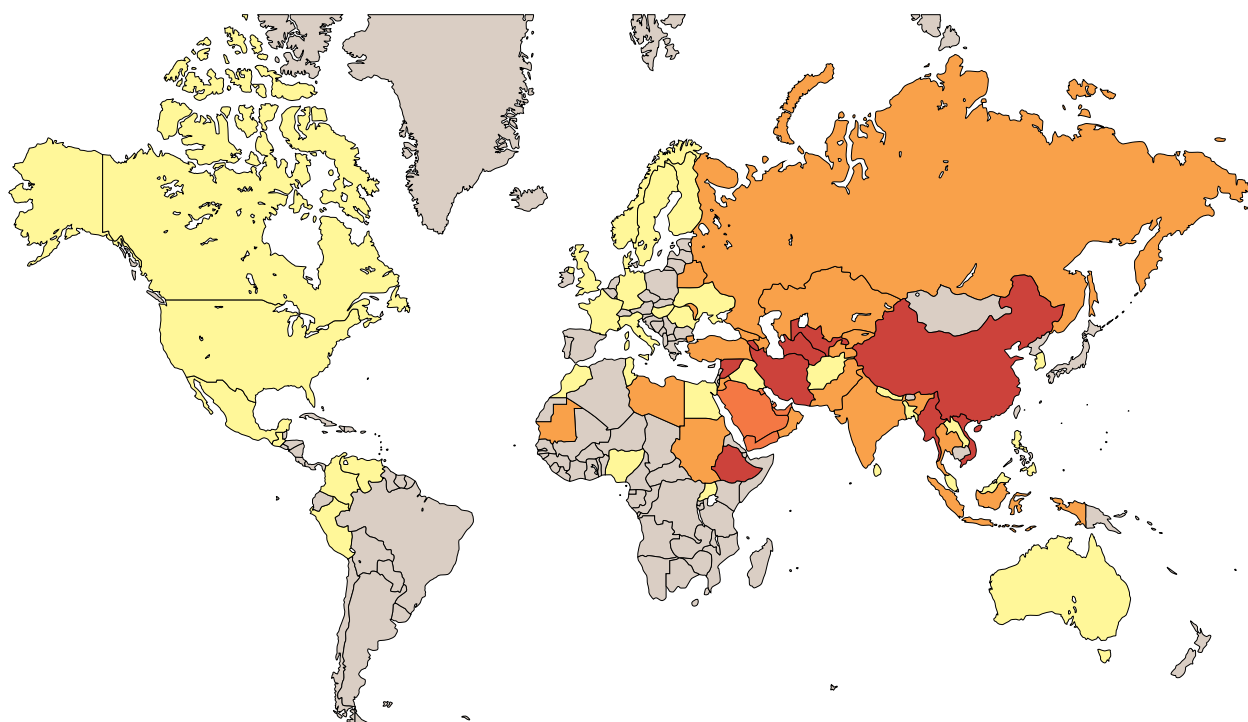


В 2013 году «Репортеры без границ» отказались от публикации традиционной карты интернет-цензуры с обзором ситуации в большом числе стран, подготовив исследование иного формата, предполагающего меньшую дискуссионность и политическую ангажированность. В нем эксперты организации сосредоточились лишь на одном аспекте ограничения свободы в Сети – на государственном отслеживании интернет-активности пользователей. В данном аспекте «Репортеры без границ» выделили 5 главных «врагов Интернета», которыми стали Китай, Вьетнам, Сирия, Иран и Бахрейн, а также пять крупнейших частных компаний, которые занимаются разработкой программного обеспечения для решения подобных задач государственными органами. Примечательно, что все компании, указанные в исследовании, являются западными, а их штаб-квартиры расположены в США, Италии, Германии, Франции и Великобритании.

➤ OpenNet Initiative

Данный проект представляет собой партнерство трех исследовательских центров: «Гражданской лаборатории» Школы международных исследований Мунка при Университете Торонто, Центра Беркмана Гарвардского Университета и SecDev Group из Оттавы. Спонсором проекта выступают Фонд МакАртуров, Фонд Форда, «Открытое общество» Сороса, а также канадские правительственные структуры.

Проект ставит своей целью исследование вопросов, связанных именно с фильтрацией интернет-контента в различных странах мира. На основе проведенных исследований публикуется несколько карт фильтрации интернет-контента в различных странах мира, в зависимости от его специфики. Категорий четыре: политический контент, «социальный» контент (включая обычную порнографию и онлайн-казино), контент, связанный с вооруженными конфликтами, и технический интернет-инструментарий (отдельные протоколы, средства поиска и хостинги). Карта фильтрации политического контента по версии OpenNet, например, выглядит следующим образом:



Levels of Filtering: Pervasive Substantial Selective Suspected No evidence

В случае России, в двух категориях из четырех (политический и «социальный» контент) она отнесена к группе стран с «выборочной» фильтрацией, в двух других категориях какой-либо фильтрации экспертами OpenNet не обнаружено. Впрочем, существенная мотивировка подобного решения отсутствует, так как последний анализ ситуации в интернет-пространстве России и стран СНГ датирован 2010 годом и не отражает ситуацию на сегодняшний день. По большинству других стран ситуация аналогична.

В целом, можно утверждать, что на сегодняшний день не существует полноценного глобального анализа ситуации с ограничениями в области Интернета в различных странах мира, основанного на прозрачной и подверженной сторонней проверке методологии. Сплошное рейтинговое стран и составление карт «интернет-свободы» по всему миру ведет к упрощению и искажению реальной ситуации, что заметно как на примере России, так и на примере других стран, которые анализируются в этом докладе. В этом контексте показательно решение организации «Репортеры без границ» отказаться от «сплошного» анализа всех стран мира и сосредоточиться на более глубоком и подробном анализе отдельных явлений, связанных с ограничениями свободы в Сети.

На сегодняшний день все большее число стран прибегает к фильтрации интернет-контента и другим ограничениям свободы в Сети. Однако цели, задачи и конкретные механизмы реализации подобных ограничений существенно варьируются. В дальнейших главах мы постарались систематизировать международный опыт в данной области и обозначить существующие модели фильтрации интернет-контента, которые демонстрируют различные подходы к решению данной задачи.

Сферы применения фильтрации интернет-контента, декларируемые цели и задачи

По мере увеличения роли Интернета в жизни общества, отношение государства к нему менялось. Все большее количество размещаемого в Сети контента вступало в противоречие с законодательством отдельных стран, их социальными нормами и политической линией властей. Интернет также оказал существенное влияние на ситуацию с интеллектуальной собственностью и телекоммуникациями, поставив под угрозу экономические интересы целых отраслей. Эти тенденции привели к появлению потребности в фильтрации определенных видов контента, и вызвали дискуссии о допустимых пределах вмешательства государства в функционирование Сети.

Для того чтобы понять, какие цели и задачи ставят различные государства при введении тех или иных ограничений, необходимо определить, какие именно типы контента наиболее часто подвергаются цензуре. Для этого целесообразно прибегнуть к методологии OpenNet Initiative², которая предполагает тестирование доступности в исследуемых странах сайтов различной тематики. В этот список включаются как международные, так и локальные ресурсы, посвященные свободе слова и религии, деятельности оппозиционных групп, наркотикам и алкоголю, порнографии, а также ряд специализированных интернет-сервисов. На основании полученных данных можно выделить несколько категорий контента, который становится объектом фильтрации.

Цензура государств, прежде всего, затрагивает материалы на местных языках. Результаты тестирования показали, что в среднем такие сайты блокируются в два раза чаще ресурсов на английском или других международных языках. Например, власти Вьетнама, Узбекистана, Сирии и Эфиопии при высокой доле фильтрации контента на локальных языках, практически не ограничивают доступ к мировым новостным и информационным ресурсам. Ближневосточные государства, такие как Саудовская Аравия, Иран и Объединенные Арабские Эмираты, напротив, активно блокируют сайты на иностранных языках. Это связано и с категорией фильтруемого ими контента – порнографией, которая, по большому счету, интернациональна, и с применяемыми средствами технической фильтрации, разработанными западными компаниями.

2. OpenNet Initiative Access Denied: The Practice and Policy of Global Internet Filtering — Cambridge: MIT Press, 2008.

Сферы применения фильтрации интернет-контента, декларируемые цели и задачи



01

Политический контент

Информация и сайты, посвященные деятельности оппозиционных движений
Сайты, посвященные защите прав человека
Сайты религиозных движений и сект
Информация об этнических меньшинствах



02

Сайты и сервисы, нарушающие экономические интересы

Сайты, нарушающие интеллектуальную собственность
Файлообменные сайты, программы и торрент-трекеры
VoIP (Voice-over-IP) программы и сервисы, позволяющие передавать голос по Интернету



03

Информация, нарушающая социальные нормы

Порнографические сайты
Сайты, посвященные половому просвещению и планированию семьи
Сайты ЛГБТ-тематики
Сайты о наркотиках и алкоголе
Онлайн-казино
Сайты, разжигающие межнациональную и религиозную рознь
Сайты, оскорбляющие государственную религию
Сайты, распространяющие клевету и диффамацию



04

Контент, блокируемый по соображениям безопасности

Сайты экстремистских, сепаратистских и террористических движений
Интернет-ресурсы военных противников
Ресурсы с конфиденциальными данными
Сайты онлайн-мошенников и финансовых пирамид
Массовая рассылка нежелательной почты (спам) и вредоносное программное обеспечение (malware)



05

Интернет-инструменты и социальные сервисы

Инструменты, позволяющие обойти интернет-цензуру
Хакерские сайты и ресурсы с информацией об обходе интернет-цензуры
Социальные сети, площадки для блогов и микроблогов, хостинги видео и изображений
Поисковые системы
Бесплатные почтовые сервисы
Онлайн-переводчики

➤ Политический контент

- Информация и сайты, посвященные деятельности оппозиционных движений, а также сообщения, содержащие критику действующей власти. В ряде стран подобный контент подпадает под формулировку «анти-государственная пропаганда». В частности, по этой статье в 2012 году во Вьетнаме были осуждены несколько блогеров³.
- Сайты, посвященные защите прав человека. Такие сайты блокируются, в частности, в Бирме. Тестирование показало, что там недоступны сайты правозащитных организаций Human Rights Watch, Amnesty International и Burma Watch, а также ресурсы, освещающие состояние дел с правами женщин в стране.
- Сайты религиозных движений и сект, деятельность которых не одобряется государством. В частности, в Китае цензуре подвергается информация о духовной дисциплине Фалуьгун. А в ряде мусульманских стран блокируются ресурсы, направленные на распространение христианства.
- Информация об этнических меньшинствах. Так, Вьетнам подвергает цензуре сведения о племенах монтаньяров.

Именно фильтрация политического контента привлекает наиболее пристальное внимание международных организаций, изучающих свободу в Интернете. Такие действия рассматриваются как нарушение базовых человеческих прав – свободы слова и религии. Все страны, отнесенные «Репортерами без границ» к группе «врагов Интернета»⁴ в том или ином виде ограничивают распространение политической информации. В то же время, фильтрация политического контента не является прерогативой исключительно авторитарных и тоталитарных политических режимов. Весьма схожие явления в странах, которые принято считать демократическими, осуществляются под эгидой обеспечения национальной безопасности или борьбы с радикальными политическими движениями, о чем будет сказано ниже.

➤ Информация, нарушающая социальные нормы

- Порнографические сайты. Большинство стран мира регулирует доступ к порнографическим материалам в Интернете. Отдельные страны, как Саудовская Аравия, пытаются заблокировать данный сегмент полностью, но усилия большинства стран направлены на ограничение доступа к ним несовершеннолетних. Сильно отличается в различных странах понимание того, что считается порнографией – например, в Иране блокируются даже изображения «провокационной одежды». Общим консенсусом же является борьба с детской порнографией.
- Сайты, посвященные половому просвещению и планированию семьи.
- Сайты ЛГБТ-тематики. В ряде мусульманских стран Среднего Востока и Африки под запрет попадают сайты знакомств и форумы для геев и лесбиянок. Белоруссию обвиняют в блокировании ЛГБТ ресурсов под предлогом того, что они содержат порнографию.

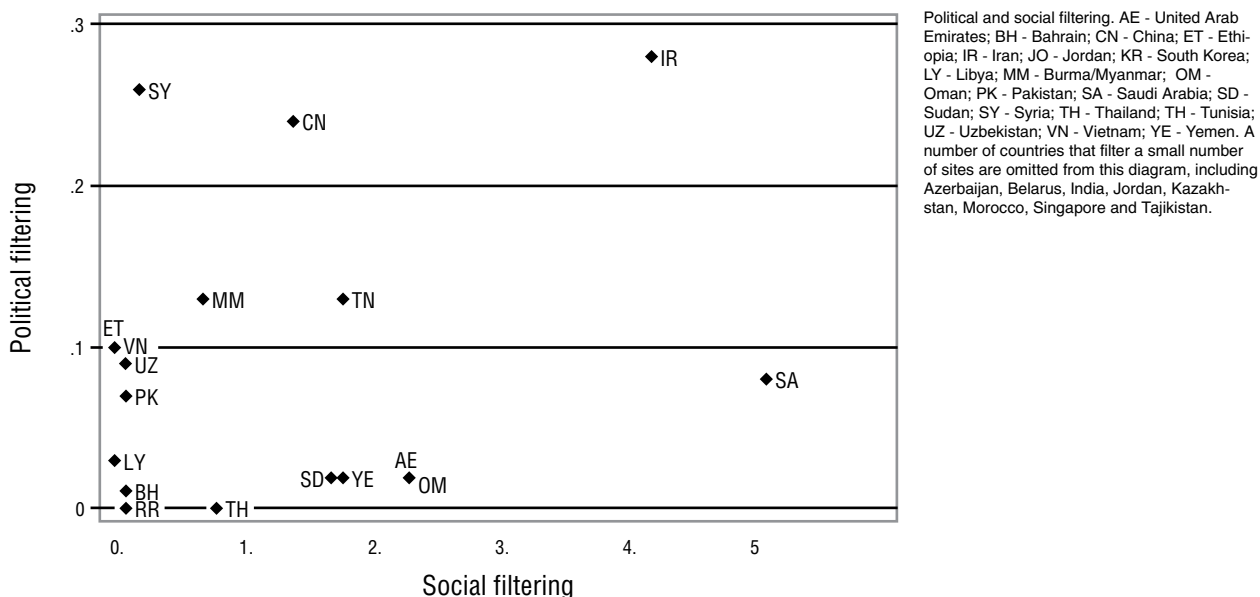
3. James Hookway. Vietnam Convicts 3 Bloggers Over Posts // [The Wall Street Journal] URL: <http://online.wsj.com/article/SB1000872396390444358804578015383720801250.html>

4. Reporters Without Borders, "Internet Enemies Report 2012," 2012.

- Сайты о наркотиках и алкоголе. Наиболее крупные сайты подобного рода попали в блок-списки сразу нескольких коммерческих интернет-фильтров.
- Онлайн-казино. До 2010 года в Италии действовал закон, блокирующий большинство зарубежных интернет-букмекеров и казино. Он был принят под давлением двух организаций, получивших монопольное право на организацию букмекерской деятельности. Однако после серии исков частных компаний и расследования Евросоюза, закон был изменен.
- Сайты, разжигающие межнациональную и религиозную рознь или призывающие к насилию. В России действует законодательство о борьбе с экстремизмом, предусматривающее блокировку подобных интернет-ресурсов. Во Франции и Германии блокируются неонацистские сайты. В 2000 году французский суд вынес громкий вердикт в деле против компании Yahoo, обязав ее ограничить доступ французских пользователей к интернет-аукциону нацистской символики. Дело оказало значительное влияние на всю последующую дискуссию в странах Евросоюза о юрисдикции государств в Интернете.
- Сайты, оскорбляющие государственную религию. В большинстве мусульманских стран блокировались ресурсы, содержащие карикатуры на пророка Мухаммеда.
- Сайты, распространяющие клевету и диффамацию, в частности, в адрес представителей властей.

Ограничение доступа к информации, нарушающей социальные нормы, широко распространено как в демократических, так и авторитарных странах. Большинство таких ограничений поддерживается населением, и поэтому рассматриваются международными организациями как допустимое регулирование Интернета. Впрочем, отдельные страны используют расплывчатые определения «защиты моральных ценностей общества» для цензуры в отношении оппозиционного политического контента. Практика фильтрации «социального» контента сильно отличается от страны к стране, как по способам реализации, так и по тому, что именно подвергается цензуре.

Ниже представлена диаграмма из книги Access Denied: The Practice and Policy of Global Internet Filtering⁵, показывающая распределение стран по шкале социальной и политической фильтрации интернет-контента:



5. OpenNet Initiative Access Denied: The Practice and Policy of Global Internet Filtering — Cambridge: MIT Press, 2008.

➤ Контент, блокируемый по соображениям безопасности

- Сайты экстремистских, сепаратистских и террористических движений. Блокирование применяется как демократическими, так и авторитарными государствами.
- Интернет-ресурсы военных противников. Южная Корея тщательно блокирует сайты Северной Кореи. В Грузии во время и некоторое время после войны с Россией в 2008 году действовали ограничения на доступ к российским сайтам.
- Ресурсы с конфиденциальными данными. В США сайт Wikileaks недоступен с компьютеров федеральных учреждений. Власти Франции в апреле 2013 года потребовали от Wikipedia удаления одной из статей, так как в ней содержалась секретная информация.
- Сайты онлайн-мошенников и финансовых пирамид.
- Массовая рассылка нежелательной почты (спам) и вредоносное программное обеспечение (malware). Блокируется большинством интернет-провайдеров, а также антивирусами и фаерволлами, установленными на компьютерах пользователей.

Грань между блокированием сайтов по соображениям национальной безопасности и политической цензурой не всегда четкая. Правительство США неоднократно обвиняли в политическом преследовании проекта Wikileaks и его основателя Джулиана Ассанжа. Другие страны блокируют ресурсы сторонников сепаратизма, даже если они находятся исключительно в политической плоскости и не являются экстремистскими. С другой стороны, борьба с мошенничеством, спамом и вредоносными программами является рутинной технической работой по обеспечению нормального функционирования Интернета.

➤ Сайты и сервисы, нарушающие экономические интересы

- Сайты, нарушающие интеллектуальную собственность. Особенно жесткое законодательство в этой сфере действует в США. Крупные поисковые системы, в частности Google, фильтруют результаты поиска с учетом жалоб правообладателей.
- Файлообменные сайты, программы и торрент-трекеры. В 2012 году под давлением американских властей был заблокирован на тот момент один из самых посещаемых сайтов Интернета – файлообменный сервис MegaUpload, а его создатели были арестованы. Широко освещается борьба с торрент-трекерами (The Pirate Bay, Demonoid, IsoHunt), которые формально не нарушают закон, но способствуют нелегальному распространению интеллектуальной собственности.
- VoIP (Voice-over-IP) программы и сервисы, позволяющие передавать голос по Интернету, такие как Skype и «Mail.Ru Агент». В Объединенных Арабских Эмиратах и Омане использование таких программ нелегально и карается большим штрафом или тюремным заключением. Причина блокирования VoIP программ двоякая – с одной стороны звонки по ним сложнее отследить и прослушать, с другой стороны, их использование ведет к убыткам компаний стационарной и сотовой связи, которые зачастую связаны с правящими кругами.

Борьба с нарушениями интеллектуальной собственности активно продвигается такими лоббистскими организациями как Американская ассоциация кинокомпаний (МРАА) и Американская ассоциация звукозаписывающих компаний (RIAA). Более того, принятие жесткого законодательства в этой области является условием вступления во Всемирную торговую организацию. Под давлением США Новая Зеландия одной из первых приняла «закон о трех предупреждениях», предусматривающий отключение от Интернета пользователей, систематически скачивающих «пиратские» файлы. Позже подобные законы были приняты или рассматривались в ряде других стран. Блокирование VoIP программ часто рассматривается как недобросовестная конкуренция со стороны телекоммуникационных компаний – пользователи лишаются возможности использовать дешевую интернет-телефонию.

➤ Интернет-инструменты и социальные сервисы

- Инструменты, позволяющие обходить интернет-цензуру. В эту категорию попадают анонимайзеры и сайты со списками прокси-серверов, так как они могут использоваться для обхода государственных фильтров.
- Хакерские сайты и ресурсы с информацией об обходе интернет-цензуры.
- Социальные сети, площадки для блогов и микроблогов, хостинги видео и изображений. В Китае заблокирован Twitter, Facebook, YouTube, Wordpress и ряд других подобных ресурсов, серверы которых расположены за рубежом. Таким образом китайское правительство принуждает своих пользователей использовать местные сервисы, которые легче контролировать и фильтровать публикуемый в них нежелательный контент.
- Поисковые системы. Так, в Китае и на Кубе блокируются американские поисковые системы Google и Bing.
- Бесплатные почтовые сервисы.
- Онлайн-переводчики. Они могут быть использованы как прокси-серверы для обхода цензуры. Помимо этого, с их помощью пользователи могут получить доступ к нежелательной информации на иностранных языках, которую сложно отследить.

