УДК 160.1

ЦИФРОВОЙ СУВЕРЕНИТЕТ: ПОЛИТИЧЕСКИЕ И ПРАВОВЫЕ РЕЖИМЫ ФИЛЬТРАЦИИ ДАННЫХ*

Винник Д.В.

Анализируются различные государственные режимы Интернет-цензуры и фильтрации данных исходя из различных целей: поддержки социального порядка и контроля, обеспечения политической стабильности, государственной и общественной безопасности, сохранения суверенитета и т.д . Предлагается классификация таких режимов.

Ключевые слова: интернет, фильтрация контента, цензура

Политическая цензура является достаточно старым и неплохо изученным политическим явлением. В странах с демократическими режимами политическая цензура запрещена и считается одним из самых больших зол, препятствующих реализации свободы слова и свободы совести. Однако следует признать, что даже в так называемых демократических странах она существует на уровне редакторской политики. Эта редакторская политика мотивируется либо конъюнктурой рынка, либо доминирующими в обществе и истеблишменте идеологическими установками или негласными договоренностями между властями и редакторами в рамках неформальных клубов. Так или иначе, до появления Интернета существовали достаточно эффективные инструменты ограничения свободы слова и свободы печати в различных диапазонах.

Внедрение Интернета в массы стало серьезным вызовом тем политическим режимам, для которых политическая цензура, осуществляемая через контроль над СМИ, была одним из привычных и эффективных

* Работа выполнена в рамках интеграционного проекта СО РАН № 21 «Исследование закономерностей и тенденций развития самоорганизующихся систем на примере веб-пространства и биологических сообществ» и проекта партнерских фундаментальных исследований СО РАН № 26 (2012–2014) «Новые парадигмы социального знания».

способов удержания власти. Если в доцифровую эпоху зарубежные пропагандистские радиостанции были существенным фактором в нарушении государственных монополий на публичное распространение информации, то можно себе представить, какую огромную роль играют зарубежные информационные порталы и дискуссионные площадки сегодня. В прошлом государства боролись с зарубежными радиоголосами с помощью технологий радиоэлектронной борьбы – «глушилок». Сегодня ситуация принципиально не изменилась: государства, склонные к жестким политическим цензурным режимам, продолжают использовать технические средства для фильтрации и блокировки нежелательной электронной информации, в рассматриваемом нами случае – не в радиоэфире, а в сетях передачи данных.

Существуют государства, которые выполняют такую фильтрацию в скрытом виде, основываясь на постановлениях, иногда секретных, органов исполнительной власти. Иными словами, само существование режима фильтрации может быть засекречено от народа. Например, в Туркменистане, зачисленном организацией «Репортерами без границ» в список «Врагов Интернета», фильтрация интернет-контента никак не оговорена на законодательном уровне, хотя существует в действительности. Многие китайские граждане также не подозревают о том, что поисковые запросы подвергаются глубокой фильтрации. Особенности работы «Великого китайского файерволла» до сих пор являются большой тайной и предметом детального изучения. В 2002 г. в Китае были введены правила для провайдеров, обязывающие фильтровать и удалять с сайтов призывы к свержению коммунистического режима, контент, в котором страдает репутация Китая как государства, а также контент, в котором пропагандируются сепаратизм или «культы зла». Под «культом зла» в первую очередь имеется в виду опальная секта «Фалуньгун», формально объявленная вне закона [1]. Любопытно, что власти КНР называют учение, проповедуемое этой сектой, «еретическим», хотя Китай является светским, более того, атеистическим государством. Впрочем, это не более чем результат неудачного перевода на европейские языки термина, означающего на китайском языке «ложное учение» [2].

У другого «врага Интернета» – Королевства Саудовская Аравия, государства с абсолютной монархией, необходимости имитировать демократию и свободу слова нет совсем, поэтому режим политической цензуры действует совершенно открыто. В этой стране, где официальной идеологией является религиозная идеология в форме ваххабистской версии ислама, критика ваххабизма запрещена, а течение шиизма объявлено

ересью. В государстве победившей шиитской теократии, являющемся заклятым врагом Саудовской Аравии, – Исламской Республике Иран ситуация не многим лучше. Уголовный кодекс Ирана определяет такие преступления, как пропаганда против государства, «оскорбление религии», создание «тревоги и беспокойства в общественном сознании», распространение «ложных слухов», критика чиновников. Другой ключевой частью законодательства для регулирования онлайн-контента в Иране стал Билль о киберпреступлениях (Cybercrimes Bill), ратифицированный в ноябре 2008 г. Он требует от провайдеров, чтобы «запрещенный» контент не отображался на их серверах, чтобы они немедленно информировали о нем правоохранительные органы и сохраняли этот контент в качестве доказательств.