Интернет-инструменты и социальные сервисы блокируются авторитарными режимами для предотвращения обхода интернет-фильтров и лучшего контроля за коммуникацией в Сети своих граждан. Только несколько стран, таких как Китай и Куба, полностью ограничивают доступ к крупным иностранным интернет-сервисам. Большинство государств используют блокировку только отдельных материалов, нарушающих действующее законодательство.

Средства и методы фильтрации контента в Интернете

С возникновением потребности в фильтрации контента в Интернете, государства столкнулись с трудностями применения традиционных методов контроля над средствами массовой информации в Сети. Одну из основных проблем для цензоров представляла динамичность социальной составляющей Интернета – огромное количество материала вновь и вновь создается множеством пользователей. Другим препятствием являлся международный характер Сети, когда серверы с информацией зачастую находятся вне юрисдикции и досягаемости правоохранительных органов отдельных стран.

В начале и середине 90-х годов прошлого века среди многих ученых и специалистов господствовала идея, что Интернет в принципе не поддается контролю. В 1998 году президент США Билл Клинтон высказался о тщетности усилий Китая по созданию национальной системы фильтрации Интернета, сравнив ее с «попыткой прибить желе к стене». Но по мере развития Интернета стала очевидна ошибочность этих суждений. Согласно исследованию OpenNet Initiative, если в 2002 году только несколько стран применяли системы фильтрации контента, то к 2007 году их число возросло до 25 (к настоящему времени эта цифра возросла еще почти вдвое). Также законы о блокировании детской порнографии в Сети были приняты в ряде европейских стран. Использование традиционных методов контроля за СМИ в сочетании с новыми техническими средствами позволило государствам ограничивать доступ своих граждан к нежелательным материалам с приемлемой эффективностью.

➤ Классификация систем фильтрации Интернета

Исследование Дерек Бамбаура из Университета Аризоны, проведенное в 2008 году⁶, предлагает классификацию интернет-фильтров, которая абстрагируется от характера блокируемого контента. Вместо этого системы оцениваются по четырем параметрам – открытость, прозрачность, точность и подотчетность. Такой подход позволяет наиболее полно оценить, насколько практика государства соответствует заявленным целям фильтрации, и нарушается ли право граждан на информацию.

6. Derek E. Bambauer Cybersieves // Duke Law Journal. — 2009.

➤ Открытость

Этот параметр оценивает то, насколько явно государство признает фильтрацию Интернета и объясняет свою мотивацию. Так, на сайте подразделения правительства Саудовской Аравии, занимающегося Интернетом, описана действующая система фильтрации. В качестве объяснения, почему правительство считает необходимым блокировать определенный материал, приводятся выдержки из Корана и ссылки на статьи. При попытке посетить нежелательный ресурс, пользователю выдается страница с указанием того, что данный материал заблокирован.

В Китае, напротив, значительная часть фильтрации осуществляется незаметно, а ее применение маскируется под технические ошибки. В результате этого, пользователь может в принципе не осознавать, какой материал блокируется и почему, так как китайские власти официально не признают отдельные эпизоды цензуры. Таким образом, несмотря на всю свою жесткость, система Саудовской Аравии гораздо более открыта, чем китайская – пользователям сообщают, что государство вмешивается в Интернет, и объясняют почему.

➤ Прозрачность

Параметр прозрачности оценивает, насколько четко прописаны критерии, по которым материал подлежит фильтрации. В законах Китая для этого используются расплывчатые формулировки вроде «распространяющий слухи» и «нарушающий национальное единство», которые позволяют блокировать любой материал, не устраивающий цензоров. Франция блокирует доступ к сайтам, разжигающим межнациональную и религиозную рознь. Критерии для определения такого рода материала являются частью уголовного законодательства страны, поэтому возможности для злоупотребления ограничены. Вместе, критерии открытости и прозрачности позволяют определить, на какой уровень контроля информации претендуют власти страны.

➤ Точность

Параметр точности позволяет оценить насколько успешно воплощается заявленная государством политика в области интернет-цензуры. Неотъемлемой проблемой большинства методов интернет-фильтрации является чрезмерное и недостаточное блокирование. При чрезмерном блокировании вместе с нежелательным материалом недоступным оказывается и вполне безобидный. Подобное можно было наблюдать в России, когда вместе с заблокированными ресурсами недоступными становились и сторонние сайты, располагающиеся на одной группе серверов. Обратный эффект наблюдается при недостаточном блокировании – пользователи могут видеть тот контент, который государство рассматривает как вредный.

И чрезмерное, и недостаточное блокирование может быть случайным и преднамеренным. К примеру, имел место случай, когда провайдер в Пенсильвании по ошибке заблокировал более миллиона сайтов, выполняя предписание суда об ограничении доступа к 400 сайтам, содержащим детскую порнографию. В Сингапуре, напротив, несмотря на заявленную государством борьбу с онлайн-порнографией, символически заблокированы только несколько сайтов.

➤ Подотчетность

Данный параметр оценивает уровень участия граждан в политике интернет-фильтрации, проводимой государством. Прошел ли закон, регулирующий Интернет, должный общественный контроль и обсуждение? Могут ли пользователи оспорить то или иное решение цензоров или, напротив, внести на рассмотрение сайт, нарушающий закон?

Закон США об авторском праве в цифровую эпоху (Digital Millennium Copyright Act), регулирующий защиту авторских прав в Интернете, был принят после серии публичных слушаний и рассмотрения в Конгрессе. С другой стороны, политика регулирования интернета в Саудовской Аравии была принята без демократического участия ее граждан, что вообще характерно для этой страны. Но при этом жители Саудовской Аравии могут внести на рассмотрение сайты для фильтрации или оспорить решение блокировать определенный ресурс. Таким образом, участие граждан возможно и при авторитарных политических режимах.

Средства и методы фильтрации контента в Интернете

ПАРАМЕТРЫ ОЦЕНКИ СРЕДСТВ ФИЛЬТРАЦИИ



Открытость



Прозрачность



Точность



Подотчетность

МЕТОДЫ ФИЛЬТРАЦИИ



ТЕХНИЧЕСКИЕ МЕТОДЫ

1. Блокирование по IP-адресу
2. Искажение DNS-записей
3. Блокирование по URL-адресу
4. Пакетная фильтрация
5. Фильтрация через HTTP прокси-сервер
6. Нарушение работы сети
7. Фильтрация результатов поиска

IP

DNS



URL



НЕТЕХНИЧЕСКИЕ МЕТОДЫ

1. Законы, запрещающие публикацию того или иного контента
2. Давление на владельцев сайтов и пользователей с целью заставить их убрать нежелательные материалы или изменить их
3. Самоцензура



СБОР ИНФОРМАЦИИ В ИНТЕРНЕТЕ

1. Хранение логов и иной технической информации
2. Наблюдение за интернет-кафе
3. Системы интернет-слежки



ВАРИАНТЫ РАЗМЕЩЕНИЯ СИСТЕМ ТЕХНИЧЕСКОЙ ФИЛЬТРАЦИИ

1. Международный шлюз
2. Интернет-провайдеры
3. Интернет-сайты и сети организаций
4. Индивидуальные компьютеры



Методы цензуры контента в Интернете

➤ Сбор информации в Интернете

Хотя сам по себе сбор информации в Интернете не относится к фильтрации контента, полученные таким методом данные могут быть использованы для выявления пользователей, получающих доступ к запрещенному материалу, сайтов, содержащих такие материалы, и способов обхода интернет-фильтров.

- **Хранение логов и иной технической информации.** В большинстве стран введены законы, обязывающие интернет провайдеров хранить информацию о пользователях и посещенных ими ресурсах. Полиция и спецслужбы могут использовать эту информацию для установления личности нарушителей в Интернете.
- **Наблюдение за интернет-кафе.** С целью предотвращения использования интернет-кафе для нелегальной деятельности в ряде стран к их владельцам предъявляются жесткие требования по обеспечению безопасности. Так, в Китае и Италии пользоваться интернет-кафе можно только при предъявлении паспорта, а владельцы обязаны хранить записи о пользователях. Во Вьетнаме и Бирме в каждом интернет-кафе должна быть установлена видеокамера.
- **Системы интернет-слежки.** Возможности по отслеживанию интернет-трафика предусмотрены законодательством практически всех стран мира. В России действует СОПМ-2, обязывающий провайдеров устанавливать специальное устройство, позволяющее спецслужбам отслеживать трафик отдельных пользователей. Аналогичная система под названием CALEA действует и в США. Особый интерес представляют системы, способные изучать трафик целой страны, используя технологию глубокого анализа пакетов (Deep Packet Inspection). С помощью подобных систем возможно осуществлять наблюдение за активностью пользователей, например определяя какие приложения и сервисы они используют и какую информацию пересылают. Применение таких систем противоречит праву граждан на частную жизнь и запрещено в ЕС и России. Тем не менее, в настоящее время на межгосударственном уровне ведутся дебаты о допустимости их применения в целях борьбы с терроризмом и нарушением авторских прав. Поскольку изучение трафика целой страны требует значительных вычислительных мощностей, позволить себе системы массового наблюдения за Интернетом могут не все государства. В США Агентство национальной безопасности в рамках «Патриотического акта» отслеживает активность в Сети с помощью суперкомпьютеров NarusInsight. Китай использует глубокий анализ пакетов в целях интернет-цензуры; среди других стран, замеченных в таком применении технологии – Иран и Тунис.

➤ Нетехнические методы

Арсенал нетехнических методов фильтрации в Интернете, находящийся в распоряжении государства, во многом совпадает с используемыми методами для контроля традиционных СМИ. Их эффективность резко повышается при параллельном использовании современных средств сбора информации в Интернете и действующих законах о хранении провайдерами технической информации.

- **Законы, запрещающие публикацию того или иного контента.** Такая мера остается одним из основных средств контроля Интернета, как в демократических странах, так и в авторитарных. Ключевое значение здесь имеет физическое расположение сервера, на котором находится запрещенный материал. Ресурсы, находящиеся на территории страны обычно сами стараются убирать противозаконные материалы во избежание неприятностей с законом, или же делают это по первому обращению надзорных органов. В спорных ситуациях последнее слово остается за судом. Если же ресурс расположен вне юрисдикции страны, то решение принимает его владелец. Например, крупные международные сайты, такие как YouTube или Twitter, в своем решении ориентируются, прежде всего, на условия своего пользовательского соглашения и неформальные переговоры с представителями властей страны. При этом решение суда не является решающим аргументом, так как оно не распространяется на граждан и организации других стран. Подобная ситуация зачастую приводит к практике «двойных стандартов» со стороны крупных социальных сервисов, когда однотипный контент может удаляться, а может не удаляться, в зависимости от качества отношений с правительствами конкретных стран.
- **Давление на интернет-провайдеров, владельцев сайтов и пользователей с целью заставить их убрать нежелательные материалы или изменить их.** В условиях, когда категории запрещенного контента определены нечетко, у властей страны остается большой простор в их трактовке. Есть масса других способов давления на пользователей – угрозы, насилие, увольнение, штрафы и т.д. В отношении провайдеров и владельцев сайтов возможностей еще больше – отзыв лицензии, deregистрация доменного имени, физический арест серверов и оборудования. Зачастую доказать давление очень трудно, поэтому международные организации, занимающиеся изучением свободы в Интернете, вынуждены полагаться только на заявления пользователей и экспертов, которые зачастую ангажированы одной из сторон конфликта.
- **Самоцензура.** В условиях, когда провайдер может лишиться лицензии, сайт быть заблокирован, а пользователь арестован, производители интернет-контента предпочитают не рисковать и сознательно избегают острых тем. Во избежание трений с властями, провайдеры и сайты удаляют контент, содержащий даже намеки на запрещенный материал. В такой ситуации властям достаточно провести несколько показательных процессов, чтобы все остальные участники Сети поняли сигнал. Особенно показателен в этом плане Китай. Крупные западные компании, как Yahoo и Microsoft в погоне за динамичным китайским рынком добровольно принимают все ограничения, навязываемые цензорами. Так, специальный клиент Skype, разработанный специально для Китая, фильтрует сообщения пользователей и опционально сохраняет часть разговоров на сервере.

► Технические методы

- **Блокирование по IP-адресу.** При применении данного метода сервер, на котором находится нежелательный материал, становится полностью недоступным для пользователя. Главным преимуществом этого метода является его простота – он может быть реализован с помощью базового сетевого оборудования, используемого интернет-провайдерами. Однако с учетом современных технологий по одному IP-адресу могут находиться тысячи сайтов, а также других сервисов, таких как FTP или электронная почта, поэтому его блокирование приведет к тому, что все они станут недоступны. Из-за низкой точности данного метода страны применяют его с осторожностью. Блокирование по IP-адресу легко обходится при помощи различных технических решений, в частности, прокси-серверов и VPN.
- **Искажение DNS-записей.** При обращении пользователя к любому сайту, компьютер посылает запрос к DNS-серверу для того, чтобы преобразовать доменное имя в IP-адрес. В случае применения данного метода, DNS сервер возвращает неверный адрес, и сайт оказывается недоступным. Искажение DNS-записи также может быть реализована без применения дополнительного оборудования. Ее преимуществом перед блокированием по IP-адресу является более высокая точность – недоступным становится только один сайт на сервере. При этом все равно происходит чрезмерное блокирование. Например, Китай периодически лишает своих пользователей доступа к CNN International из-за появляющихся там нежелательных новостей. Хотя ставится цель фильтрации только одной страницы новости, остальные страницы сайта также становятся недоступны. Искажение DNS-записей легко обходится пользователями – в настройках браузера достаточно указать альтернативный DNS-сервер или вручную прописать IP-адрес заблокированного сайта.
- **Блокирование по URL-адресу.** В HTTP-протоколе URL-адрес содержит доменное имя сайта, а также параметры запроса. Они могут быть сверены со списком заблокированных ключевых слов, и в случае соответствия, связь пользователя с запрошенным ресурсом разрывается, или он перенаправляется на блок-страницу. Данный метод является более эффективным по сравнению с блокированием по IP-адресу и искажением DNS-записи, но требует дополнительного оборудования, так как использует поверхностный анализ пакетов. Его дополнительным преимуществом является то, что он способен динамически блокировать новые страницы, если в их адресе содержатся запрещенные слова. Например, в Китае блокируются все запросы, содержащие слова “falun” и “gong”. Однако при неправильной настройке ключевых слов точность метода резко ухудшается – он может пропускать нежелательный материал или, наоборот, допускать чрезмерное блокирование. Блокирование по URL-адресу нельзя обойти с помощью обычных прокси-серверов – необходимы инструменты, которые шифруют трафик, такие как VPN или TOR.
- **Пакетная фильтрация.** Наиболее сложный и дорогостоящий метод, так как он требует применения глубокого анализа пакетов. На данный момент полноценно реализован только в Китае. При использовании пакетной фильтрации, изучаются не только заголовки пакетов, содержащих URL адрес, но и все их содержимое. В случае наличия запрещенных слов, связь между пользователем и сервером разрывается. Метод позволяет фильтровать нежелательный контент не только в веб-страницах, но и во всех протоколах – электронной почте, сервисах мгновенных сообщений и др.

Существенным недостатком данного метода является то, что применение глубокого анализа пакетов может привести к снижению скорости интернет-соединения, что, к примеру, наблюдается при доступе из Китая к зарубежным интернет-серверам. В остальном, пакетная фильтрация обладает теми же достоинствами и недостатками, что и блокирование по URL-адресу.

- **Фильтрация через HTTP прокси-сервер.** Данный метод наиболее часто используется организациями для подключения корпоративных сетей к Интернету, но его можно использовать для фильтрации интернета в рамках всей страны. Гибридный вариант под названием Cleanfeed эффективно применяется в Великобритании и Канаде для борьбы с детской порнографией. Каждый запрос пользователя сверяется со списком IP-адресов, содержащих запрещенные материалы. Если совпадений нет, то запрос пользователя отсылается напрямую. В противном случае, он перенаправляется на прокси-сервер общественной организации Internet Watch Foundation. Прокси-сервер получает запрашиваемую страницу и анализирует ее на наличие детской порнографии. Если страница не содержит запрещенных материалов, то пользователь получает к ней доступ, иначе – создается видимость, что ресурс недоступен. Гибридные варианты фильтрации через HTTP прокси-сервер позволяют при низкой стоимости точно блокировать узкие категории контента. При этом, они столь же легко обходятся, как и фильтрация по IP-адресу.
- **Нарушение работы сети.** В экстренных случаях, таких как массовые беспорядки, власти страны могут пойти на полное или частичное отключение Интернета. Достигается это путем физического отключения роутеров из Сети или же изменения их настроек, из-за чего большая часть соединений сбрасывается. Данный метод применялся в Египте в ходе беспорядков 2011 года, Ливии, Сирии и Бирме. Тем не менее, опыт использования данного метода в ряде стран показывает, что полное блокирование доступа в Сеть зачастую провоцирует дополнительный рост массовых беспорядков. Более подробно об этом рассказывается в отдельной главе доклада.
- **Фильтрация результатов поиска.** В ряде стран, таких как Китай, Франция и Германия, работающие там поисковые системы обязаны исключать из результатов поиска ссылки на запрещенные материалы. Так, во французских и германских версиях Google из поисковых результатов исключаются ссылки на неонацистские группы и другие материалы, запрещенные законом. Таким образом, пользователи не могут найти нежелательный контент. Фильтрация результатов поиска – один из основных методов борьбы с нарушениями авторских прав в Интернете. Метод обходится использованием других поисковых систем – например, международная версия Google не исключает из результатов сайты неонацистских группировок и при этом доступна из Франции и Германии.

Ниже представлена таблица из книги Access Denied: The Practice and Policy of Global Internet Filtering⁷, в которой обозначено использование различными странами указанных методов фильтрации интернет-контента:

Blocking Techniques				
	IP blocking	DNS tampering	Blockpage	Keyword
Azerbaijan	X		X	
Bahrain		X	X	
China	X			X
Ethiopia	X			
India	X	X		
Iran			X	X
Jordan	X			
Libya	X			
Myanmar			X	
Oman			X	
Pakistan	X	X		
Saudi Arabia			X	
Singapore			X	
South Korea	X	X	X	
Sudan			X	
Syria			X	
Thailand			X	
Tunisia			X	
United Arab Emirates			X	
Uzbekistan*			X	
Vietnam			X	
Yemen			X	X

➤ Варианты размещения систем технической фильтрации

Обязательным условием установки интернет-фильтров, является их размещение на ключевых участках сети, через которые проходит весь трафик. Поэтому возможны следующие уровни их установки:

- **Международный шлюз.** Этот вариант предполагает централизованный подход к фильтрации контента. Программное и аппаратное обеспечение устанавливается на участке, соединяющем национальную сеть с международными магистралями. Преимуществом данного метода является более полный контроль и единообразие подхода к цензуре – политика фильтрации может оперативно корректироваться, а ее изменения будут затрагивать сразу всех пользователей. Однако, создание централизованной системы фильтрации Интернета, способной точно блокировать нежелательный контент, требует существенных затрат, пропорциональных объему внешнего трафика. Данный метод используется большинством мусульманских стран Ближнего востока. В Китае, Пакистане, Узбекистане и Иране он применяется совместно с фильтрацией на уровне интернет-провайдеров.
- **Интернет-провайдеры.** Другим подходом к цензуре в Интернете является установка систем фильтрации всеми провайдерами страны. В вопросе того, какие ресурсы подлежат блокировке, они ориентируются на решения су-

7. OpenNet Initiative Access Denied: The Practice and Policy of Global Internet Filtering — Cambridge: MIT Press, 2008.

дов, или на реестр, который ведут государственные или негосударственные органы. В случае если методы фильтрации не регламентируются, их реализация остается на усмотрение каждой компании. В результате, практика фильтрации может существенно варьироваться от провайдера к провайдеру, как в сторону избыточного, так и недостаточного блокирования. В частности, в России из-за некорректной реализации требований закона 139-ФЗ отдельными компаниями, для их пользователей оказались недоступны все блоги на платформе Wordpress. Фильтрация на уровне интернет-провайдеров применяется большинством европейских стран, а также Вьетнамом, Бирмой и Южной Кореей и рядом других государств.

- **Интернет-сайты и сети организаций.** Фильтрация на уровне сетей организаций чаще всего применяется частными компаниями для контроля использования Интернета своими сотрудниками, но также используется государствами для регулирования работы школ, библиотек, и правительственных учреждений. Так, в США в соответствии с Актом о защите детей в Интернете условием получения государственных субсидий для школьной библиотеки является установка фильтров, ограничивающий доступ несовершеннолетних к порнографии. Поскольку требование не является обязательным для всех учреждений, а закон предусматривает отключение фильтров по просьбе взрослых пользователей, Акт не ограничивает свободу слова, закрепленную в Конституции США.

В государствах, где по закону интернет-сайты и сервисы отвечают за контент, размещаемый на них пользователями, их владельцы нанимают сотрудников, отвечающих за цензуру, и устанавливают специальное программное обеспечение, отслеживающее запрещенный контент. Например, действовавшая в Китае блог-платформа компании Microsoft MSN Spaces не допускала названия блогов, содержащие слова «демократия» и «свобода», автоматически отклоняя такие варианты. Сервис микроблогов Sina Weibo блокирует записи по обширному набору ключевых слов, а в его штате числятся сотни сотрудников, осуществляющих цензуру вручную.

- **Индивидуальные компьютеры.** Данный подход предусматривает установку программного обеспечения для фильтрации непосредственно на компьютеры пользователей. Главной проблемой здесь является трудность отслеживания того, чтобы пользователь не удалил или отключил фильтр. С учетом этого, чаще всего индивидуальные фильтры используются на компьютерах частных компаний, которые могут технически ограничить права своих сотрудников вносить изменения в настройки, а также родителями для защиты детей от нежелательного контента в Сети. Попытки применять данный подход для государственной цензуры предпринимал Китай. В планах его властей была установка программного обеспечения «Зеленая дамба», блокирующего доступ к удаленно обновляемому списку сайтов и способного распознавать порнографические изображения, на все компьютеры страны. Но из-за многочисленных технических трудностей государственные органы отказались от этой инициативы.

Модели цензуры в Интернете

Законы, регулирующие Интернет, применяемые методы фильтрации и блокируемый контент специфичны для каждого государства. Тем не менее, существуют группы стран, которые преследуют схожие цели в вопросах интернет-цензуры. На основании общности задач и доводов, которые эти страны используют для обоснования вмешательства в Интернет, а также схожести инструментов, решающих данную задачу, можно выделить 5 моделей цензуры. При этом отдельные государства могут демонстрировать характеристики сразу двух моделей.

➤ Азиатская модель

Характерная черта: расплывчатое определение категорий блокируемого контента, предоставляющее правительству широкие возможности в области цензуры.

Примеры стран: Китай, Вьетнам, Южная Корея, Сингапур.

Цели и задачи фильтрации Интернета: Несмотря на существенные различия в политическом устройстве указанных государств, общей чертой этих стран является преобладающая точка зрения на патерналистскую роль государства, которое должно ограничивать доступ своих граждан к нежелательной информации. Законы, регулирующие Интернет, прямо указывают на главенствующую роль государства в охране общественных устоев и национальной безопасности. В Китае определены 9 категорий информации, которая рассматривается как вредная, в том числе для «национального единства». Вьетнам запрещает «злоупотребление демократическими свободами во вред интересам государства». Южная Корея – информацию, которая нарушает «общественное спокойствие и порядок, мораль и хорошие традиции». В Сингапуре задачей агентства, которое регулирует прессу, является предотвращение появления материалов «против общественных интересов, порядка и национальной гармонии».

Категории блокируемого контента: Расплывчатое определение материала, считающегося запрещенным, дает правительствам стран широкие полномочия в трактовке законов. Приоритет отдается политическому контенту и информации, блокируемой по соображениям безопасности. Китай фильтрует самый широкий спектр чувствительных тем – начиная от независимости Тайваня и заканчивая духовным движением Фалуньгун. Особо тщательно блокируются международные сайты, содержащие критику Коммунистической партии Китая, и популярные социальные сервисы. Схожая картина наблюдается и во Вьетнаме, где главным объектом цензуры выступают сайты, подвергающие сомнению руководящую роль его властей. Южная Корея блокирует узкую категорию контента, но делает это с высокой эффективностью – под запретом все, что связано с северным соседом, а также отдельные антигосударственные материалы. Помимо борьбы с сайтами в Интернете, уголовному преследованию подвергаются пользователи, остав-

ляющие сообщения с похвалой Северной Корее в социальных сетях. В Южной Корее также активно борются с нарушениями авторских прав - с 2009 года там действует закон «о трех предупреждениях». Он предусматривает отключение от Интернета пользователей, систематически скачивающих нелегальную продукцию. Власти Сингапура видят одну из основных угроз в расизме – население острова многонационально и там проживает значительное число иностранцев. В 2005 три пользователя были арестованы в соответствии с «Актом о подстрекательстве» за расистские сообщения в Интернете. Несмотря на то, что формально порнография относится к фильтруемому контенту во всех странах этой группы, исследование OpenNet показало, что там недоступна незначительная часть таких сайтов. Лишь Китай провел в 2010 году широкую кампанию по блокированию порнографических материалов и онлайн-казино. В Сингапуре символично заблокированы лишь несколько сайтов с порнографией.

Используемые методы фильтрации: Основные методы, на которые полагаются власти данной группы стран – самоцензура и сбор информации в Интернете. Все пользователи Южной Кореи, использующие крупные сайты, до недавнего времени должны были регистрироваться под своим настоящим именем. Сингапур обязывает проходить процедуру регистрации не только интернет-провайдеров, но и пользователей, «распространяющих или обсуждающих политическую или религиозную информацию, связанную с Сингапуром». И в Китае, и во Вьетнаме правительственные агентства осуществляют активную слежку в Интернете и регулируют работу интернет-провайдеров. Учитывая, что в этих государствах пользователи неоднократно подвергались уголовному преследованию за высказывания в Интернете, такие меры позволяют жестко контролировать ход онлайн-дискуссий. Помимо этого, страны применяют системы технической фильтрации различной сложности. Если Китай обладает самой продвинутой на сегодняшний день системой «Золотой щит», использующей все методы фильтрации, то Вьетнам и Южная Корея полагаются на более простые способы. Так, Вьетнам применяет искажение DNS-записей, а власти Южной Кореи делегируют удаление нежелательного контента провайдерам.

Страна с характеристиками сразу двух моделей: Южная Корея (азиатская и континентальная модели).

➤ Ближневосточная модель

Характерная черта: доминирующий религиозный фактор при принятии решений о блокировании интернет-ресурсов.

Страны: Саудовская Аравия, Катар, Оман, Бахрейн, Йемен, Объединенные Арабские Эмираты, также к этой категории можно отнести Индонезию.

Цели и задачи фильтрации Интернета: Саудовская Аравия, Оман и Катар – монархии, Индонезия – формально демократическая республика. На практике регулирование Интернета в этих странах значительное влияние оказывает религия. Ислам исповедует большинство населения, и власти стремятся заблокировать контент, который противоречит его нормам. Так, список заблокированных сайтов Саудовской Аравии регулярно пополняется с помощью предложений граждан. Согласно постановлению Совета Министров страны, запрещены материалы «нарушающие святость ислама» и «противоречащие государству или его системе». Закон Омана о прессе дает властям полномочия применять цензуру в отношении «оскорбительных» материалов. Парламентом Индонезии были приняты «Закон об

электронной информации и транзакциях», запрещающий диффамацию, а также закон против порнографии, предусматривающий наказание до 12 лет тюрьмы. Эти законы легли в основу регулирования Интернета в Индонезии.

Категории блокируемого контента: Приоритетом для фильтрации в этой группе стран является порнография и другой контент, противоречащий нормам ислама. В Саудовской Аравии помимо этого блокируются сайты политической оппозиции, религиозных движений, отличных от официальной салафии. Также недоступны сайты о планировании семьи, организаций по защите прав человека, ресурсы, содержащие критику ислама, информацию об алкоголе, наркотиках и секс-меньшинствах. Катар и Оман придерживаются схожей политики в фильтрации контента, в Омане запрещены VoIP сервисы. Индонезия блокирует порнографию и материалы, разжигающие межнациональную и религиозную рознь, хотя отдельные провайдеры ограничили доступ и к некоторым сайтам политической направленности.

Используемые методы фильтрации: Характерная особенность систем фильтрации данной группы стран – применение коммерческого программного обеспечения западных IT-компаний. Саудовская Аравия и Оман используют Smart-Filter от McAfee, Катар – Netsweeper одноименной компании. Интернет-провайдеры Индонезии блокируют порнографию с помощью HTTP прокси-серверов различных производителей. Преимуществом такого подхода является то, что составление и обновление блок-листов берет на себя поставщик программного обеспечения. Как результат, Саудовской Аравии удастся заблокировать значительную долю порнографических сайтов – впечатляющее достижение, если учесть их количество в Интернете. Его обратной стороной является то, что блокируется преимущественно англоязычный контент, в то время как ресурсы на арабском языке подвергаются ограничениям в последнюю очередь. Помимо технических методов, страны активно преследуют нарушителей законов в Сети. Комитет по защите журналистов признал Саудовскую Аравию одной из самых худших стран для блогеров – за выступления с критикой государства пользователи регулярно подвергаются уголовному преследованию. Катар и Оман прибегают к арестам пользователей в меньших масштабах. В Индонезии случаев уголовного преследования блогеров мало – в частности, один пользователь был арестован за размещение карикатуры на пророка Мухаммеда на своей странице в Facebook.

➤ Рестрикционная модель

Характерная черта: акцент на блокировании интернет-ресурсов радикальной политической оппозиции и правозащитных групп.

Страны: Иран, Сирия, Эфиопия, Узбекистан

Цели и задачи фильтрации Интернета: Сирия, Эфиопия и Узбекистан – по своей конституции демократические республики, Иран – исламская республика, фактически – теократия. Главной задачей фильтрации Интернета в этих странах является борьба с политической оппозицией, зачастую радикального и исламистского толка. Конституции Сирии и Эфиопии прямо гарантируют свободу прессы и информации, Конституция Узбекистана – свободу выражения. Несмотря на это, действие этих статей ограничено различными дополнительными законами, дающими властям широкие полномочия на применение цензуры. Дополнительным стимулом для жесткого контроля над Интернетом в этих странах является политическая нестабильность. Эфиопия вовлечена в конфликт сразу с двумя

соседями, а ее власти борются с исламским радикализмом внутри страны. В Сирии с 2011 года фактически идет гражданская война, участие в которой на стороне оппозиции принимают исламистские группировки, близкие к «Аль-Каиде». Власти Узбекистана противостоят росту влияния радикальных исламских групп; в Иране также действует радикальная политическая оппозиция.

Категории блокируемого контента: Основной целью фильтрации Интернета в этих странах являются сайты оппозиции, правозащитных организаций, а также ресурсы, содержащие критику действующего режима. Помимо этого, Иран блокирует материалы, противоречащие нормам ислама, и сайты, посвященные правам женщин. Власти Эфиопии целенаправленно блокируют политические блоги и сервисы VoIP. Сирийские власти фильтруют сайты «Братьев-мусульман» и курдских меньшинств.

Используемые методы фильтрации: Методы, применяемые данными странами, схожи с азиатской моделью. Это сочетание систем технической фильтрации и слежки в Интернете. Для облегчения работы спецслужб, работа интернет-кафе строго регулируется. Власти Ирана, Сирии и Эфиопии также практикуют уголовное преследование пользователей и журналистов за сообщения в Интернете. Такие действия обеспечивают подавление политической активности пользователей в Сети. Иран обладает одной из самых продвинутых систем технической фильтрации в мире. Изначально в ее основе лежал Smart-Filter (как утверждает компания-создатель программного обеспечения, незаконно используемый). Но, опасаясь «закладок» в системе, способных дать доступ спецслужбам западных стран, власти Ирана перешли на программные решения местных компаний. В 2008 Иран приобрел у Nokia и Siemens оборудование, способное осуществлять глубокий анализ пакетов. Сирия и Узбекистан используют HTTP-прокси фильтрацию, способную блокировать контент по ключевым словам. Во время крупных демонстраций в 2011 году власти Сирии прибегли к отключению Интернета

Страна с характеристиками сразу двух моделей: Иран (рестрикционная и ближневосточная модели).

➤ Континентальная модель

Характерная черта: фильтрация социально-опасных ресурсов по четко обозначенным категориям, а также борьба с нарушениями авторских прав.

Страны: Франция, Германия, Великобритания, Бельгия

Цели и задачи фильтрации Интернета: Все страны этой группы являются развитыми демократиями. Европейская конвенция по правам человека гарантирует свободы выражения мнения и информации, но уточняет, что они могут быть ограничены «в интересах национальной и общественной безопасности», а также защиты «здоровья и морали». В соответствии с этими принципами, государства допускают фильтрацию информации, которая противоречит их законодательству. Таким образом, большинство европейских стран пытаются найти баланс между базовым правом на свободный доступ к информации и защитой общества. При этом контент, подлежащий блокированию, строго определен в рамках права, а законы перед принятием проходят положенные демократические процедуры.

Категории блокируемого контента: Общими для всех стран данной груп-

пы являются усилия по борьбе с детской порнографией и нарушениями авторских прав. Принятый во Франции закон HADOPI предусматривает отключение от Интернета пользователей, замеченных в нелегальном скачивании защищенного правами контента. Во Франции и Германии блокируются материалы, прославляющие нацизм, отрицающие холокост и разжигающие межнациональную и религиозную рознь. В большинстве стран действуют законы против нарушения неприкосновенности частной жизни. Например, в Бельгии по этому закону были заблокированы сайты, распространяющие информацию о педофилах. Строгие законы против диффамации в Великобритании привели к тому, что хостеры предпочитают убирать сомнительный контент по первому требованию, опасаясь возможных исков.

Используемые методы фильтрации: Европейские страны выбрали два различных подхода в вопросе фильтрации контента. В Великобритании используется система Cleanfeed - интернет провайдеры добровольно сотрудничают с общественной организацией, блокирующей сайты с детской порнографией. Эта добровольность весьма условна – в 2008 представитель правительства Великобритании заявил, что если провайдеры не пойдут на такой шаг, Парламент обяжет их делать это по закону. В Германии действует схожая система. Правительственная организация поддерживает список материалов, которые считает вредными для детей, а самые крупные поисковые системы страны добровольно исключают их из результатов поиска. Стандартной практикой же является блокирование сайтов по решению суда. Другой подход решили использовать власти Франции. После широких общественных дебатов, Конституционный суд признал законным часть положений закона LOPPSI 2, предусматривающих ведение Министерством внутренних дел списка сайтов, которые обязаны блокировать интернет-провайдеры. Закон дал повод обвинить Францию во введении цензуры в Интернете – опасения у пользователей вызвала возможность блокировать без решения суда материалы, отличные от детской порнографии.

Россию можно отнести именно к континентальной модели фильтрации контента с поправкой на то, что борьба с систематическим нарушением авторских прав в Рунете ведется значительно менее активно по сравнению со странами Западной Европы.

➤ Либеральная модель

Характерная черта: стремление избежать централизованного и систематического блокирования определенных категорий интернет-ресурсов. Одновременно с этим принятие властями мер к закрытию нарушающих закон ресурсов и преследование их владельцев.

Страны: США, Япония, Бразилия

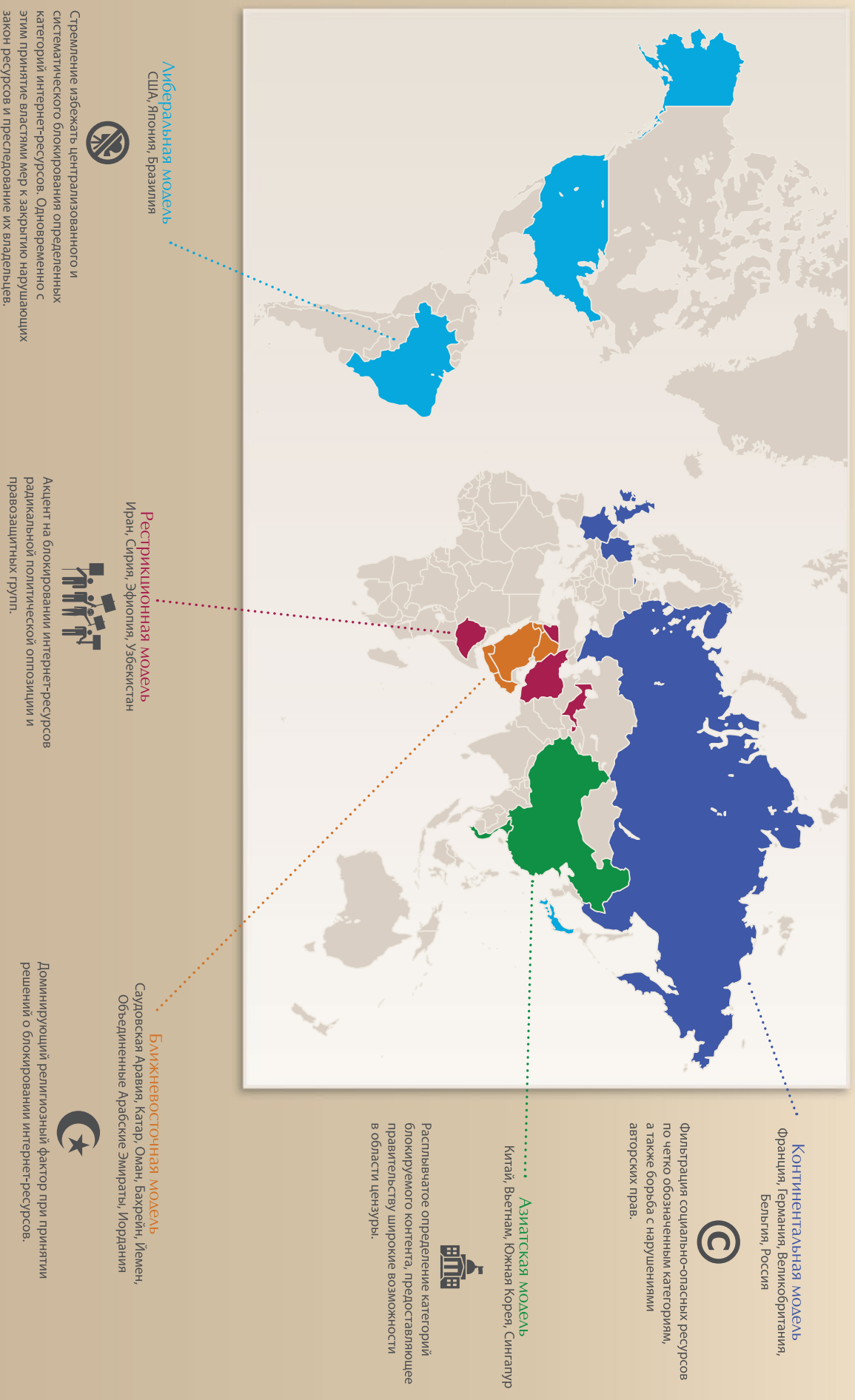
Цели и задачи фильтрации Интернета: США, Япония и Бразилия – развитые демократии. В отличие от большинства других стран, Первая поправка Конституции США прямо запрещает принимать законы, ограничивающие свободу слова. Как результат, техническая фильтрация в США практически не применяется. Ряд предложенных законов о регулировании Интернета были признаны неконституционными. Законы Японии и Бразилии гарантируют свободы слова и прессы, и власти никак не ограничивают их на практике.

Категории блокируемого контента: В США, как и в Европе, особое внимание уделяется борьбе с детской порнографией и защите интеллектуальной собственности. В Японии, напротив, одни из самых мягких законов по отношению к детской порнографии – в частности, легальным является ее хранение. Запрещено распространение нецензурированной порнографии; для нарушителей предусмотрено уголовное преследование. Впрочем, на практике закон применяется крайне редко. В то же время власти Японии в апреле 2013 года предложили заблокировать на территории страны использование сервиса анонимизации Tor. Бразилия не распространяет свободу слова на расистские материалы.

Используемые методы фильтрации: В отсутствие возможностей для технического блокирования нежелательных материалов, власти США активно используют другие стратегии. С помощью давления со стороны частных и общественных организаций и угроз исков, правительство пытается добиться удаления нежелательного контента. Показателен пример с российским сайтом alfofmp3. Его закрытие называли одним из условий вступления России в ВТО. Под давлением международной федерации звукозаписывающих компаний сайт был заблокирован в Дании, а другая организация RIAA подала иск на сумму в 1.65 триллиона долларов. Вскоре после того как ряд платежных систем отказались работать с сайтом, alfofmp3 закрылся. Другая практика – добровольные соглашения интернет провайдеров и хостеров удалять незаконный контент. Так, в 2008 году основные провайдеры страны подписали соглашение с прокурором Нью-Йорка по борьбе с детской порнографией. Бразилия в вопросе регулирования Интернета полагается на судебные иски, обязывающие хостеров удалить запрещенный контент. В Японии распространена самоцензура. Например, новостные агентства Японии обвиняли в том, что они воздерживались от резкой критики действия властей в ситуации с аварией на ядерной станции в Фукусиме.

Страна с характеристиками сразу двух моделей: Япония (либеральная и азиатская модели).

Модели цензуры в Интернете



Способы обхода интернет-фильтрации

➤ Методы обхода фильтрации в интернете

При всем многообразии применяемых странами методов цензуры, интернет-активисты неустанно пытаются разработать методы ее обхода. Многие инструменты также подвергаются блокированию – особенно эффективно в этом направлении действует Китай. Но последнее слово все равно остается за пользователями. Как признал руководитель программы по контролю над Интернетом в Саудовской Аравии, остановить технически грамотных пользователей интернет-фильтры не в состоянии.