Впрочем, не стоит впадать в иллюзию, что запрещение враждебных идеологий и фильтрация нежелательного политического контента характерны только для так называемых «азиатских деспотий». В таких «столпах западной демократии», как, в частности, Франция, официально запрещена пропаганда нацизма.

Вероятно, не будет большим преувеличением сказать, что феномен запрещения конкретных форм светской и религиозной идеологии является прямым вызовом свободе слова и свободе выражения мнений, попранием общепринятых представлений о правах человека. Однако возможно допустить, что в ряде обществ такие запреты оправданны по причине особых исторических условий (например, необходимость денацификации Германии) либо разделяемы большинством граждан или подданных. Рассмотрим подходы разных государств к регулированию публичного контента более подробно.

Международный опыт регулирования контента: цензура Интернета и фильтрация данных

Власти *Франции* декларируют поддержку свободы прессы и интернет-полемики, однако осуществляют фильтрацию детской порнографии и сайтов, продвигающих терроризм и призывы к насилию по расовому и национальному признаку. Помимо реализации политики ограничения контента этого типа французские власти уделяют особое внимание защите авторских прав в Интернете. В этом вопросе они продвинулись настолько далеко, что готовы ограничивать доступ пользователям за нарушение авторских прав. Правовым основанием для этого послужил так называемый закон Хадопи, принятый в 2009 г. и назван-

ный в честь французского агентства HADOPI, обязанностью которого является мониторинг соблюдения авторских прав в Сети. Этот закон позволяет отключать от Интернета пользователей, которых поймали на нелегальной загрузке контента, нарушающей авторские права, или на отказе защитить свои операционные системы (с помощью настроек или специального ПО) от подобных нелегальных скачиваний. В августе 2009 г. этот закон был дополнен так называемым законом Хадопи II.

В *Германии* блокировке подвергается некоторая часть интернет-контента и поисковых запросов, как правило, из соображений защиты несовершеннолетних и в рамках политики денацификации. Правовой основой цензуры является в первую очередь Базовый закон (Grundgesetz) [3], аналог Конституции, который ограничивает свободу слова только в тех случаях, когда выражается нечто «оскорбительное, несправедливое или неприличное». Германия поддерживает черный список книг, комиксов, журналов, видеокассет и музыки – так называемый Индекс. Список, первоначально предназначавшийся для защиты молодежи от порнографии, был расширен и стал включать в себя материалы, в которых идеализируется история Германии, продвигаются идеи неонацизма или отрицается Холокост. Риторика ненависти (Volksverhetzung), понимаемая в Германии как «разжигание ненависти в отношении меньшинств при определенных условиях», также строго запрещена и уголовно наказуема [4]. Закон о теле- и медиакоммуникации (Telemediengesetz, TMG) [5] принят парламентом в январе 2007 г. Параграф 8 TMG прямо говорит, что поставщики не несут ответственности за передаваемую информацию, если не они инициировали ее передачу или изменение передаваемых данных [6].

Федеративное устройство Германии позволяет осуществлять цензуру Интернета на региональном уровне. В 2002 г. Земельный правительственный округ Дюссельдорф обязал провайдеров ограничивать доступ к четырем сайтам, зарегистрированным в США и содержащим материалы праворадикальной направленности. Ограничения, которые должны были действовать в Земле Северный Рейн – Вестфалия, могли быть реализованы любым из трех способов: DNS-блокировкой, IP-блокировкой или использованием прокси-серверов [7]. Онлайн-петиции, осуждающие эти попытки заблокировать доступ, собрали более 26 тыс. подписей. Однако ни политические демонстрации, ни судебные иски против этого решения не достигли успеха: решением административного суда Дюссельдорфа в 2005 г. блокировка была одобрена.