Но государства, фильтрующие контент в Интернете, и не преследуют такой цели. Как показало исследование Хэла Робертса, Этана Цукермана и Джона Полфри, проведенное в Гарвардском университете⁸, большинство средства обхода цензуры обладают рядом существенных недостатков и сложны в применении - их использует менее двух процентов пользователей стран, где действуют интернет-фильтры. Помимо этого, если какое-то средство обхода цензуры становится известно большому числу граждан, власти тоже узнают о нем и предпринимают меры к тому, чтобы заблокировать. То есть, несмотря на то, что наиболее продвинутые пользователи имеют возможность обойти фильтры, государствам успешно удается контролировать доступ к информации подавляющего большинства своих жителей.

HTTP Proxy-серверы. Представляют собой серверы-посредники, через которые может быть направлен запрос на заблокированный ресурс. HTTP прокси получает от него информацию и отправляет ее обратно пользователю. Их применение позволяет обойти блокирование по IP-адресу и искажение DNS-записей. Необходимым условием использования прокси-сервера для обхода цензуры является его нахождение вне фильтруемой части Интернета. Существуют прокси-серверы, поддерживающие работу через протокол HTTPS, обеспечивающий шифрование данных. Их использование позволяет обойти более совершенные методы фильтрации, такие как блокирование по ключевым словам. Существенными недостатками HTTP прокси-серверов является увеличение времени доступа к сайтам при работе через них, ограниченная функциональность и соображения безопасности. Так как через прокси-сервер проходит все запросы пользователя, в распоряжении его владельца могут оказаться важные частные данные - пароли и банковская информация. Часть прокси-серверов фильтруют более сложные компоненты сайтов, такие как JavaScript, Java апплеты, Flash-элементы и ActiveX, что делает невозможным их применение для работы на некоторых сайтах. Использовать прокси-сервер довольно легко – достаточно указать его в настройках браузера. Основную проблему представляет поиск прокси – государства, применяющие цензуру, обычно активно блокируют их, а также сайты, распространяющие свежие

8. The Berkman Center for Internet and Society, "Circumvention Landscape Report Methods, Uses, and Tools," 2007.

списки прокси-серверов.

CGI Proxy-серверы. Прокси серверы с веб-интерфейсом, позволяющим работать с ними напрямую через браузер. Это делает их использование более простым для пользователей.

SOCKS Proxy-серверы. Позволяют обходить цензуру не только при работе через браузер, но и в программах мгновенных сообщений и электронной почте.

Онлайн-переводчики и сервисы по сжатию трафика. Ряд сервисов в интернете фактически действуют как прокси-серверы. Так, с помощью Google Translate возможно получить доступ к заблокированным по IP-адресу ресурсам, так как запросы пользователя сначала идут к серверу Google. Поэтому зачастую данные сервисы блокируются государствами, практикующими цензуру в интернете.

Виртуальные частные сети (VPN). Технология, при которой между компьютерами создается виртуальная сеть поверх другой сети, в том числе и через Интернет. Используя подключение через VPN, пользователь направляет запрос к заблокированному ресурсу через другой компьютер виртуальной сети. Поскольку при использовании VPN трафик между компьютерами шифруется, виртуальные частные сети могут быть использованы для обхода большинства технических методов фильтрации. Их дополнительным преимуществом является относительно высокая скорость работы и возможность применения всех видов интернет-сервисов, включая VoIP-программы и мессенджеры. Так как информация, передаваемая по VPN, доступна компьютерам внутри сети в открытом виде, возникает та же проблема с безопасностью, что и при использовании прокси-серверов. Интернет-провайдеры могут легко выявлять действующие VPN сети, анализируя трафик. Например, Иран активно блокирует все незарегистрированные виртуальные частные сети. В Китае ситуация иная – поскольку большое число китайских и западных компаний применяют VPN в повседневной работе, власти, в основном, закрывают на них глаза. Существует большое количество платных и бесплатных сервисов, предоставляющих доступ к Интернету по VPN, кроме того пользователи могут самостоятельно настроить подобную сеть. Однако для использования VPN необходима установка специального программного обеспечения, что требует от пользователей высокого уровня технических знаний.

Tor, JonDonym, Psiphon, Relakks и другие инструменты. Эти системы используют разное сочетание шифрования, технологии VPN и маршрутизации между несколькими узлами сети для обеспечения высокого уровня анонимности и обхода фильтрации. При использовании Tor трафик от пользователя направляется к запрошенному сайту через три случайно выбранных анонимных прокси-сервера. При этом, на каждом этапе трафик подвергается шифрованию, что обеспечивает то, что ни один из узлов не имеет доступа ко всей информации о пользователе. JonDonym работает по схожему принципу, но вместо анонимных узлов использует серверы доверенных организаций. Использование таких систем требует установки дополнительного программного обеспечения, но позволяет обойти большинство методов фильтрации в Интернете. Недостатком Tor является медленная скорость работы – по результатам тестирования Гарвардского исследования, он показал один из самых худших результатов. Китаю удастся успешно заблокировать большинство узлов сети Tor, и для его использования требуется поиск альтернативных точек доступа – так называемых «мостов». Это делает его использование затруднительным для большинства пользователей.

Использование кэша поисковых систем, зеркал, RSS-агрегаторов и сервисов Web to E-mail. Эти сервисы объединяет то, что с их помощью можно

читать заблокированные сайты новостей и блоги. Так как поисковые системы сохраняют на своих серверах все найденные страницы, то их можно посмотреть, даже если сайт, с которого они получены, для пользователя заблокирован. Кэш Google был доступен некоторое время в Китае, но был частично заблокирован по требованию официальных властей. RSS-агрегаторы позволяют собирать информацию с других сайтов в одном месте, а сервисы Web to E-mail посылают веб-страницы на электронную почту пользователей. Эти методы легки в использовании, но полноценно пользоваться, например, Facebook или Twitter с их помощью нельзя.

Регулирование Интернета в США

На практику регулирования Интернета в США большое влияние оказали сразу несколько факторов, сделавших ее уникальной среди других стран. Во-первых, США – историческая родина Интернета, а многие американские IT-компании, такие как Google, Facebook и Twitter, занимают лидирующие позиции в Сети. Во-вторых, первая поправка Конституции США прямо запрещает принимать законы, ограничивающие свободу слова, а, следовательно, многие методы регулирования Интернета американским законодателям недоступны. В третьих, ведущая роль США в мировой политике и экономике позволяет добиваться от иностранных стран и компаний выполнения требований американских властей.

Попытки обязать интернет-провайдеров и регистраторов доменов блокировать доступ к сайтам по решению суда неоднократно предпринимались правообладателями и сторонниками борьбы с детской порнографией. Но каждый раз такие законы не принимались Конгрессом, а решения судов отменялись. Так, в 2004 году штат Пенсильвания принял закон, предписывающий интернет-провайдерам фильтровать сайты с детской порнографией. Механизм блокирования не был хорошо отработан, и в результате помимо нелегального контента недоступными оказались более миллиона других сайтов. Вскоре федеральный судья вынес решение о несоответствии данного закона первой поправке.

В 2012 году Конгресс рассматривал проекты законов SOPA и PIPA, которые обязывали провайдеров и хостеров блокировать доступ к сайтам с нарушающими авторские права материалами по требованию правообладателей. В знак протеста тысячи сайтов, включая Википедию и Craigslist, на день престали работать. Петиция против законов, размещенная на сайте Google, собрала более 4,5 миллионов подписей. В результате, Конгресс отложил их рассмотрение.

В 2000х годах Минюст США применял тактику по конфискации доменов сайтов, нарушающих закон, трактуя их как имущество, используемое для криминальной деятельности. Эта мера также подверглась критике активистов по защите свободы слова в Интернете. Помимо этого, ее эффективность была сомнительной – зачастую сайты становились доступны по новому адресу. Другой случай блокирования DNS-записей государством – применение Акта о торговле с врагом, который запрещает ведение бизнеса с рядом государств. В соответствии с его положениями компания-регистратор доменов была вынуждена блокировать DNS-записи туристического агентства, рекламирующего туры в Кубу.

В целом, на сегодняшний день Интернет в США остается свободным от технических методов цензуры со стороны государства. Вместо этого фильтрация контента добровольно осуществляется частными компаниями при поддержке государственных структур. Например, в случае с детской порнографией, ряд крупных интернет-провайдеров подписали соглашение с окружным прокурором Нью-Йорка, согласившись добровольно блокировать доступ к таким ресурсам.

Другим важным инструментом государства по регулированию Интернета остается давление на иностранные компании. Поскольку в США нелегальны большинство видов онлайн азартных игр, а государство не имеет возможности

блокировать доступ к иностранным сайтам, власти пошли на ряд жестких мер в отношении нарушителей. Конгресс принял закон, предусматривающий запрет онлайн-казино и букмекерским конторам принимать платежи от американских граждан. Google и Yahoo отказались от размещения рекламных баннеров таких сайтов, после того как Минюст США заявил, что реклама может быть расценена как содействие преступлению. Ряд владельцев букмекерских контор, работающих онлайн, были подвергнуты уголовному преследованию. Такое давление позволяет добиваться от компаний, находящихся вне юрисдикции США, выполнения требований американских законов.

США одними из первых приняли законы, регулирующие интеллектуальную собственность в Интернете. Ключевой концепцией Акта об авторском праве в цифровом тысячелетии является понятие «безопасной гавани». Согласно акту, интернет-провайдеры и хостинговые компании освобождаются от судебной ответственности за передачу и хранение информации, нарушающей авторские права, если они удаляют ее после обращения правообладателя. Закон привел к тому, что, опасаясь исков, сайты зачастую удаляют контент по первому требованию, не вникая действительно ли он нарушает авторские права. Например, Google получает несколько миллионов запросов в месяц на удаление ссылок из результатов поиска.

Настоящим тестом для действия первой поправки Конституции США в Интернете стал скандал вокруг сайта Викиликс. Неприятности с американским правосудием у него начались еще в 2008 году - по иску швейцарского банка суд предписал заблокировать доменное имя сайта. Решение вызвало протесты со стороны активистских групп и вскоре было отменено. Настоящие проблемы же вызвала публикация в 2010 году засекреченных документов и материалов, в частности видеозаписи расстрела американскими военными гражданских лиц в Ираке и дипломатической переписки посольств. Их обнародование нанесло существенный ущерб национальным интересам США. Несмотря на то, что формально, публикация третьей стороной незаконно полученной информации не противоречит законодательству страны, Министерство юстиции рассматривало возможность уголовного преследования создателя сайта Джулиана Ассанджа по обвинению в «краже государственной собственности» и нарушении Акта о шпионаже от 1917 года. Власти США заблокировали доступ к сайту с компьютеров федерального правительства и оказали беспрецедентное давление на компании, работающие с Викиликс. В частности, Amazon отказался от предоставления услуг хостинга сайту, а платежные системы Visa, Mastercard и PayPal перестали принимать платежи в его адрес. Тем не менее, подавляющее большинство интернет-пользователей США по-прежнему могут беспрепятственно посещать сайт Викиликс.

Великобритания: источник российской модели

Подход к фильтрации контента в Великобритании представляет собой особый интерес в связи с тем, что именно британская система регулирования Сети была взята за образец при создании Лиги безопасного Интернета и инициировании закона №139-ФЗ, в рамках которого появился «реестр запрещенных сайтов». Российская система в ее окончательном виде, по ряду критериев отличается от британского аналога, однако подход остается схожим.

Правительство Великобритании в середине 2000-х годов обозначило две ключевых задачи, которые должна преследовать фильтрация интернет-контента: борьба с терроризмом и предотвращение распространения детской порнографии. Позже к этому перечню добавилась борьба с систематическим нарушением авторских прав.

Ключевую роль в вопросах регулирования контента в Сети играют не государственные органы, а благотворительный Фонд наблюдения за Интернетом (Internet Watch Foundation), основанный в 1996 году. Финансирование фонда частично обеспечивают британские операторы связи, интернет-компании и производители программного обеспечения, а частично – правительство Великобритании и структуры Евросоюза.

Официально декларируемой задачей IWF является «минимизация доступности потенциально незаконного интернет-контента, особенно детской порнографии, вне зависимости от того, где он размещен, а также удаление незаконного порнографического контента, размещенного на территории Великобритании». Ранее организация ставила своей целью также борьбу с разжиганием расовой ненависти, однако в 2011 году эта функция была передана полицейскому проекту TrueVision, который призван аккумулировать жалобы на преступления, связанные с разжиганием ненависти в отношении различных групп населения, и закрывать данные ресурсы, если они расположены на британских серверах.

Функция IWF сводится к ведению реестра запрещенных сайтов, который представляет собой набор ссылок, преимущественно связанных с детской порнографией. Непосредственным ведением данного реестра занимаются несколько специалистов, обученных полицией. По разным оценкам, всего в списке IWF одномоментно содержится порядка 1000 функционирующих сайтов.

В свою очередь, у интернет-провайдеров установлено специальное программное обеспечение Cleanfeed, призванное блокировать доступ к запрещенным сайтам. Данная система была разработана государственной корпорацией British Telecom в 2004 году и в настоящее время ее использование является обязательным для всех провайдеров Великобритании, вне зависимости от того, частные они или государственные. В результате, действие системы Cleanfeed распространяется практически на всех британских интернет-пользователей.

Провайдеры сами определяют, сообщать или нет своим пользователям о том, что сайт, на который они хотели перейти, заблокирован Cleanfeed. Некоторые выводят соответствующее сообщение, однако большая часть сообщает о том, что данная страница отсутствует на сервере (page not found). Таким образом, пользователи не знают о том, что тот или иной контент был заблокирован. Так как блокировка осуществляется не по решению суда, а сам оператор реестра не является государственным, процедура апелляции блокировки осуществляется по внутренним правилам IWF.

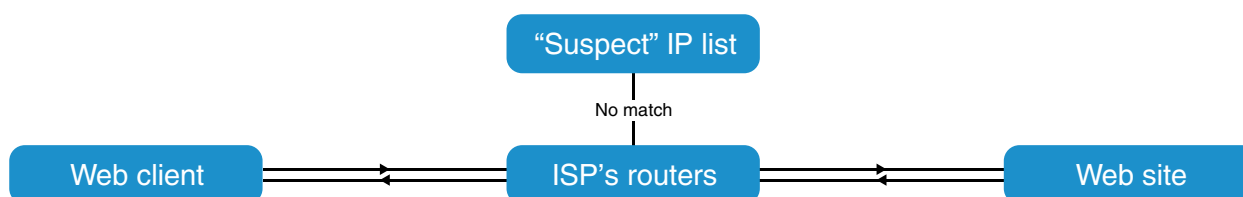
С 2011 года система Cleanfeed используется операторами связи не только для борьбы с детской порнографией. Британская ассоциация кинематографистов через суд вынудила провайдеров использовать систему фильтрации контента для блокировки сервисов обмена нелицензионным контентом, нарушающим авторские права. В частности, в мае 2012 года среди прочих блокировке подвергся крупнейший торрент-трекер The Pirate Bay.

Техническая реализация системы выглядит следующим образом. Существует конфиденциальный список запрещенных интернет-страниц (не сайтов), доступ к которому есть только у специалистов IWF. Он не доступен ни провайдерам, ни рядовым пользователям. Провайдерам предоставляется список IP-адресов сайтов, на которых размещены данные страницы, для того, чтобы именно к этим адресам применялись правила фильтрации.

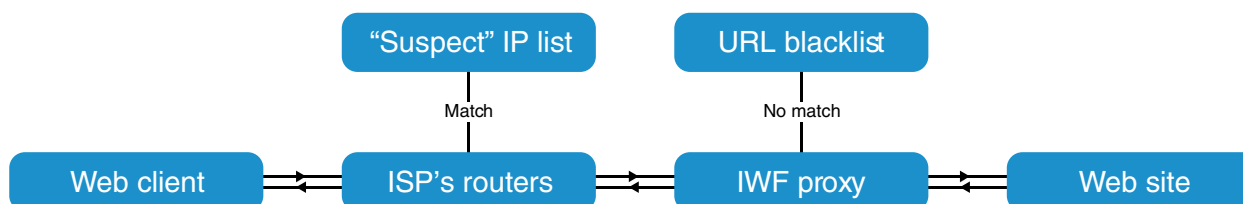
Провайдеры перенаправляют трафик, идущий на эти адреса, на специальные прокси-серверы, которые сравнивают HTTP-запросы с адресами страниц, содержащихся в реестре запрещенных адресов. Если они не совпадают – трафик проходит фильтр и пользователь попадает на запрашиваемую страницу.

В работе «Anonymity and traceability in cyberspace» Ричарда Клейтона из Университета Кембриджа проанализировано, каким образом осуществляется работа Cleanfeed. Она происходит в два этапа:

1. Проверка IP-адреса, к которому обращен запрос.



2. Сравнение страницы, к которой обращается пользователь, со списком адресов в реестре запрещенных ресурсов.



Позднее система Cleanfeed была экспортирована в некоторые страны британского содружества. В Канаде в настоящее время она используется на добровольной основе крупнейшими провайдерами страны, обслуживающими порядка 80% интернет-пользователей. В Австралии внедрение данной системы столкнулось с политическим противодействием, и ее реализация в масштабах страны была отложена на неопределенный срок.

В августе 2011 года после массовых беспорядков в крупнейших британских городах, премьер-министр Великобритании Дэвид Кэмерон встретился с руководством крупнейших интернет-компаний с целью обсуждения возможных мер, которые позволили бы предотвратить использование социальных сетей погромщиками. По этому поводу Кэмерон сделал следующее заявление в парламенте:

«Все мы поражены тем, что ужасные события, произошедшие в нашей стране, организованы при помощи социальные медиа. Свободный поток информации может использоваться во благо. Но также он может использоваться и со злым умыслом. Когда люди используют социальные медиа для провоцирования насилия, наша задача – остановить их. Поэтому мы работаем вместе с полицией, разведывательными службами и интернет-индустрией над вопросом о том правильно ли будет приостановить интернет-коммуникацию через определенные сайты и сервисы, если нам известно, что при помощи них планируются действия, связанные с преступностью и насилием»⁹.

Впрочем, после того как погромы прекратились, британское правительство не стало предлагать новые законодательные инициативы, связанные с регулированием Интернета, хотя дискуссии по этому поводу до сих пор периодически возникают в британской политической и общественной повестке.

9. Cameron Exploring Crackdown on Social Media After Riots”, Eric Pfanner, New York Times, 11 August 2011

Великобритания: источник русской модели

КОНТРОЛИРУЮЩИЙ ОРГАН

Internet Watch Foundation
(негосударственный фонд)

Роскомнадзор
(государственный орган)

Роспотребнадзор
(экспертиза)

ФСКН
(экспертиза)

БЛОКИРУЕМЫЕ САЙТЫ

С детской порнографией
Сервисы, нарушающие
авторские права

С детской порнографией
Ресурсы пропагандирующие
употребление наркотиков
Сайты с пропагандой
суицида

СПОСОБ БЛОКИРОВКИ

Двухэтапная проверка

Проверка по IP

Проверка по URL

Блокировка

Одноэтапная проверка

Проверка по URL/IP

Блокировка

АПЕЛЛЯЦИЯ



Через механизмы
фонда, заведующего
списком



Через суд

Китай: мифы и реальность интернет-цензуры

Когда речь заходит о систематическом цензуровании интернет-контента на государственном уровне, почти всегда приводится пример Китая – страны, где якобы запрещено практически все. Однако, как это часто бывает, реальность оказывается гораздо сложнее, нежели созданный миф.

Прежде всего, для анализа китайской модели блокирования контента в Сети необходимо остановиться на том, что вообще представляет собой китайский сегмент Интернета. На сегодняшний день Китай с 564 миллионами интернет-пользователей занимает первое место в мире по данному показателю, а уровень их активности в Сети не только не уступает, но и в некоторых сегментах значительно превосходит активность граждан других государств, несмотря на отсутствие доступа к популярным международным коммуникационным сервисам. Аналогичная ситуация и в коммерческой составляющей Сети – Китай не уступает странам Европы в части развития развлекательного и коммерческого сегментов: существуют крупные торговые площадки, развита система микроплатежей, а рынок онлайн-игр занимает первое место по своему объему в мире с огромным количеством локальных продуктов.

В то же время, гигантский с точки зрения аудиторных и финансовых параметров интернет-сектор Китая уживается со сложной системой цензуры, которая состоит из трех базовых элементов:

3. Система фильтрации трафика «Золотой щит» (она же «Великий китайский фаервол»);
4. Система блокировки поиска нежелательной информации;
5. Ручная система фильтрации контента, публикуемого в социальных сетях и блогосфере;

➤ «Золотой щит»

«Золотой щит», он же «Великий китайский фаервол» - это система фильтрации интернет-контента, разработка которой началась в 1998 году, а официальный запуск состоялся в 2003. По оценкам экспертов, стоимость ее создания могла составить до \$800 млн., а в ее разработке принимали участие крупные американские корпорации, в частности, IBM. Задачей «Золотого щита» является блокирование доступа пользователей из материкового Китая к некоторым интернет-ресурсам, расположенным на серверах за пределами страны. Список запрещенных ресурсов формируется непосредственно в Пекине и в него входят как сайты политической направленности, так и, что более важно, ведущие мировые социальные сервисы, неподконтрольные пекинским властям.

На начало прошлого года было известно о примерно 2600 сайтах, доступ к которым заблокирован при помощи системы «Золотой щит». Среди этих сайтов 45 ресурсов, входящих в список 1000 самых посещаемых в мире интернет-сайтов по версии сервиса статистики Alexa. Так, в списке заблокированных находятся Facebook.com, Youtube.com, Twitter.com, Blogspot.com, Blogger.com, Vimeo.com, Nytimes.com, Wordpress.com, а также крупнейшие порнографические ресурсы Сети. Крупнейшие российские социальные сети «ВКонтакте» и «Одноклассники» доступны китайским пользователям, однако лишь потому, что местные жители ими практически не пользуются.

Доступ к некоторым сайтам ограничен лишь частично. Так, китайским пользователям доступен сайт Википедии, однако отсутствует доступ к статьям, затрагивающим вопросы китайской политики. Аналогичная ситуация наблюдалась с поисковиком Google, функции которого были доступны лишь частично, до того как компания приняла решение прекратить свою работу в материковом Китае.

Технологически «Золотой щит» предусматривает следующие методы фильтрации:

- Блокировка IP-адресов;
- Фильтрация DNS-запросов и их переадресация;
- Блокировка интернет-адресов (URL);
- Фильтрация на этапе пересылки пакетов;
- Блокировка соединений, осуществляемых через VPN.

Таким образом, «Золотой щит» сочетает в себе практически все возможные на сегодняшний день технические методы фильтрации, используя их выборочно по отношению к тем или иным ресурсам. Это повышает гибкость и точность интернет-цензуры: одни ресурсы могут блокироваться полностью, а другие лишь частично. Анализ пакетов и блокировка VPN и TOR-соединений, в свою очередь, усложняют обход государственных фильтров для рядовых пользователей.

Впрочем, несмотря на расхожее представление, китайские интернет-пользователи совсем не страдают от нехватки сервисов коммуникации. С момента запуска системы «Золотой щит» крупнейшие локальные компании непрерывно копируют наиболее успешные западные интернет-продукты. Так, в Китае существуют практически полные (а зачастую даже усовершенствованные) аналоги сервисов Google (Baidu), Facebook (RenRen), Twitter (Sina Weibo), YouTube (Tudou, YouKu), Wikipedia (Baikе). Аналогами коммерческих сервисов Amazon и eBay являются, соответственно, порталы Dangdang и Taobao.

Масштабы использования данных сервисов колоссальны, так, сервисом микроблогов Sina Weibo регулярно пользуются примерно 300 млн. человек, что превышает аналогичный показатель всего мирового Twitter. Большинство общественно-политических дискуссий, происходящих в китайском сегменте Интернета, сосредоточены преимущественно в этом сервисе, причиной чего отчасти являются особенности китайского языка (1 китайский твит из 140 символов равен по количеству информации примерно 4 английским), а также реализованная система комментариев к твитам, которая больше напоминает Facebook. Таким образом, с точки зрения содержательной насыщенности китайские микроблоги скорее ближе к «большой» блогосфере, нежели к «твиттеру» в российском и американском его понимании.

Несмотря на то, что основной груз цензуры лежит на втором и третьем уровнях системы, они были бы невозможны без существования «Золотого щита». Ключ-

чевая задача этого государственного «фаерволла» - это не блокирование доступа китайских пользователей к политической информации, размещенной на зарубежных сайтах, а создание условий для государственного контроля над ключевыми участниками китайского интернет-рынка. Именно поэтому блокировке подвергаются, прежде всего, глобальные социальные сервисы, предназначенные для обмена информацией между людьми, а отнюдь не политические ресурсы.

Задачей китайского правительства является максимизация возможностей по управлению тем, что и как публикуется в национальном сегменте Интернета без тотального ограничения граждан на самовыражение Сети. «Золотой щит» решает эту задачу, создавая ситуацию, при которой крупнейшие поисковые системы и социальные сервисы принадлежат китайским компаниям (преимущественно частным) и расположены на китайских серверах. Тем самым, главный «рычаг» всегда находится в руках государства.

➤ Блокировка поиска нежелательной информации

На все поисковые системы, работающие в китайском сегменте Интернета, распространяются правила фильтрации поисковой выдачи по ряду ключевых запросов.

Можно разделить все заблокированные ключевые фразы на две группы: постоянные и временные. Постоянная блокировка касается наиболее чувствительных тем, связанных с критикой Коммунистической партии Китая и вопросам прав человека. Примеры постоянно заблокированных ключевых слов: «демократия», «права человека», «диктатура», «митинг», «красный террор», «репрессии», «независимость Тибета» и др. Также в списке заблокированных поисковых запросов большинство имен китайских диссидентов и лидеров запрещенного религиозного культа Фалуньгун. Примечательно, что среди заблокированных поисковых запросов есть и словосочетание «китайско-российская граница», что связано с распространенной критикой в адрес правительства со стороны пользователей, посчитавших демаркацию границы между двумя странами предательством национальных интересов.

Временной блокировке подвергаются слова и фразы, связанные с ограниченными во времени кризисными ситуациями, вне зависимости от их характера. Речь может идти о политических выступлениях, экологических бедствиях или коррупционных скандалах. В этом случае блокировка предназначена снизить потенциальную «вирусность» темы и градус ее обсуждения в блогосфере. Такая блокировка может действовать несколько дней, недель или месяцев.

Поисковые ограничения распространяются не только на специализированные поисковые системы. Аналогичные правила действуют и в крупнейших китайских социальных сервисах, в частности, в сервисе микроблогов Sina Weibo.

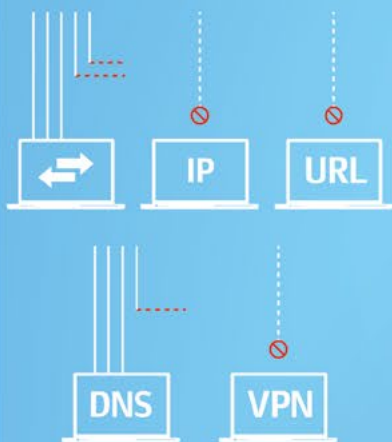
➤ Фильтрация контента в социальных медиа

Несмотря на то, что в публичном поле преимущественно обсуждается «Великий китайский фаерволл», ключевую роль в фильтрации контента играет совсем не он, а десятки тысяч интернет-цензоров, которые вручную просматривают и фильтруют сообщения, публикуемые сотнями миллионов китайских интернет-пользователей в блогах и социальных сетях.

Китай: три этапа интернет-цензуры



«Золотой щит»



Ручная фильтрация
в социальных медиа



50 000 интернет-цензоров
начинают действовать, когда нега-
тивный для китайских властей
информационный повод приобре-
тает «вирусные» черты.



Блокировка поиска
нежелательной
информации

Постоянная блокировка:

Митинг
Диктатура
Репрессии
Фалуньгун
Демократия
Права человека
Красный террор
Независимость Тибета

Временная блокировка:

Экологические бедствия
Коррупционные скандалы
Политические выступления



Ручная фильтрация
в социальных медиа



«Золотой щит»



Блокировка поиска
нежелательной
информации

За последние годы было опубликовано два ключевых исследования, позволяющих понять, как работает эта система: «How Censorship in China Allows Government Criticism but Silences Collective Expression», опубликованное в American Political Science Review гарвардскими профессорами Гарри Кингом, Дженнифером Пэном и Маргарет Робертс, и «Tracking and Quantifying Censorship on a Chinese Microblogging Site», подготовленное группой американских исследователей под руководством китайского независимого эксперта Тао Жу. В обоих случаях анализ проводился преимущественно на основе сервиса микроблогов Sina Weibo, как наиболее значимого интернет-сервиса для общественно-политических дискуссий в Синете (самоназвание китайского сегмента Сети).

В обоих случаях исследователи пришли к выводу о том, что принципы функционирования и задачи китайской интернет-цензуры не так просты, как это принято считать. Анализ фильтруемых сообщений показал, что целью китайской интернет-цензуры не является тотальное искоренение какой-либо политической или общественной критики в социальных сетях. Китайские пользователи не меньше прочих, в том числе и российских, оставляют критические сообщения в адрес правительства и чиновников, и эти сообщения не цензурятся.

Цензоры начинают действовать, когда негативный для китайских властей информационный повод приобретает «вирусные» черты, грозя перерасти в массовые политические выступления, панику или политическое движение, в том числе, виртуальное. Задачей является «срезать» информационную волну, снизив масштаб и накал обсуждения. И, в целом, китайским «интернет-полицией» это зачастую удается.

Эта система состоит из нескольких уровней:

- Правительственные интернет-цензоры;
- Региональные интернет-цензоры;
- Цензоры внутри крупных интернет-компаний;

Китайское правительство не раскрывает данные о численности подразделений «интернет-полиции», но по различным данным на уровне правительства и региональных центров численность цензоров составляет от 20 000 до 50 000 человек. В то же время, основную работу выполняют не они, а цензоры, работающие внутри частных интернет-компаний. В крупнейших компаниях, таких как Sina и Tencent, численность сотрудников, в чьи обязанности входит фильтрация контента, достигает тысячи человек.

При помощи масштабного анализа и задействования сложного технического инструментария американскими исследователями был выявлен как перечень цензурируемых тем, так и различные параметры, связанные с фильтрацией контента.

Логика вмешательства следующая: как только количество сообщений по какой-то теме начинает резко возрастать, а сама тема приобретает характер «информационной волны», цензоры предпринимают меры для разрушения коммуникативных связей между пользователями и препятствуют дальнейшему обсуждению темы. Спустя непродолжительное время, пользователи, лишившиеся возможности публиковать и/или получать отклик аудитории на свои сообщения со стороны других пользователей, начинают терять интерес к теме.

В то же время, в спокойной информационной ситуации, не предвещающей массовых политических выступлений и информационных скандалов, критика

правительства, региональных чиновников и различных явлений общественно-политической жизни не возбраняется. Более того, по мнению ряда исследователей, китайское правительство с большим вниманием относится к критическим публикациям блогеров, особенно в части критики региональных чиновников, воспринимая это как один из ключевых элементов необходимой «обратной связи» для управления страной.

Инструменты фильтрации контента в рамках Sina Weibo можно разделить на три категории: проактивные, реактивные и прочие.

К проактивным инструментам фильтрации относятся:

- Предотвращение отправки сообщений. В этом случае при отправке сообщения Weibo информирует пользователя, что в сообщении содержится контент, который нарушает правила сервиса и не может быть опубликован.
- Премодерация сообщений. В этом случае Weibo принимает к отправке сообщение, однако информирует пользователя, что оно будет опубликовано в течение нескольких минут. Это время требуется для ручной проверки контента цензорами.
- Соккрытие сообщений от других пользователей при публикации. Weibo публикует сообщение, однако делает его невидимым для других пользователей. В этом случае автор сообщения никак не информируется о подобном статусе его публикации.

Реактивные инструменты:

- Удаление ранее опубликованных сообщений. Вместе с оригинальным сообщением удаляются в течение нескольких минут и все «репосты» и комментарии к нему.
- Закрывание аккаунтов наиболее «вредных» пользователей.

Прочее:

- Ограничение поиска по сервису микроблогов.

При «реактивном» удалении сообщений по теме, подавляющее их большинство удаляется в течение часа после публикации. Примерно 90% цензурируемых сообщений, включая репосты и комментарии, удаляются в течение суток после их публикации.

Впрочем, китайские пользователи социальных сервисов быстро научились обходить ограничения блокировки тех или иных слов и выражений при помощи особенностей китайского языка. Так, иероглиф «цензура» в Сети заменяют иероглифом «речной краб», который при различном написании одинаково произносится. Аналогичная ситуация и с другими формально запрещенными словами. Впрочем, подобные уловки могут затруднить работу цензоров, но не делают ее невозможной. При возникновении кризисной информационной ситуации замаскированный контент также подвергается удалению.

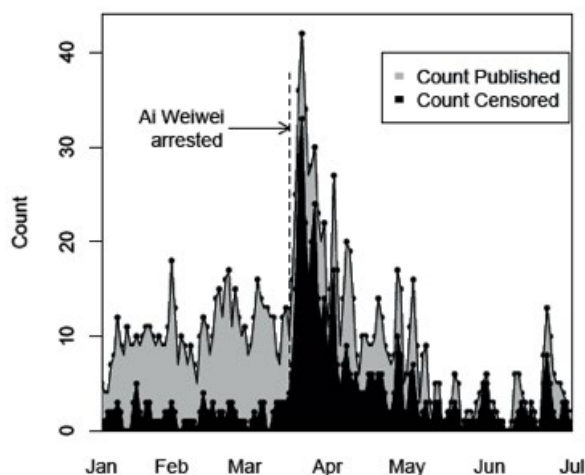
При возникновении потенциально опасной «информационной волны» предпринимаются меры не только направленные на фильтрацию отдельных сообщений, но и на ликвидацию ключевых источников негативной информации. Аккаунты наиболее активных блогеров удаляются, а сами они могут подвергнуться преследованию со стороны правоохранительных органов. Впрочем, сроки ареста для блогеров, как правило, небольшие – от нескольких дней до месяца.

Разумеется, цензоры не в состоянии вручную отслеживать абсолютно все сообщения, публикуемые в системе микроблогов. Мониторинг осуществляется двумя путями. Во-первых, при помощи поиска ключевых слов, относящихся к фильтруемой теме, включая слова-заменители, используемые пользователями для обхода системы фильтрации контента. Второй способ – это персональный мониторинг наиболее «неблагонадежных» пользователей, ранее замеченных в обсуждении чувствительных для китайских властей тем. Их сообщениям уделяется наиболее пристальное внимание.

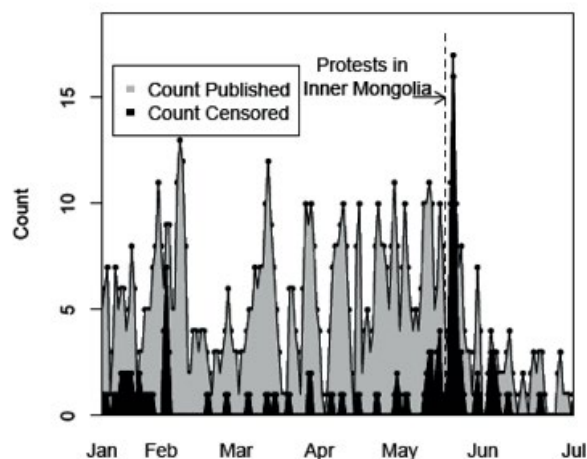
Американским исследователям удалось выделить темы, сообщения по которым подвергались цензуре в период с июля по август 2012 года:

- Наводнение в Пекине, повлекшее смерть нескольких десятков человек, и связанные с ним сюжеты (ключевая общественно-политическая тема периода);
- Антироссийские и антикитайские заявления сирийских боевиков;
- Экологические протесты в восточном Китае по поводу строительства трубопровода;
- Повторный арест правозащитника Ли Гуижи;
- Фотографии группового секса с участием региональных чиновников;
- Избиение японского корреспондента, который брал интервью у участников политических протестов;
- Слух об обрушении одной из станций метро в Пекине;
- Обсуждение высказываний бывшего премьер-министра Китая Вэна Дзябао о политических реформах в Китае в эфире телеканала CNN;
- Протесты в Гонконге против введенного в школах курса «национального образования»;
- Смерть матери и ребенка в результате принудительного аборта, сделанного в рамках политики «одна семья – один ребенок».

Как уже было сказано выше, сообщения по вышеуказанным темам цензурировались ровно в тот момент, когда они приобретали характер «информационной волны» и могли привести к массовым выступлениям. После того как накал темы спадает, активность цензоров постепенно сходит на нет. Проследить это позволяют данные из работы *How Censorship in China Allows Government Criticism but Silences Collective Expression*, собранные в 2011 году:

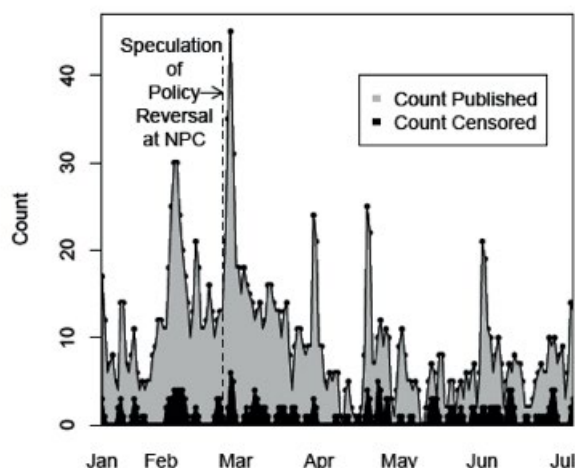


(c) Dissident Ai Weiwei

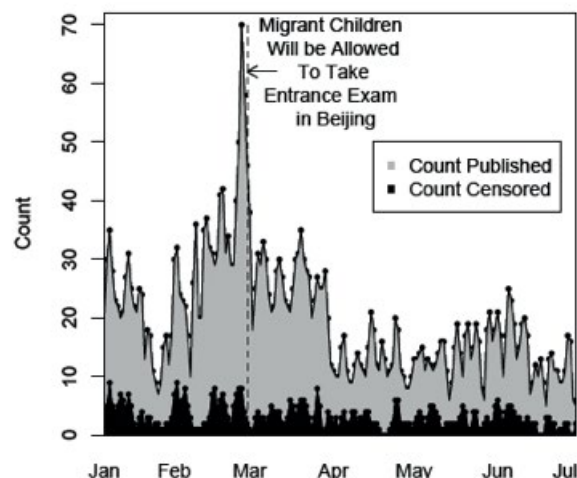


(d) Inner Mongolia Protests

Как уже было сказано, обсуждение тем, негативных для правительства страны, но не предполагающих массовых выступлений граждан, практически не подвергается какой-либо цензуре:

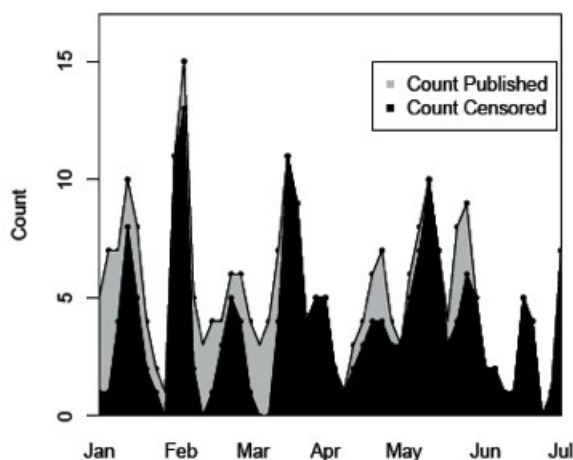


(a) One Child Policy

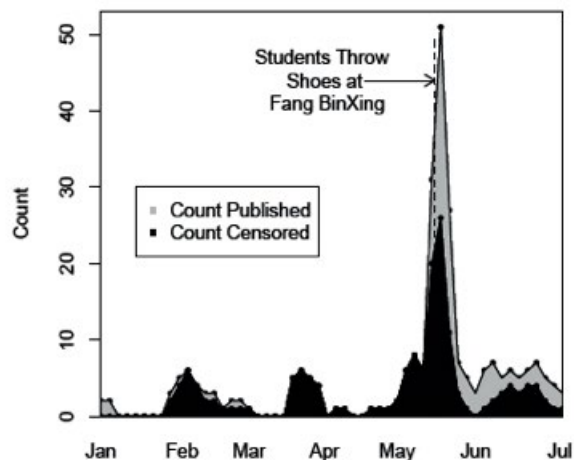


(b) Education Policy

Впрочем, анализ показал, что есть две темы, сообщения по которым фильтруются практически полностью вне зависимости от уровня их обсуждения – это порнография и сама деятельность цензоров:



(a) Pornography



(b) Criticism of the Censors

Стоит отметить, что подобная система цензуры существует не только в Sina Weibo и других крупных общенациональных интернет-сервисах. Цензурируются и сообщения, оставляемые на многочисленных и популярных в Китае региональных и муниципальных интернет-форумах. В данном случае процесс удаления нежелательных записей занимает несколько больше времени, но все равно подавляющее большинство нежелательного контента удаляется в течение суток.

Впрочем, несмотря на наличие столь масштабной и многоуровневой системы контроля за контентом в Сети, китайские власти регулярно выступают с инициативами по введению новых элементов, призванных оградить граждан от

нежелательной информации. Наиболее интересной инициативой подобного рода можно назвать программный комплекс «Зеленая дамба», запущенный в 2009 году.