Исламская Республика Иран вкладывает немалые средства в технологии фильтрации контента Интернета, которые являются одними из самых развитых в мире. В 2000 г. в стране была установлена система выявления и блокировки нежелательных сайтов с усиленной фильтрацией на уровне провайдера; за публикацию онлайн-материалов власти арестовали несколько десятков человек. В тот же период Иран перешел на усиленную и более сложную систему цензуры Интернета, которая координируется различными ведомствами и службами. С 2008 г. стали вводиться средства централизованной фильтрации, причем собственного производства, что уменьшило зависимость Ирана от западных технологий. Основой контент-контроля в стране является маршрутизация всего интернет-трафика через прокси-серверы. Это позволяет блокировать конкретные веб-страницы, а также ключевые слова. Так, во время президентских выборов 2009 г. блокировались политические сайты, в частности сайт www.yaarinews.ir в поддержку бывшего президента Мохаммада Хатами [8]. В 2006–2009 гг. были случаи блокировки Facebook, блокировалась загрузка с таких видеохостов, как Youtube и Flickr.

Институциональные основы для технологии фильтрации в Иране содержатся в ряде изданных в декабре 2001 г. указов Верховного Совета Культурной революции (ВСКР) о необходимости использовать систему фильтров для провайдеров. Год спустя был создан межведомственный Комитет, ответственный за определение неавторизованных сайтов. Этот комитет также принимает решение о блокировке определенных доменов. ВСКР устанавливает для этого комитета руководящие принципы и курирует деятельность его членов, среди которых есть представители Министерства связи и информационных технологий, Министерства культуры и исламской ориентации, Министерства разведки и национальной безопасности, а также Генеральный прокурор Тегерана [9].

Активную роль в установлении стандартов контента также начал играть Корпус Стражей Исламской революции (КСИР). Представители этой организации заявили о создании 10 тыс. блогов, ведущихся членами Басидж – добровольческих отрядов народного ополчения, подчиняющихся КСИР, что показывает, что информационная война в Интернете включает различные стратегии и поддерживается правительством Ирана.

Две трети пользователей глобальной сети *Саудовской Аравии* – это женщины, при том что Интернетом пользуются 38,5% подданных. Жен-

щины в этой стране, являющейся родиной ислама, в подавляющем большинстве – домохозяйки, их свобода ограничена строгими религиозными правилами. По этой причине Интернет является для них и окном в мир, в который они не могут выйти без «сопровождения» мужчины, и попыткой социализации и эмансипации.

В Королевстве Саудовская Аравия с февраля 1999 г. публичный доступ к Интернету, включая входящий и исходящий трафик, осуществляется через «бутылочное горлышко» единственного в стране правительственного контрольного центра. Следует отметить, что в этом экономически преуспевающем государстве Интернет стал доступен именно в 1999 г., т.е. не раньше момента, когда государство сумело наладить соответствующую инфраструктуру для цензуры.

Внутренний сегмент саудовского Интернета сообщается с глобальной сетью через «прокси-ферму», расположенную в Королевском технополисе (KACST). Контент-фильтр основан на программном обеспечении фирмы «Secure Computing». С октября 2006 г. Комиссия по коммуникациям и информационным технологиям (CITC) разместила на этой «ферме» структуру DNS и систему фильтрации. Кроме того, множество сайтов были заблокированы согласно двум черным спискам, составляемым и пополняемым Подразделением Интернет-сервиса – Internet Services Unit (ISU) [10] Королевского технополиса. На страничке этого подразделения открыто разъясняется, что и какими средствами блокируется. Отмечается, что 95% заблокированных сайтов являются порнографическими, остальные посвящены наркотикам, алкоголю, азартным играм, антиисламской и антигосударственной пропаганде. Пропаганда религиозной идеологии шиизма также может привести к блокировке. Королевская семья очень чувствительна к любой критике официальной ваххабистской версии ислама, и все сайты, на которых критикуется ваххабизм, заблокированы. Характерной особенностью данной системы цензуры является то, что она в принципе направлена на сотрудничество с подданными: на сайте подразделения можно написать заявление с предложением блокировать тот или иной ресурс. Для этого существует специальная форма, и, как сообщается, от обеспокоенных моралью подданных Королевства ежедневно поступают сотни заявлений.