Все ранее методы фильтрации относятся к либо к производителям и распространителям контента, либо к связи между пользователем и контентом. Однако в данном случае есть еще и третий элемент – сам пользователь. Программное обеспечение «Зеленая дамба» было призвано фильтровать информацию на стороне клиента, представляя собой аналог пользовательского фаерволла.

Предполагалось, что предустановка данной программы будет обязательной на всех персональных компьютерах, продаваемых в Китае с 1 июля 2009 года. Однако сперва правительство КНР приняло отложить дату запуска системы из-за многочисленных технических проблем и того факта, что производители компьютеров не успевали установить программу на свою продукцию. Впрочем, уже в августе 2009 года было принято решение сделать установку «Зеленой дамбы» необязательной, а к концу 2010 года правительство отказалось от данного проекта вовсе, пообещав, однако, что в будущем вернется к этому вопросу.

В конце 2012 года была предпринята еще одна попытка усиления государственного контроля над интернет-пространством. Власти Китая решили воспользоваться опытом соседней Южной Кореи и провести масштабную деанонимизацию китайской блогосферы. Был принят закон, обязывающий пользователей регистрироваться в социальных сервисах, таких как Sina Weibo, под своими настоящими именами. Те пользователи, которые зарегистрировались ранее, также должны были сообщить свои паспортные данные операторам сервисов. Впрочем, спустя некоторое время выяснилось, что несоблюдение данной нормы не приводит к каким-либо санкциям, поэтому значительная часть блогеров предпочла сохранить свой анонимный статус.

Интернет-цензура в Иране

По доли населения, пользующегося Интернетом, Иран занимает второе место на Ближнем Востоке, уступая только Израилю. В стране особенно развита блогосфера – по оценкам экспертов, число регулярно обновляемых блогов превышает 60000. Усилия правительства Ирана, с одной стороны, направлены на развитие инфраструктуры Интернета, с другой – на полный контроль того, что публикуется пользователями в Сети.

В условиях жестких законов, регулирующих прессу, Интернет до 2004 года оставался одной из немногих площадок, где можно было свободно выражать свое мнение. Но постепенно такой источник свободомыслия привлек внимание властей Ирана, и они начали реализацию последовательной политики по борьбе с нежелательным контентом. Действие положений закона о прессе было расширено на электронные публикации. Дополнительным стимулом для усиления контроля над Интернетом стали массовые протесты после президентских выборов 2009 года, когда оппозиция использовала социальные сети для координации акций и связи с западными новостными агентствами.

Ограничения своды слова прямо предусмотрены иранской конституцией, в которой сказано, что «средства массовой информации должны воздерживаться от разрушительных и анти-исламских практик». Закон о прессе также ограничивает недопустимую информацию, в частности «освещение тем, которые вредны для основ Исламской республики», «оскорбление Лидера Революции», «подстрекательство граждан к действиям против безопасности, достоинства и интересов Исламской республики». Также запрещены любые публикации, оскорбляющие ислам. Такие расплывчатые категории позволяют властям блокировать практически любую информацию по своему усмотрению.

Фильтрация контента в Интернете до недавнего времени осуществлялось на основании серии постановлений Верховного Совета Культурной революции, а определение критериев для блокирования было вверено межведомственному комитету, в который входят представители министерств культуры, безопасности и Генеральной прокуратуры. Практической реализацией политики фильтрации занимается подразделение главной государственной телекоммуникационной компании и агентство Министерства по коммуникациям. В 2012 году лидер Ирана Хаменеи объявил о создании Верховного совета по киберпространству, который с этого момента занимается выработкой единой политики в отношении Интернета.

Все провайдеры страны должны получать лицензию от государственных органов, а пользователи подписывают обязательство не посещать «анти-исламские сайты». Для домохозяйств действует лимит на скорость в 128 Кбит/с, который облегчает нагрузку на систему фильтрации, а также ограничивает доступ пользователей к нежелательным западным фильмам и музыке. На организации и университеты он не распространяется. На данный момент Иран остается единственной страной, где действует законодательное ограничение на скорость доступа в Интернет для пользователей.

Одним из условий предоставления провайдерам лицензии является установка системы фильтрации, которая блокирует список веб-страниц, предоставленный государством. Первоначально вся цензура осуществлялась именно на уровне провайдеров, но в последние годы власти Ирана разработали и внедрили централизованную систему, которая работает в связке с фильтрами провайдеров. Этот шаг обеспечил большее единообразие в политике цензуры, так как ранее она сильно варьировалась от провайдера к провайдеру. Техническая фильтрация в Иране прозрачна - при попытке обращения к сайту, занесенному в государственный список, выдается блок-страница с разъяснением, что ресурс недоступен, и контактами администратора, которому можно направить запрос.

Фильтры, применяемые в Иране, представляют собой прокси-серверы, на которые перенаправляется трафик пользователей. Каждый запрос сверяется со списком заблокированных сайтов и страниц, а также анализируется на предмет наличия определенных ключевых слов. В случае совпадения пользователь перенаправляется на блок-страницу.

Ранние исследования OpenNet Initiative показывали, что техническим решением, которое устанавливали интернет-провайдеры, был SmartFilter американской фирмы Secure Computing. Сама компания-производитель отвергала продажу программного обеспечения, утверждая, что Иран использует его незаконно. Сотрудничество с Ираном в этой сфере могло стать не только серьезным ударом по репутации Secure Computing, но и возможным нарушением экономических санкций США.

Власти Ирана были недовольны зависимостью своей системы фильтрации от западных технологий, опасаясь встроенных уязвимостей, которые могут нарушить ее работу. Поэтому их усилия были направлены на переход к информационным решениям, разработанным местными компаниями. На сегодняшний день техническая система фильтрации Ирана использует собственные разработки не только для блокирования сайтов, но и для автоматического поиска запрещенного контента в Сети.

В Иране действует жесткая система контроля за пользователями. Интернет-провайдеры обязаны хранить в течение 3 месяцев не только логи, но и саму информацию, передаваемую пользователями. Когда один из иранских диссидентов был арестован за высказывания в системе мгновенного обмена сообщениями, доказательством его вины выступала распечатка его переписки. Пользователи интернет-кафе должны предоставлять свою идентификационную информацию, а владельцы обязаны устанавливать в помещении камеры и хранить записи о посетителях.

Мнения специалистов расходятся в оценке способности Ирана применять технологию глубокого анализа пакетов. В 2008 году компанию Nokia Siemens Systems обвинили в поставках главному телекоммуникационному оператору страны оборудования, способного массово перехватывать сообщения пользователей. Однако представитель NSS заявил, что его возможности ограничены только законным отслеживанием коммуникаций отдельных пользователей в рамках деятельности правоохранительных органов. Расследование Reuters и Wall Street Journal показало, что две китайские корпорации Huawei и ZTE сотрудничали с властями Ирана в создании системы интернет-слежки. Их представители также отвергли эти обвинения. Тем не менее, имеется ряд свидетельств того, что Иран обладает подобной технологией. Так, в 2012 году в преддверье выборов власти блокировали весь зашифрованный трафик.

Поправки к закону о прессе Ирана, принятые в 2009 году, обязывают владельцев сайтов проходить процедуру регистрации в Министерстве культуры, которое имеет право отзывать лицензию и запрещать отдельные публикации. По положениям другого закона, интернет-сервисы отвечают за материал, размещаемый в них другими пользователями. В этих условиях, широкое распространение получила самоцензура, когда пользователи опасаются высказывать свое мнение онлайн, а владельцы сайтов по своей инициативе удаляют любой спорный контент.

Власти Ирана активно применяют уголовное преследование в отношении пользователей Интернета, в том числе смертную казнь. По информации Human Rights Watch, в 2011 Иран установил рекорд по количеству арестованных блогеров и журналистов. По уголовному кодексу Ирана наказание вплоть до смертной казни предусмотрено за «пропаганду против государства», «оскорбление религии», «волнение общественности» и «распространение ложных слухов». Так, в 2004 году блоггер был арестован за сообщение об аресте трех других пользователей. В 2012 году по обвинению в распространении дезинформации был арестован администратор сайта, который сообщал о курсе национальной валюты по отношению к доллару.

По заявлению представителя официальных властей, в 2006 году в Иране были заблокированы более 10 миллионов сайтов, 90% из которых относились к «аморальному контенту». Порнография остается одним из главных приоритетов для блокирования. При этом к ней Иран относит даже изображения провокационной одежды. Поисковые запросы, содержащие слова «секс», «женщина» и «фотография» на фарси или английском также блокируются. Фильтруются и многие другие сайты, близкие к этой тематике, в частности сайты знакомств, материалы по половому просвещению и ресурсы ЛГБТ-сообщества.

Другой широкой категорией контента, доступ к которой в Иране ограничивается, являются сайты, нарушающие нормы ислама. Блокируются ресурсы, связанные с употреблением наркотиков и алкоголя, а также азартными играми. За критику государственной религии предусмотрено суровое наказание, а подобные сайты, расположенные за рубежом, тщательно блокируются.

Согласно результатам тестирования OpenNet Initiative, Иран занимает первое место в мире по доле заблокированных ресурсов политического характера. Основные усилия цензоров сосредоточены на материалах на фарси; из сайтов на иностранных языках блокируются только самые крупные новостные порталы, такие как The Huffington Post, Al-Arabiya и Global Voices.

Среди фильтруемого политического контента находятся сайты политической оппозиции, правозащитных организаций, в частности выступающих за права женщин, этнических и религиозных меньшинств, активистов и журналистов, критикующих режим. Если после выборов 2009 года активно блокировались ресурсы кандидатов, выступающих против действующего президента Ахмадинежада, то в 2011 году недоступным оказался и сайт группы его сторонников.

По состоянию на 2012 год, в Иране заблокированы крупнейшие международные интернет-сервисы, такие как Facebook, YouTube, Twitter и Flickr. Доступ к сервисам Google периодически пропадает, что затрудняет их использование. Заблокированы большинство платформ для ведения блогов, в том числе Livejournal и Xanga.

В 2011 году Иранские власти объявили о планах по созданию Национального Интернета, предусматривающих защиту страны от киберугроз, ограничение доступа пользователей к контенту за рубежом, а также более строгий контроль за их действиями. Инициатива предполагает создание национальных аналогов по-

исковых систем, почтовых сервисов и платформ для ведения блогов. Недостаток официальной информации привел к появлению разных версий того, какие цели преследует Иран. По одной из них, под Национальным Интернетом подразумевается сеть, полностью изолированная от глобальной, наподобие действующей в Северной Корее. В то же время, представители властей заявили, что в качестве базовой модели выбрано регулирование Интернета в Китае, когда весь внешний трафик строго контролируется, но доступ к нему сохраняется.

Социальные медиа и кризисы политической легитимности. Возможные меры реагирования со стороны властей

Считается, что наиболее значимо «новые медиа» показали себя в ходе институциональных кризисов, когда массовая политизация социально активного сегмента Интернета привела к взрывному росту влияния блогосферы и социальных сетей на ход кризисных событий. Тем не менее, всплеск интереса к влиянию социальных медиа в подобных ситуациях, хоть и привел к появлению термина «твиттер-революций», но до сих пор так и не стимулировал формирование полноценной научной базы.

➤ 2009 год. Появление понятия «Twitter-революций»

Политические кризисы в Молдавии, а затем в Иране, которые пришлось на весну-лето 2009 года, обозначили «сетевое» изменение публичной сферы этих стран. Массовые протесты людей, неудовлетворенных результатами выборов, были отмечены всплеском популярности социальных сетей и блогосферы среди «ядра» протеста – идеологов и неформальных лидеров групп, составлявших базу оппозиционного движения.

Именно молдавские события подтолкнули европейских и американских журналистов к тиражированию понятия «Twitter-революции», несмотря на то, что сами по себе они слабо соответствовали образу, который создавался в медиа. Несоответствие реального положения дел и описательных характеристик,, которые массово распространялись в медиа, обусловлено «ускоренной эксплицитностью» - стремлением наблюдателей (прежде всего журналистов и политических комментаторов) оперативно закрепить определенное понятие в общественном поле и, тем самым, предопределить дальнейшие форматы применения данного понятия. Образ «Twitter-революции», растиражированный

западными СМИ¹⁰¹¹ при описании ситуации с массовыми протестами в Молдавии, предопределил дальнейшие исследования использования социальных медиа в рамках политических кризисов различных стран.

Следует заметить, что в начале апреля 2009 г. не «революционно» новым, но самым популярным методом мобилизации в Молдавии стали флэшмобы, организуемые при помощи SMS-сообщений, которые использовались и в ходе самих выборов, и после них. Флэшмобы и вирусные кампании также организовывались в социальных сетях – в частности, на популярном в стране сайте «Одноклассники». Сервис микроблогов Twitter стал активно использоваться позже, но именно его использование ядром оппозиционных активистов привлекло внимание западных СМИ¹². Более того, среди тех, кто активно освещал события в Кишиневе, самыми заметными микроблоггерами оказались не непосредственные участники событий, а наблюдатели, румынские журналисты и граждане Молдавии, проживающие за рубежом. В результате, Twitter использовался не для координации и мобилизации, но практически исключительно для привлечения внешнего внимания – в основном при помощи «географического» хэштега #rman (около 30 тысяч твитов). Плотность записей составляла около 10 твитов в минуту¹³.

Первый масштабный случай интернет-цензуры в Молдавии пришелся на 7 апреля – спустя двое суток после дня голосования, когда у многих пользователей наблюдались проблемы с доступом в Сеть. Однако достаточно быстро общий доступ в Интернет был восстановлен и подконтрольные государству провайдеры применяли ограничения избирательно: проблемы наблюдались с информационными ресурсами оппозиции, сайтами НКО. По мере возрастания роли Twitter, лояльные власти активисты включались в дискуссии по соответствующим хэштегам, чтобы затруднить координацию противников коммунистической партии. 9 апреля 2009 г. на территории Молдавии был заблокирован доступ в социальную сеть «Одноклассники», в которой функционировали оппозиционные группы. В целом, молдавские власти сконцентрировались на цензуровании сайтов, чьи хостинги располагались в Молдове, в то время как Twitter был обойден властями вниманием.

Молдавские события показали, что использование социальных сетей позволяет частично масштабировать не только сами события, но и роль активистов-блоггеров в них. Также нельзя недооценивать роль традиционных медиа – румынских телеканалов и радиостанций, которые транслировали оппозиционный контент, тем самым участвуя в запуске своеобразного «информационного бумеранга», когда традиционные СМИ масштабируют контент «новых медиа» и тем самым повышают уровень значимости блоггеров-активистов¹⁴.

В июне 2009 г. после прошедших в Иране президентских выборов был зафиксирован масштабный кризис легитимности политической власти в стране, который привел к массовым беспорядкам и жертвам среди местного населения. В то же время, роль социальных медиа в тех событиях считалась столь примечательной, что некоторые предлагали присудить Нобелевскую премию мира в 2009 г. сервису микроблогов Twitter.

10. Stack, G. (2009). 'Twitter revolution' Moldovan activist goes into hiding. The Guardian

11. Hodge, N. (2009). Inside Moldova's Twitter Revolution. The Wired

12. Morozov, E. (2009). More analysis of Twitter's role in Moldova. Foreign Policy.

13. Desouza, K.C. & Lysenko, V.V. (2012). Moldova's internet revolution: analyzing the role of technologies in various phases of the confrontation. Technological forecasting & social change: an international journal. Vol. 79.

14. Blogs and Bullets: New Media in Contentious Politics. (2010). Peaceworks.

Согласно статистике, которую приводит Американский институт мира, уже в 2007 г. Интернетом в Иране пользовались больше 32% населения. Власти страны осознавали важность роста проникновения Сети не только для предотвращения оппозиционной мобилизации в блогосфере, но и предлагая свою информационную повестку – прежде всего задействуя консервативный и религиозный кластеры пользователей¹⁵. В течение нескольких лет, предшествовавших выборам президента, в Иране была налажена система политической и религиозной цензуры Сети, что предопределило высокую степень самоорганизации среди активистов оппозиционных сил. Жесткая фильтрация контента в Иране и массовое присутствие сторонников власти в социальных сетях, таким образом, сделало протестное движение более консолидированным и ожесточенным¹⁶.

Как и в случае Молдавии, большинство населения Ирана оставалось в роли сторонних наблюдателей за протестами, частично координировавшимся при помощи Facebook и Twitter. По оценкам ряда экспертов¹⁷, активных пользователей Twitter, принимавших участие в уличных протестах, насчитывалось всего лишь около 100, а главным инструментом координации стали SMS. Twitter использовался для привлечения внимания международного сообщества – в первую очередь американских СМИ. «Вирусное» видео, запечатлевшее трагическую гибель Неды Солтани, принимавшей участие в тегеранских выступлениях, стало известным на весь мир благодаря телеканалу CNN. Неудивительно, что главным объектом цензуры со стороны иранских властей стал видеохостинг YouTube, заблокированный в дни массовых протестов. Основной упор в ограничении коммуникации, тем не менее, пришелся на мобильную связь.

В момент эскалации кризиса легитимности в Иране, как и до него, деятельность лояльных сторонников власти в социальных сетях, по оценкам экспертов, была сравнима по количественным характеристикам с активностью сторонников оппозиции. Несмотря на использование многими активистами английского языка в апелляциях к международному сообществу посредством Twitter и масштабное распространение контента оппозиционных иранских блоггеров в западных СМИ, политические последствия вирусного «эффекта бумеранга» столкнулись не с виртуальными, а реальными действиями иранских властей и правоохранительных органов.



15. Burns, A. & Eltham, B. (2009). Twitter Free Iran: an Evaluation of Twitter's Role in Public Diplomacy and Information Operations in Iran's 2009 Election Crisis. Communications Policy & Research Forum

16. Blogs and Bullets: New Media in Contentious Politics. (2010). Peaceworks.

17. A Look at Twitter in Iran (2009). Sysomos Blog.

Популярность Twitter и социальных сетей в иранских событиях привела к жесткой ответной реакции спецслужб, получивших доступ к открытым данным пользователей – участников и организаторов массовых протестов. Таким образом, облегченный доступ к личной информации со стороны представителей власти и анализ видео- и фотоматериалов, которые публиковали участники уличных выступлений, составляют одну из ключевых характеристик возможных последствий актуализации новых медиа в моменты политических кризисов¹⁸. Поддержка извне, в том числе при помощи инструментов новых медиа, в конечном итоге была скомпрометирована.

➤ «Арабская весна»

Выступление бывшего Госсекретаря США Хиллари Клинтон в январе 2010г.¹⁹, в котором она сделала акцент на недопустимости цензуры Интернета и эффективности блогосферы и «новых медиа» в области защиты прав человека, пришлось на период относительного «затишья» в осмыслении нового феномена. В своей речи Клинтон отдельно выделила блоги, электронную почту, социальные сети и текстовые сообщения, «открывшие новые площадки для обмена идеями и создавшие новые цели для государственной цензуры». В декабре того же года самосожжение тунисского торговца овощами Мохаммеда Буазизи и видео инцидента, распространенное в Сети, послужили триггером серии кризисов легитимности политических режимов в арабском мире.

Показательно, что новость о самосожжении Буазизи была проигнорирована традиционными СМИ Туниса, в результате чего роль Twitter (распространение соответствующего хэштега и т.п.) и Facebook чрезвычайно возросла. Информационный вакуум местных СМИ был также заполнен арабским спутниковым каналом Al-Jazeera, что в отличие от ситуации в Иране-2009 и роли CNN, заметно усиливало эффект местного «информационного бумеранга». Стремительный рост доверия альтернативным источникам информации вне зоны влияния государственных властей следует считать отличительной чертой указанных событий.

Кроме существовавшей государственной интернет-цензуры в Тунисе (блокировка сервисов YouTube, Flickr, Vimeo), власти страны ввели жесткие ограничения доступа к соцсети Facebook. Помимо этого, были заблокированы ряд арабских и европейских новостных сайтов, размещавших информацию о ситуации в Тунисе (BBC, France24). Внедряя дополнительные цензурные ограничения, тунисские власти частично осложнили коммуникацию между участниками уличных выступлений, однако альтернативная информационная повестка со стороны прежнего политического режима не пользовалась популярностью²⁰.

Цензура в Египте во время политического кризиса стала одной из наиболее жестких среди аналогичных мер других государств. Осенью 2010 г. в стране прошла серия громких увольнений в египетских медиа. Это предопределило знаковую роль, которую в египетских событиях сыграли журналисты. Параллельно в Египте

- 18. Gladwell, M. (2010). Small Change: Why the revolution will not be tweeted. The New Yorker.

19. Clinton, H.R. (2010). Remarks on Internet Freedom.

20. Freedom on the Net (2012). Freedom House.

внедрялась тематическая цензура, были заблокированы сайты оппозиционных газет Dostora и Ikhwanī Web. В конце января перед властями Египта встал выбор – блокировать ли Facebook, Twitter, Bambuser полностью. Решение приостановить доступ к Facebook и Twitter было принято после того, как была налажена успешная координация между оппозиционными активистами и широкую популярность приобрела оппозиционная страница «Мы все Халед Саид»²¹.

Name	Times Rted	Followers	Affiliation	Location
@ghonim	35265	12491	individualC	ario
@dima_khatib	25062	11320	journalist	Latin America
@bencnn	24066	21147	journalist	Cairo
@3arabawy2	1607	9022	journalist	Cairo
@sandmonkey2	0714	6943	bloggerC	airo
@alarabiya_ar1	5681	14011	mainstream media	Arab World*
@monaeltahawy	14150	16048	journalist	Cairo
@ajenglish	13791	145246	mainstream media	Arab World*
@ajarabic	12687	30244	mainstream media	Arab World*
@monasosh	12609	2535	blogger	Alexandria

Самые популярные Твиттер-аккаунты во время политического кризиса в Египте. Kate Starbird, Leysia Palen, University of Colorado Boulder, 2012.

27 января на территории Египта практически полностью был заблокирован доступ в Интернет. Блокировка длилась до 2 февраля, а обмен SMS был затруднен вплоть до 6 февраля. Многие аналитики, в том числе Александра Данн из Каирского Института прав человека, полагают, что именно цензурирование сотовой связи, а не сетевая цензура, привело к мощной волне социального возмущения и вынудила неполитизированные слои общества стать участниками политических событий того периода²². Кроме того, в результате столь резкого вмешательства государства, еще более популярным источником информации стали спутниковые СМИ – прежде всего телеканал Al-Jazeera, и политический режим стал еще более подвержен информационному давлению извне²³. Согласно тем же данным, более 45 процентов «твитов», посвященных событиям в Египте, были опубликованы за пределами Египта и прилегающих стран арабского мира. Жители Каира являлись авторами лишь 29% записей о волнениях в стране. Более 60% сообщений составляли «ретвиты»²⁴. В Египте, как ранее в Иране, наблюдалось широкое использование английского языка – особенно в распространении мемов, публикуя которые активисты стремились «интернационализировать» освещение происходящих в стране процессов²⁵.

21. Dunn, A. Unplugging a Nation: State Media Strategy During Egypt's January 25 Uprising. (2011). Fletcher Forum of World Affairs.

22. Dunn, A. Unplugging a Nation: State Media Strategy During Egypt's January 25 Uprising. (2011). Fletcher Forum of World Affairs.

23. Mourtada, R., & Salem, F. (2011). Civil Movements: The Impact of Facebook and Twitter. Arab Social Media Report. 1(2). Dubai: Governance and Innovation Program at the Dubai School of Government.

24. Palen, L. & Starbird, K. (2012). (How) Will the Revolution be Retweeted? ACM Conference on Computer Supported Cooperative Work.

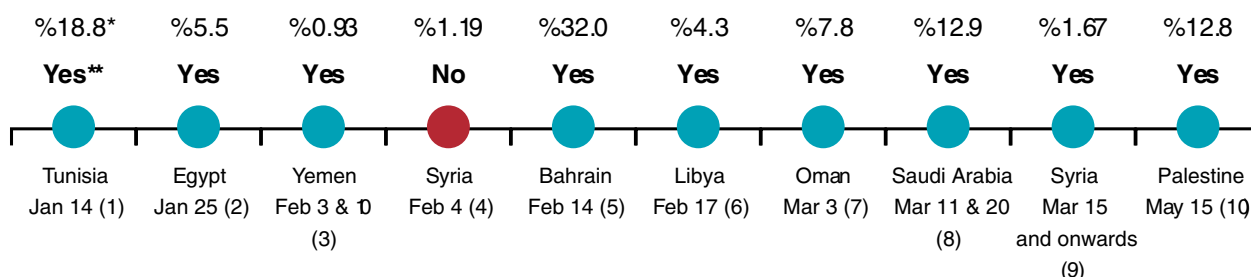
25. Mourtada, R., & Salem, F. (2011). Civil Movements: The Impact of Facebook and Twitter. Arab Social Media Report. 1(2). Dubai: Governance and Innovation Program at the Dubai School of Government.

➤ Общие характеристики волны 2011 г.

Помимо очевидных различий между примерами Туниса, Египта, Сирии, Ливии, Бахрейна, ОАЭ, Алжира и других стран, в этом регионе фиксировались схожие черты всплеска популярности инструментов социальных сетей на фоне политики государственной цензуры в Сети и обострения ряда социальных и политических конфликтов.

Согласно данным сайта телеканала Al-Jazeera, охват аудитории этого СМИ достигает 260 миллионов домовладений. При этом около 50% посетителей сайта телекомпании проживает на территории Северной Африки, где в течение 2011-2012 гг. фиксировалась ситуация крайней политической нестабильности²⁶. По аналогии с примерами Молдавии и Ирана, роль традиционных медиа во многом состояла в ретрансляции контента блогосферы и соцсетей и запуске медийного «бумеранга», масштабирующего политические явления.

Обострение политической ситуации, во время которого отмечался всплеск политизации «новых медиа», совпал с интернет-бумом в целом ряде стран региона. Так, согласно данным Школы управления Дубаи количество пользователей Facebook в арабском мире выросло на 78% за 2010 год²⁷. Практически во всех странах региона создание страницы-мероприятия Facebook, связанной с проведением общенационального митинга, приводило к реальным уличным выступлениям.

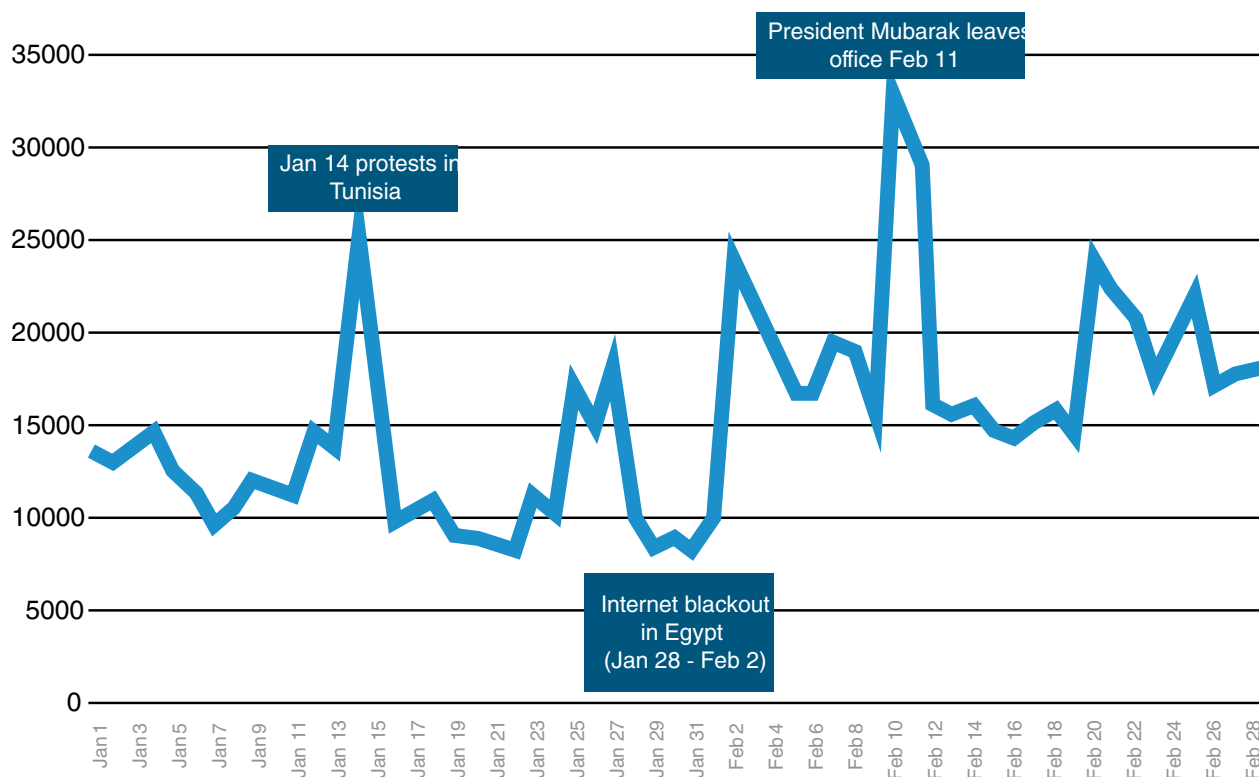


Существование мероприятий в Facebook и фактические уличные выступления. В виде процентов указана степень проникновения Facebook. Arab Social Media report, Vol.1, 2011

Активное использование Facebook и Twitter в ходе социальных протестов стремительно перешло в политическую плоскость по мере смены локальных социальных кризисов политическими. По сравнению с проникновением Facebook в Египте и Тунисе на 2011 г. (7,66% и 22,49% соответственно) показатели Twitter гораздо меньше – 0,15% и 0,34%. Странами-лидерами по охвату Twitter на тот момент являлись Кувейт, Катар и ОАЭ. Тем не менее, популярность этого сервиса в западных странах, граждане которых поддерживали хэштеги #protest, #egypt, #jan25 и другие, внесла лепту в итоговую роль Twitter в арабском мире образца 2011 г. Среднее количество записей достигало около трех твитов в секунду.

26. Al Jazeera (2012). Facts and figures. Al Jazeera official web page.

27. Mourtada, R., & Salem, F. (2011). Civil Movements: The Impact of Facebook and Twitter. Arab Social Media Report. 1(2). Dubai: Governance and Innovation Program at the Dubai School of Government.



Пиковые события в Twitter стран арабского мира зимой 2011 г. Arab Social Media report, Vol.1, 2011

Одной из причин решающей роли Facebook в сравнении с Twitter стал доступный на тот момент языковой арабский интерфейс социальной сети, в то время как распространение англоязычного Twitter редко выходило за пределы населения столиц Египта и Туниса и еще нескольких крупных городов. Однако, преувеличивать роль Facebook в организации протестных акции и внушительной политической мобилизации также не следует – многие исследователи полагают, что без налаженных горизонтальных «традиционных» (не виртуальных) сетевых структур стран арабского мира, виртуальное чувство солидарности не нашло бы применения в политической практике. Именно благодаря подобным сетям, количество пользователей социальных сетей, степень их мобилизации и политизации заметно возросли во время событий в странах арабского мира.

В результате действий государственных органов по ограничению доступа в Интернет, наблюдатели фиксировали резкое падение трафика. Одним из немногих исключений в этом контексте стала Сирия, где ограничение доступа в YouTube, привело только к росту популярности этого видеохостинга.



Трафик YouTube в Сирии, февраль 2011 г. Google Transparency Report, 2011.

Популярность социальных сетей и степень самоорганизации граждан, в том числе, были предопределены широким распространением смартфонов, которые превратились в медийные инструменты, будучи источниками оперативной информации и визуальных данных. Согласно данным профессора Университета имени шейха Зайеда (ОАЭ) Мэтта Даффи, доля обладателей смартфонов среди протестующих в Египте составляла 15%²⁸. При помощи смартфонов действиям участников событий был придан новый импульс – активисты стали журналистами, размещавшими пользовательский контент практически в прямом эфире. Помимо этого, смартфоны позволяли организовывать неподцензурную коммуникацию (речь, в частности, идет о телефонах Blackberry).

Очевидно, что несмотря на существующий тренд «утяжеления» доли социальных медиа не только в общественно-политической жизни государств, но и повышения их значимости в ходе структурных и институциональных кризисов, следует предположить, что исследование воздействия данных инструментов коммуникации на конкретные социальные явления может не быть настолько же динамичным. Социальные сети постепенно становятся столь же привычным инструментом мобилизации и фактором в организации массовых протестных движений, как короткие текстовые сообщения и традиционные СМИ. Несмотря на то, что общественные явления в 2000-х годах проходили под влиянием бума мобильной связи, никому из исследователей не приходит в голову называть, к примеру, события на Украине 2004 г. «SMS-протестами».

Можно предположить, что пик информационной актуализации новых медиа в этом смысле пройден и в ближайшие годы их растущей роли будет уделяться заметно меньше внимания, нежели чем в 2009-2012 гг. Этому также способствует низкая институциональная ценность социальных медиа в странах, продолжающих находиться в ситуации политической нестабильности. Дискурс, показавший себя в организации протестного движения, оказался куда менее эффективным по прошествии кризисных пиков. Кроме того, открытый и расширяющийся общественный дискурс, представленный в социальных сетях, позволяет представителям власти отслеживать и анализировать потенциально кризисные явления и предотвращать их.

➤ Перспективы

Значимость оперативного реагирования государственной власти на повестку социальных медиа возрастает с каждым годом. Постепенно это явление утрачивает суть феномена и перестает быть чрезвычайно популярным объектом для изучения, как это было в 2009-2011 гг.. Социальные сети с течением времени становятся столь же привычным инструментом мобилизации и значимым фактором при организации массовых протестных движений, как каналы традиционных СМИ, мобильные средства связи и непосредственное «живое» общение.

Проанализированные примеры реакции властей на активность в социальных медиа во время политических катаклизмов доказывают, что наиболее эффективным методом контроля над ситуацией является предложение альтернативной повестки, которая может частично заместить оппозиционный дискурс в Интернете. При этом особую роль играет правильно выбранная целевая аудитория для соответствующей информационной политики. К примеру, массовое вовлечение неполитизированных

28. Duffy, M. (2011). Smartphones in the Arab Spring. International Press Institute.

пользователей далеко не всегда приносит искомый результат. Регулярный мониторинг и анализ трендов дискуссий, выявление потенциальных конфликтов, также трудно переоценить в контексте предотвращения кризисных ситуаций.

В то же время, существование комплексной сетевой цензуры без формирования альтернативных медийных каналов, может негативно повлиять на попытки контроля за ситуацией. Ядро политических активистов в таких случаях оказывается более отобризованным к моменту обострения политической ситуации и готовым к реализации нестандартных решений. Обратной стороной данной ситуации является силовой сценарий, при котором правоохранительные органы государства получают облегченный доступ к личным данным сетевых активистов, подозреваемых в нарушении закона и призывах к массовым беспорядкам.

Тотальная сетевая цензура (блокировка главных ресурсов оппозиционных активистов), введенная во время обострения политической обстановки, не гарантирует снижения уровня мобилизации, а наоборот может привести к эскалации конфликта вне Сети. Ослабление социальных связей в виртуальном пространстве предоставляют власти временное преимущество, которым еще надо грамотно воспользоваться²⁹. Тематическая цензура может быть также неэффективной в случае, если альтернативные источники информации (в т.ч. традиционные медиа) поставляют контент взамен запрещенного. В целом, эффективность контроля над ситуацией в «новых медиа» неразрывно связана с положением традиционных СМИ, усиливающих «эффект бумеранга» в случае введения интернет-цензуры.

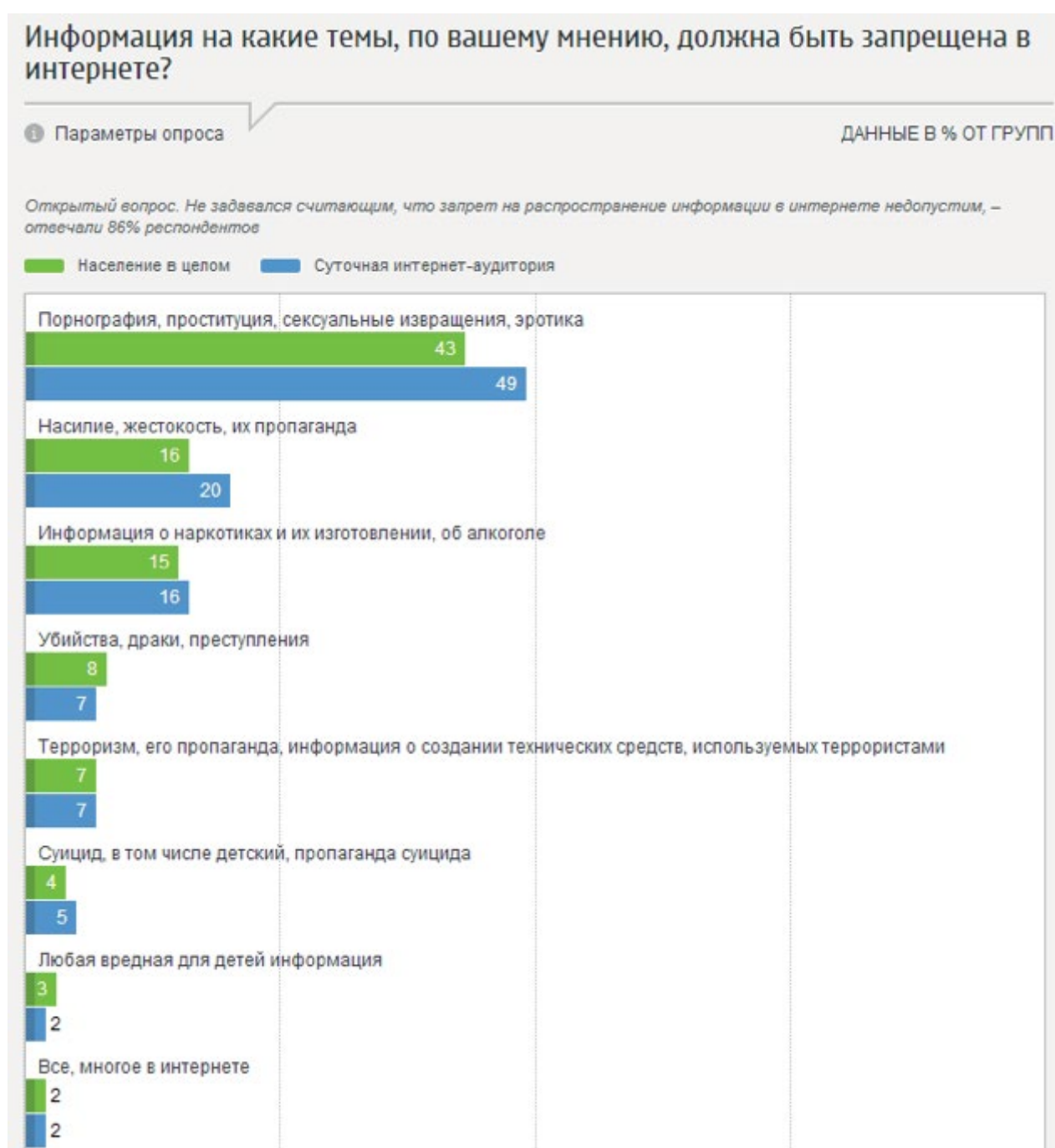
Показательно, что во многих странах, переживших серьезные политические кризисы легитимности с 2009 по 2012 гг., социальные сети зачастую не являются инструментом консолидации социума или выработки нового общественного договора. Согласно исследованию Crimson Hexagon и Sanitas International, спустя несколько месяцев после свержения режима Каддафи в Ливии, треть всех дискуссий в Twitter была по-прежнему посвящена разделу имущества и наказанию семьи бывшего правителя страны³⁰. Методы коммуникации, проявившие себя в организации протестного движения, оказались существенно менее эффективными для выстраивания политической коммуникации по прошествии кризисных пиков.

29. Gladwell, M. (2010). Small Change: Why the revolution will not be tweeted. The New Yorker.

30. Franceschi-Bicchieri, L. (2013), What Happens to Social Media After a Twitter Revolution? Mashable.

Рекомендации для России

Бессмысленно рассуждать о полном копировании в России любой модели фильтрации интернет-контента, используемой в других странах. Любые решения в этой области должны приниматься исходя из тех целей и задач, которые ставят перед собой государство и общество. Последнее социологическое исследование на тему того, что россияне думают о государственном регулировании Сети, было проведено Фондом «Общественное мнение» в январе 2013 года. Наиболее интересные данные из этого исследования приведены ниже³¹:



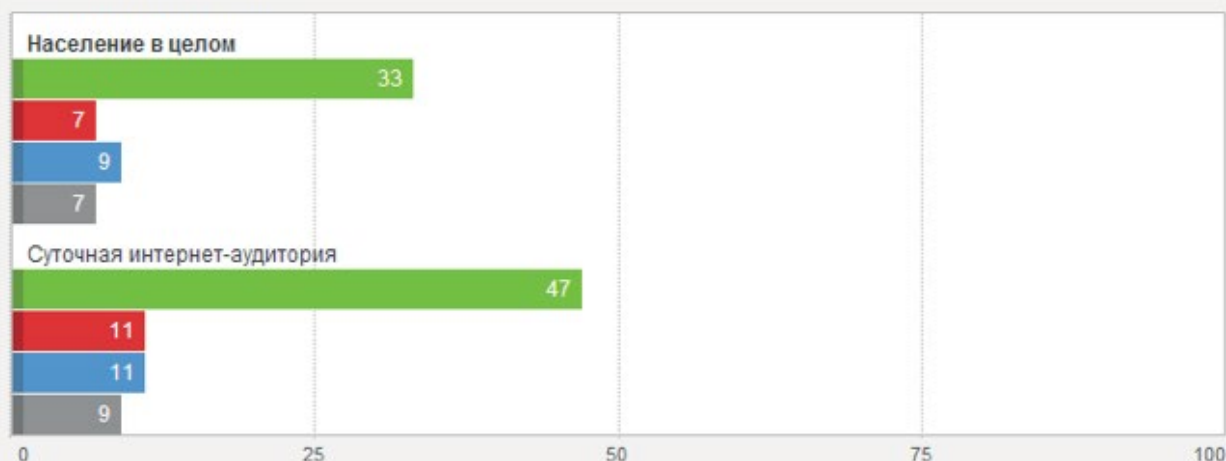
Как вы оцениваете деятельность Роскомнадзора по ведению реестра запрещенных сайтов – положительно или отрицательно?