В 2011 г. правительство Саудовской Аравии ввело новые правила и регулятивные нормы для всех онлайн-газет и блогеров, требующие наличие специальной лицензии от Министерства культуры и информации [11]. Согласно новым правилам, все авторы, пишущие в Сети, включая участников форумов и даже авторов коротких сообщений на сайте

«Twitter», должны получить эту лицензию, срок действия которой составляет три года. Следует обратить внимание на то, что Саудовская Аравия по количеству блогеров занимает одно из первых мест среди арабских стран. Подающие заявление на получение лицензии должны быть старше 20 лет и иметь законченное полное среднее образование. Им также требуется предъявить документы, которые «доказывают их хорошее поведение». Любой зафиксированный блогер без лицензии подвергается штрафу в 100 тыс. риалов (примерно 27 тыс. долларов) и/или будет забанен, возможно навсегда. Правительство Королевства объяснило это нововведение тем, что необходимо защитить общество от тлетворных влияний, и отметило, что оно, в любом случае, уже давно осуществляет политику интернет-цензуры. В то же самое время, когда вышли новые правила, правительство заблокировало страницу «WikiLeaks»на арабском языке.

Китай обладает одной из самых развитых и сложных систем интернет-фильтрации в мире. Собственно китайские сайты до появления в Интернете подлежат регистрации и проверке. Практически весь иностранный контент также проходит те или иные фильтры. Широко известен уже упоминавшийся выше китайский проект централизованной фильтрации «Золотой щит» (The Golden Shield Project; неофициальное английское название «Great Firewall of China» намекает на Великую Китайскую Стену), введенный в использование в 2003 г. Он представляет собой систему серверов на Интернет-канале между провайдерами и международными сетями, в которой ведется фильтрация по ключевым словам и адресу сайта. Иностранные поисковые машины, работающие в Китае, включая «Google», «Yahoo» и «Bing», аналогичным образом фильтруют результаты поиска. Так, в январе 2009 г. власти Китая закрыли доступ к интернет-сайту, на котором были выложены пляжные фотоснимки китайской актрисы Чжан Цзыи в компании израильского бизнесмена Авива Нево. Запрет привел лишь к тому, что эти фотографии стали самыми разыскиваемыми и скачиваемыми на Тайване, а авторитетное израильское издание «The Marker» посвятило этой истории отдельную статью [12]. 25 сентября 2009 г. под блокировку Великого китайского файерволла попало 80% IP-адресов публичных серверов анонимной сети «Tor» [13].

В Китае разрабатываются и другие способы фильтрации трафика Интернета. Одним из них был проект фильтрации на уровне пользовательского компьютера «Green Dam Youth Escort». Программное обеспечение, которое должно было устанавливаться на все компьютеры китай-

ского производства, было заявлено как защита несовершеннолетних от контента, предназначенного для взрослых. В исследовании специалистов из ONI и «Stop Badware» выяснилось, что эти программы не только неэффективны в фильтрации порнографии, но и блокируют многие политические и религиозные материалы, обычно ассоциирующиеся с проектом «Золотой щит» [14]. После публикации этих выводов Министерство промышленности и информационных технологий (МІІТ) сделало установку программ опциональной. Несмотря на очевидный провал проекта, подобный пакет под названием «Blue Dam» в сентябре 2009 г. было поручено установить всем провайдерам.

В неопубликованном отчете об исследовании, предпринятом Дэвидом Бандурски из «China Media Project», сказано, что две трети из нескольких сотен тайных внутренних отчетов, которым лидеры КПК уделяют особое внимание, приходят из отдела Интернета Управления информации Государственного совета [15].

Туркменистан получил доступ к интернету в 1997 г. на основе договора с «MCI Communications» (позднее – «MCI WorldCom»). Небольшое число независимых провайдеров были изгнаны из бизнеса в 2001 г., когда «Туркментелеком» получил монополию на услуги по передаче данных. Теперь все интернет-каналы проходят через систему серверов и центральный узел «Туркментелеком», все они тщательно контролируются службами безопасности. Есть основания полагать, что на серверах установлена технология фильтрации, настроенная на определенные ключевые слова или, например, на шифрованные сообщения, а отправители сообщений могут быть отслежены [16].

«Туркментелеком» предупреждает на своем сайте, что Интернет не является «местом для непродуманного поведения». Пользователи должны воздерживаться, например, от размещения материалов, содержащих нецензурную брань, от демонстрации «неадекватного поведения» в онлайне, от размещения информации, которая конфликтует с общепринятыми нормами поведения и законодательства, а также от загрузки порнографических материалов.