Параметры опроса

ДАННЫЕ В % ОТ ГРУПП

Вопрос не задавался тем, кто ничего не слышал о «черном списке» сайтов, – отвечали 56% респондентов

■ Положительно
 ■ Отрицательно
 ■ Ничего не знаю об этой деятельности Роскомнадзора
 ■ Затрудняюсь ответить



Источник: проект «Доминанты», опрос «ФОМнибус», 2 декабря 2012

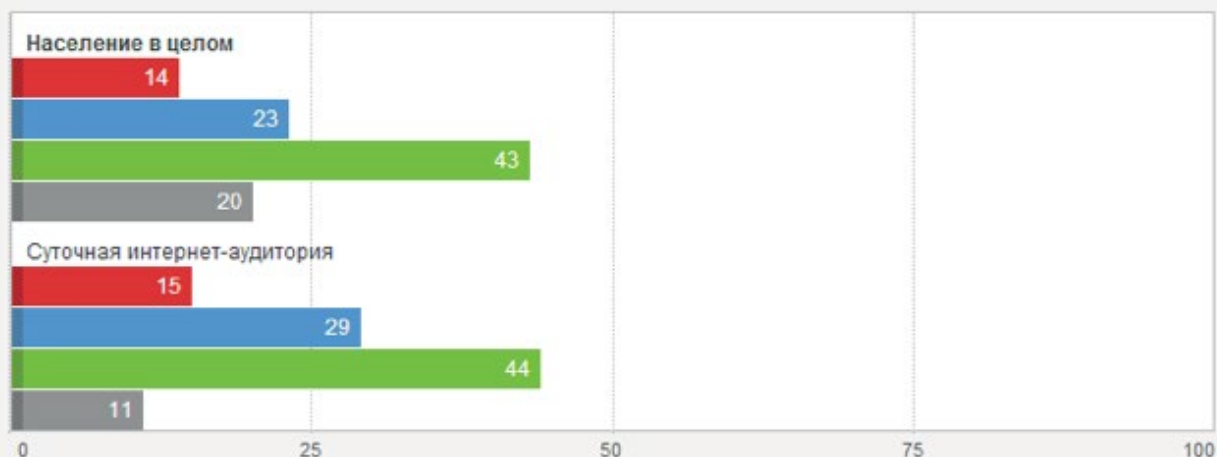
С каким из следующих утверждений вы согласны больше всего?

Параметры опроса

ДАННЫЕ В % ОТ ГРУПП

Карточка, один ответ

■ Запрет на распространение какой-либо информации в интернете недопустим – ни по решению суда, ни без него
 ■ Запрет на распространение некоторой информации в интернете допустим, но только по решению суда
 ■ Запрет на распространение некоторой информации в интернете допустим и без решения суда
 ■ Затрудняюсь ответить



Источник: проект «Доминанты», опрос «ФОМнибус», 2 декабря 2012

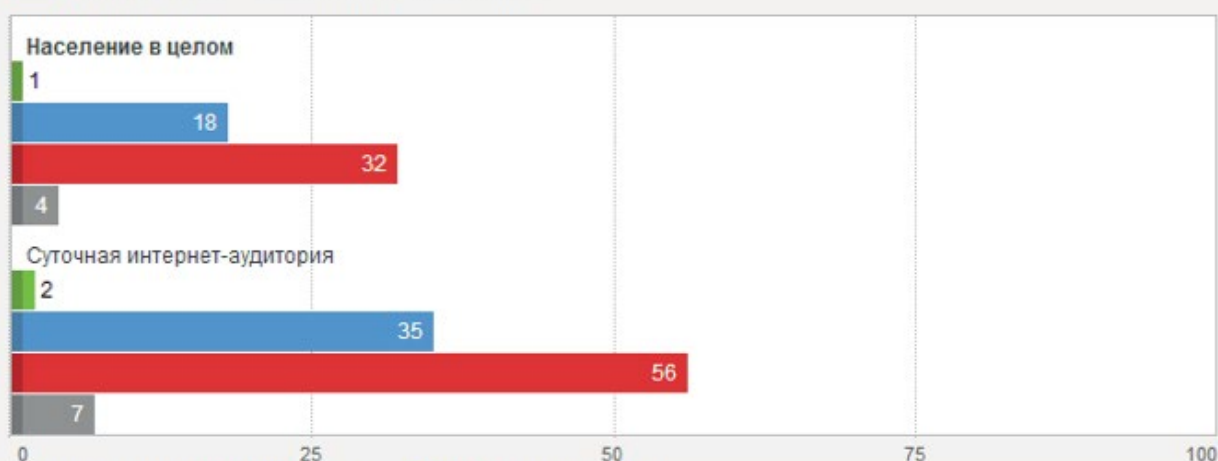
А вы встречали или не встречали в интернете материалы по запрещенным для распространения темам (детская порнография, пропаганда и распространение наркотиков, побуждение к суициду)? И если встречали, то обращались или не обращались в Роскомнадзор?

Параметры опроса

ДАННЫЕ В % ОТ ГРУПП

Вопрос задавался тем, кто пользовался интернетом в последний месяц – отвечали 54% респондентов

Встречал(-а) и обращался(-ась) в Роскомнадзор Встречал(-а), но не обращался(-ась) в Роскомнадзор
Не встречал(-а) Затрудняюсь ответить



Источник: проект «Доминанты», опрос «ФОМнибус», 2 декабря 2012

Схожие результаты демонстрирует и опрос «Левада-центра», проведенный в сентябре 2012 года³²:

Какая из точек зрения по поводу цензуры в интернете вам ближе

В интернете существует множество опасных сайтов и материалов в связи с чем необходимо ввести цензуру в Интернете	63
Опасности в Интернете переоцениваются, и в любом случае - нельзя вводить цензуру в Интернете	19
Затрудняюсь ответить	17

Как видно из этих опросов, российское общество довольно консервативно настроено по отношению к тому контенту, который размещается в Сети, и, в целом, считает желательным его регулирование со стороны государства. На этом фоне позиция представителей государственной власти выглядит даже несколько более либеральной. В этом контексте целесообразно обратиться к заявлениям Президента Владимира Путина по вопросам, связанным с границами допустимого государственного вмешательства в Сеть.

9 февраля 2012 года на заседании президиума Правительства РФ Владимир Путин следующим образом прокомментировал инициативу Лиги безопасного Интернета по созданию «реестра запрещенных сайтов»³³:

32. Левада-центр (2012), Пресс-выпуск «Россияне поддерживают цензуру в Интернете».

33. Официальный сайт Правительства Российской Федерации, <http://government.ru/docs/18054/>

«Негативные явления, которые, безусловно, есть везде, в том числе в Интернете, не должны использоваться как предлог для ограничения свободы Интернета. И для того чтобы этого не случилось, и в то же время чтобы общество могло себя оградить от этих негативных явлений, все действия в этой сфере должны быть предельно прозрачными и предприниматься и вырабатываться совместно с самим интернет-сообществом».

Год спустя, 14 февраля 2013 года, Владимир Путин на расширенной коллегии Федеральной службы безопасности РФ прокомментировал вопросы распространения экстремистского контента в Рунете³⁴:

«Прямая связь экстремистских и террористических группировок очевидна. Поэтому при нейтрализации разного рода экстремистских структур нужно действовать максимально решительно, блокировать попытки радикалов использовать для своей пропаганды возможности современных информационных технологий, ресурсы Интернета, социальных сетей».

Последнее выступление Президента на данную тему прозвучало в ходе телевизионной «прямой линии» 25 апреля 2013 года, в рамках которой прозвучал вопрос о целесообразности усиления государственного контроля над Интернетом. Владимир Путин ответил на этот вопрос следующим образом³⁵:

«Интернет – это действительно пространство свободы, там невозможно ничего ограничить и запретить. Но общество может и должно ограничить себя от чего? От педофилии, от детской порнографии, от распространения наркотиков и от обучения суицидам. Но ведь только эти три-четыре позиции, на которые мы обратили внимание и указали на них в законе, и что, там сразу всё закрывается? Нет! Закон ведь как выстроен? Если появились элементы, связанные с детской порнографией или педофилией, или обучение суициду, то провайдер должен просто сам обратить на это внимание и закрыть. Ему должны на это указать, и он должен сделать. Ничего после принятия этого закона по ограничению деятельности в интернете не произошло. Во всех развитых странах такие законы давно уже приняты. Позвольте мне сказать, и я убежден, что противники таких ограничений действуют не по соображениям свободы интернета, а прежде всего по коммерческим соображениям, связанным с получением прибыли от размещения там рекламы. Объем размещения рекламы в интернете сравнялся с ведущими федеральными каналами. Там идёт борьба, в том числе за деньги. Деньги – это хорошо, надо за них бороться, но общество обязано и должно ограничить себя от таких явлений, как педофилия, как детская порнография и обучение суицидам. Мы обязаны это сделать во имя будущего нашей страны».

Таким образом, Президент четко обозначил в своих выступлениях те категории контента, которые должны являться объектами ограничений со стороны государства:

- Материалы экстремистского содержания, направленные на разжигание национальной, религиозной и социальной розни;
- Детская порнография;
- Ресурсы, распространяющие наркотические вещества и пропагандирующие их употребление;
- Материалы, пропагандирующие совершение суицида.

34. Официальный сайт Президента Российской Федерации, <http://kremlin.ru/news/17516>

35. Официальный сайт Президента Российской Федерации, <http://www.kremlin.ru/news/17976>

Все вышеперечисленные категории, разве что кроме пропаганды суицида, которая встречается в Сети сравнительно редко, относятся к контенту, фильтрация которого допустима, по мнению международных правозащитных организаций, с точки зрения обеспечения свободы слова в Интернете. Следует отметить и тот факт, что в России практикуется весьма либеральное отношение к ресурсам, связанным с систематическим нарушением авторских прав, в частности, торрент-трекерам и крупным файлообменным сервисам.

В то же время, в настоящее время отчетливо видны проблемы с механизмами реализации законов, обеспечивающих фильтрацию вышеуказанных категорий контента. Несмотря на несовершенство закона №139-ФЗ, ситуация с реализацией закона «О противодействии экстремизму», в части блокирования доступа к экстремистским материалам, размещенным в сети, обстоит еще худшим образом. Все заблокированные ресурсы, за редким исключением, так или иначе касались тех категорий ресурсов, которые и должны подвергаться блокировке в соответствии с законом. С другой стороны, очевидны недостатки функционирующей в России системы фильтрации вредной для детей информации. Кратко, их можно охарактеризовать следующим образом:

- Недостаточный уровень экспертизы государственных органов (Роспотребнадзор и ФСКН), принимающих решения о внесении тех или иных сайтов в реестр;
- Избыточная фильтрация сторонних сайтов из-за несовершенства механизма блокировки ресурсов по IP-адресу;
- Сложность процедуры апелляции для владельцев внесенных в реестр интернет-ресурсов;
- Отсутствие отработанных и прозрачных алгоритмов взаимодействия с крупными международными сервисами.

Преодоление этих недостатков, возможно, потребует в ближайшее время корректировки механизма реализации закона №139-ФЗ. Для того чтобы фильтрация указанных в законе категорий контента осуществлялась более эффективно, но при этом не происходило избыточного блокирования, функции ведения реестра запрещенных сайтов должны быть переданы от непрофильных государственных ведомств негосударственной организации, обладающей достаточной экспертизой в подобных вопросах и поддержанной всеми значимыми участниками интернет-рынка. В то же время, появление подобной организации напрямую зависит от того, в состоянии ли на сегодняшний день российская интернет-индустрия заниматься вопросами саморегулирования хотя бы на подобном уровне.

Для решения проблемы избыточного блокирования из-за фильтрации сайтов по IP-адресу может быть использован опыт Великобритании, где система фильтрации Cleanfeed работает на основе двойной проверки, в результате чего блокировке подвергается лишь URL-адрес. Подробнее эта система описана в соответствующей главе доклада.

Гораздо хуже обстоит дело с реализацией закона «О противодействии экстремизму» в части блокирования доступа к экстремистским материалам, размещенным в Сети. В отличие от «реестра запрещенных сайтов», наполнение списка экстремистских материалов осуществляется Министерством юстиции на основе судебных решений. При этом в отличие от 139-ФЗ в законе отсутствует механизм взаимодействия между Минюстом и операторами связи, позволяющий оперативно обеспечивать блокировку внесенных в список материалов. В

результате, большая часть операторов связи вообще не блокирует материалы, внесенные в список, а остальные блокируют их лишь частично. Фактически, можно утверждать, что данный закон в настоящее время в части Интернета практически не действует.

Исходя из вышесказанного, представляется целесообразной доработка закона «О противодействии экстремизму» с целью приведения его в актуальный и функционирующий вид, на основании тех задач, которые ставятся руководством страны. Одновременно с этим целесообразно предусмотреть в законе механизмы оперативной фильтрации контента, связанного с публичными призывами к насилию в отношении конкретных лиц или социальных групп в Интернете, без нарушения нормального функционирования социальных сервисов, в рамках которых подобный контент публикуется. С учетом сложности решения подобной задачи, данная тема должна стать предметом общественной дискуссии с участием представителей интернет-отрасли.

Впрочем, оптимизация тех законов, которые в настоящее время призваны фильтровать определенные категории контента, не дает ответа на вопрос о том, а каким в принципе должно быть государственное регулирование Интернета в период, когда Сеть становится основным коммуникационным и информационным пространством, отодвигая на второй план традиционные СМИ, включая федеральное телевидение. Ответ на этот вопрос лежит исключительно в политической плоскости и во многом связан с теми тенденциями, которые можно наблюдать в российском сегменте Интернета в последние годы (подробнее о них в докладе Фонда развития гражданского общества «Рунет сегодня»). Ключевая из них – это медленный, но непрерывный процесс глобализации Рунета, предполагающий, что через несколько лет локальные сервисы уйдут на второй план, а доминирующие позиции на рынке займут глобальные игроки, не подконтрольные национальным властям.

В подавляющем большинстве стран мира уже сложилась подобная ситуация. Лишь Китаю удалось создать полноценный механизм регулирования Сети, который, с одной стороны, почти не ограничивает экономический и коммуникационный потенциал Интернета, а с другой обеспечивает доминирование локальных сервисов на национальном рынке. Впрочем, «китайский путь» не применим для России по целому ряду факторов, одним из которых является то, что введение жестких ограничений в Китае пришлось на момент первоначального роста числа интернет-пользователей в стране и потому не спровоцировало массового недовольства аудитории, привыкшей пользоваться теми или иными зарубежными сервисами. В России, где больше половины взрослого населения в настоящее время являются активными пользователями Интернета, введение аналогичных мер, как минимум, сильно затруднено.

С другой стороны, у России, в отличие от большинства других стран, существует конкурентное преимущество: благодаря специфике русского языка и большому числу квалифицированных специалистов, многие российские сервисы по-прежнему занимают ключевые позиции на интернет-рынке естественным образом, за счет своих технологических и маркетинговых решений. В частности, речь идет о поисковом сервисе «Яндекс» и социальных сетях «ВКонтакте» и «Одноклассники».

Создание комфортных условий работы в национальной юрисдикции как для лидеров рынка, так и локальных стартапов, а также внедрение различных мягких форм государственной поддержки, включая налоговые льготы, может дать дополнительный импульс развитию российских интернет-компаний, которые получают преимущества в конкуренции с международными корпорациями, по крайней мере, на российском рынке.

➤ Список литературы

1. OpenNet Initiative Access Denied: The Practice and Policy of Global Internet Filtering — Cambridge: MIT Press, 2008.
2. James Hookway. Vietnam Convicts 3 Bloggers Over Posts. The Wall Street Journal
3. Reporters Without Borders, "Internet Enemies Report 2012," 2012.
4. Derek E. Bambauer Cybersieves // Duke Law Journal. — 2009.
5. The Berkman Center for Internet and Society, "Circumvention Landscape Report Methods, Uses, and Tools," 2007.
6. OpenNet Initiative Access Controlled: The Shaping of Power, Rights, and Rule in Cyberspace — Cambridge: MIT Press, 2010.
7. OpenNet Initiative Access Contested: Security, identity, and resistance in Asian cyberspace — Cambridge: MIT Press, 2011.
8. The Berkman Center for Internet and Society, "2011 Circumvention Tool Evaluation," 2011.
9. How To Bypass Internet Censorship // [<http://www.howtobypassinternetcensorship.org/>].
10. Freedom House, "Freedom on the Net 2012," 2012.
11. Claudio Squarcella, Emile Aben Alberto Dainotti Analysis of Country-wide Internet Outages Caused by Censorship // Proceedings of the 2011 ACM SIGCOMM conference on Internet measurement conference. — 2011.
12. William H. Dutton и др., "Freedom of connection, freedom of expression: the changing legal and regulatory ecology shaping the Internet," 2011.
13. Tim Wu Jack Goldsmith Who Controls the Internet: Illusions of a Borderless World USA — s.l.: Oxford University Press, 2008.
14. A Look at Twitter in Iran (2009). Sysomos Blog.
15. Al Jazeera (2012). Facts and figures. Al Jazeera official web page.
16. Blogs and Bullets: New Media in Contentious Politics. (2010). Peaceworks.
17. Burns, A. & Eltham, B. (2009). Twitter Free Iran: an Evaluation of Twitter's Role in Public Diplomacy and Information Operations in Iran's 2009 Election Crisis. Communications Policy & Research Forum.
18. Clinton, H.R. (2010). Remarks on Internet Freedom.
19. Desouza, K.C. & Lysenko, V.V. (2012). Moldova's internet revolution: analyzing the role of technologies in various phases of the confrontation. Technological forecasting & social change: an international journal. Vol. 79.
20. Duffy, M. (2011). Smartphones in the Arab Spring. International Press Institute.
21. Dunn, A. Unplugging a Nation: State Media Strategy During Egypt's January 25 Uprising. (2011). Fletcher Forum of World Affairs.
22. Google Transparency Report (2011).
23. Franceschi-Bicchierai, L. (2013). What Happens to Social Media After a Twitter Revolution? Mashable.
24. Freedom on the Net (2012). Freedom House.

25. Gladwell, M. (2010). Small Change: Why the revolution will not be tweeted. The New Yorker.
26. Hodge, N. (2009). Inside Moldova's Twitter Revolution. The Wired.
27. Khanfar, W. (2012). Al Jazeera and the Arab Spring. Chatham House.
28. Morozov, E. (2009). More analysis of Twitter's role in Moldova. Foreign Policy.
29. Mourtada, R., & Salem, F. (2011). Civil Movements: The Impact of Facebook and Twitter. Arab Social Media Report. 1(2). Dubai: Governance and Innovation Program at the Dubai School of Government.
30. Palen, L. & Starbird, K. (2012). (How) Will the Revolution be Retweeted? ACM Conference on Computer Supported Cooperative Work.
31. Revolution in the Arab World: Tunisia, Egypt, And the Unmaking of an Era. (2011). Foreign Policy Magazine.
32. Safranek, R. (2012). The Emerging Role of Social Media in Political and Regime Change. ProQuest Discovery Guide.
33. Stack, G. (2009). 'Twitter revolution' Moldovan activist goes into hiding. The Guardian.
34. King, Gary, Jennifer Pan, and Margaret E Roberts. (2013). How Censorship in China Allows Government Criticism but Silences Collective Expression. American Political Science Review.
35. Tao Zhu, David Phipps, Adam Pridgen, Jedidiah R. Crandall, Dan S. Wallach. (2013). Tracking and Quantifying Censorship on a Chinese Microblogging Site.
36. Freedom on the Net (2011). Freedom House.
37. The Enemies of Internet (2013). Reporters without borders.
38. The Enemies of Internet (2012). Reporters without borders.
39. Abbott, Jason P. The Political Economy of the Internet in Asia and the Pacific Digital Divides, Economic Competitiveness, and Security Challenges. New York: Praeger, 2004.
40. Richard Clayton. "Anonymity and traceability in cyberspace", 2005
41. Film-makers seek injunction to block pirate site". BBC News. 28 June 2011.
42. Cameron Exploring Crackdown on Social Media After Riots", Eric Pfanner, New York Times, 11 August 2011
43. Левада-центр (2012), Пресс-выпуск «Россияне поддерживают цензуру в Интернете».
44. Фонд «Общественное мнение» (2013), «О реестре запрещенных сайтов», проект «Доминанты», опрос «ФОМнибус», 2 декабря 2012.