Для частных организаций, коммерческих и других, в Туркменистане сохраняется запрет на открытие интернет-кафе. В государственных интернет-кафе посетители предъявляют паспорт, а их деятельность записывается на правительственном сервере. Стоимость доступа в Интернет в Туркмении фантастически высокая, что делает его обеспечение услугой, недоступной повседневно даже для представителей высшей прослойки среднего класса.

Республика Корея (Южная Корея) является одним из самых передовых секторов ИКТ в мире, однако Интернет остается под строгим правовым и технологическим контролем центрального правительства. Цензура выражается, например, в закрытии сайтов противников воинской обязанности, сайтов гомосексуалистов, сайтов партий, симпатизирующих Северной Корее, а также в удалении записей из блогов, критикующих президента. Наиболее частым методом является блокирование по IP на уровне провайдера. Провайдер несет ответственность за то, чтобы содержащийся в его сети контент для взрослых был недоступен несовершеннолетним. Недавно правительство объявило о применении новых систем предварительной цензуры в будущем.

В 2008 г., незадолго до президентских выборов, в Южной Корее был введен в действие скандально известный среди интернет-общественности закон «Система действительных имен в интернете» (Internet Real-Name System), который требовал, чтобы все крупные интернет-порталы проверяли личность своих пользователей. Это относилось ко всем пользователям, которые выкладывали контент в открытом доступе. Например, для того чтобы добавить комментарий к новостной статье, требовались регистрация и указание идентификационного номера гражданина. Иностранцы, которые не имели такого номера, должны были отправлять по факсу копию паспорта. Хотя этот закон изначально натолкнулся на протесты общественности, большинство крупных порталов, в том числе «Daum», «Naver», «Nate» и «Yahoo Korea», осуществляли такие проверки [17]. Администрация «Youtube» отказалось подчиниться закону, предпочтя отключить функцию комментирования на корейском сайте. Закон был принят в целях борьбы с киберпреступностью, а также для того, чтобы уменьшить количество клеветы и оскорбительных комментариев в южно-корейском Интернете. В течение пяти лет южно-корейские пользователи Интернета не могли анонимно оставлять комментарии на местных сайтах. Однако сделать интернет-пространство более дружелюбным властям так и не удалось. Южно-корейские интернет-пользователи, чтобы сохранить свою анонимность, просто перешли на зарубежные веб-ресурсы, популярность же отечественных сайтов упала до предела. При этом количество оскорбительных комментариев уменьшилось лишь на 0,9%. 24 августа 2012 г. Конституционный суд Южной Кореи отменил закон о раскрытии данных, который, по мнению других государств, нарушал свободу слова в стране, гарантированную Конституцией. Согласно судебному постановлению, отмененный закон препятствовал формиро-

ванию плюрализма мнений, который является основой демократии. Главная интернет-ассоциация Южной Кореи горячо поддержала решение Конституционного суда.

Цифровая цензура, социальные доминанты и политическое устройство

Государственные режимы регулирования сети Интернет в рамках национальных юрисдикций различаются весьма существенно как по количественным, так и по различным качественным характеристикам. Считаем целесообразным выделить несколько классификаций государственных режимов по различным основаниям.

Прежде всего, в целях анализа следует разделить государства дихотомически: на государства, *заинтересованные* в развитии информационных технологий в публичной сфере, и государства, *не заинтересованные* в этом. Иными словами, существуют государства, в которых имеется открытый и публичный доступ в Интернет (таких подавляющее большинство) и государства, в которых этого доступа нет (таких явное меньшинство). К последним можно отнести некоторые государства из уже упоминавшегося списка так называемых «врагов Интернета», составленного и редактируемого организацией «Репортеры без границ». Это такие страны, как КНДР, Туркменистан, Куба, Мьянма и Йемен. Названные государства составляют *вырожденный тип*. Большинство из них (кроме Мьянмы) в той или иной степени объединяют коммунистическое прошлое, однопартийная система и наличие аппарата цензуры.

В странах из списка «врагов Интернета» количество граждан, имеющих *свободный доступ* к Интернету *на относительно постоянной основе*, не превышает 1% от общего количества населения. Однако следует отметить, что сама по себе доля граждан, имеющих подобный доступ, не является достаточным критерием для включения страны в эту категорию. Гораздо важнее не абсолютное число пользователей глобальной сети и даже не относительное по отношению к общему количеству населения (что существенно зависит от экономического развития, географии, плотности населения, образа жизни – оседлого или кочевого), а сама готовность и желание властей предоставлять гражданам или подданным доступ к Интернету и развивать эту отрасль.

Рассмотрим режимы ограничения доступа к Интернету, характерные для стран вырожденного типа. Характерно, что эти режимы могут применяться как в комплексе, как это делается в КНДР и на Кубе, так

и по отдельности, как в Мьянме, Туркменистане и прочих «врагах Интернета».

1. *Политика экономического препятствования доступа к Интернету с помощью заградительных тарифов.* В Северной Корее существуют интернет-кафе для иностранцев, которые, в принципе, могут посетить и граждане страны, однако тариф в 10 долл. США за час не только является запредельно высоким для иностранцев, но и сопоставим с месячной зарплатой большинства жителей этой страны [18].

В Туркменистане во времена правления президента С. Ниязова Интернет был фактически запрещен, хотя не известно об издании ни одной соответствующей юридической нормы. В настоящее время в стране появилось чуть более 10 интернет-кафе и существует возможность подключения к Сети по модему и выделенной линии. Стоимость модемного подключения домашнего Интернета типа ADSL с минимальной скоростью 256 кбит/с сегодня составляет 459,6 туркменских манат в месяц [19]. Если эту сумму перевести в рубли, то это будет более 4500 руб. в месяц. Учитывая, что средняя зарплата в Туркменистане ниже, чем в России, о доступности этого вида связи говорить не приходится. Подключение на скорости 34 мбит/с по выделенной линии обойдется в «космическую» сумму – 96023 манат, что равно более чем 1 млн руб. в месяц!

На Кубе средняя цена за один час доступа к Интернету составляет от 5 до 8 долл. США [20]. Если учесть, что средняя зарплата кубинца составляет 20 долл. в месяц, то становится очевидно, что попытка воспользоваться глобальной сетью для подавляющего большинства граждан просто разорительна.

2. *Политика ограничения скорости.* При этой политике, *вкупе с прочими искусственно создаваемыми техническими препятствиями,* любая попытка воспользоваться Интернетом должна восприниматься пользователями как крайне сложное предприятие. Модемные соединения постоянно рвутся, скорость резко падает почти до нулевых величин, загрузка файлов прерывается на 99%, сайты с java-приложениями не загружаются, функции поиска и навигации затруднены.

Иногда подобные меры признаются открыто, однако обосновываются в качестве мер по разумному использованию ресурсов сети. В качестве примера можно привести Йемен. В правилах и условиях провайдера «ТелеЙемен» прямо сказано следующее: «Приложения,

которые передают или получают видео или аудио в реальном масштабе времени, или другие запросы, существенно сказывающиеся на пропускной способности сети, рассматриваются в качестве неразумных и доступ к ним запрещен» [21].

3. *Политика введения разрешительно-надзорной системы, удостоверяющей право граждан на доступ к Интернету и контролирующей способ использования его ресурсов.* В рамках этой политики гражданин должен обосновать свою необходимость пользования ресурсами глобальной сети в случае желания подключить домашний Интернет; регистрировать каждый сеанс в интернет-кафе; при желании завести блог и заниматься любой формой публицистической деятельности получить на это разрешение. В рамках данной политики Интернет трактуется исключительно как ресурс для служебных целей (научно-образовательный или справочный) [22].

Подобная система существует на Кубе. В этой стране декларируется что доступ в Интернет является «фундаментальным правом» кубинцев, однако с момента появления здесь Интернета в 1996 г. Декрет 209 устанавливает процедуру аккредитации для использования его ресурсов. Фактически использование ресурсов глобальной сети было запрещено до 2000 г. С 2000 г. доступ в Интернет осуществляется при условии государственной авторизации. Для владения частным компьютером, принтером или сотовым телефоном на Кубе вплоть до 2007 г. требовалось получение официального разрешения властей. Для установки беспроводной сети Wi-Fi до сих пор необходимо такое разрешение. Вследствие слабой пропускной способности каналов связи власти страны отдают преимущество доступа к Интернету на публичной основе: на рабочих местах, в школах, НИИ и библиотеках [23].

В Мьянме подавляющее большинство пользователей пользуются Интернетом в общественных центрах доступа (ОЦД) со стоимостью от 0,3 до 0,5 долл. США за час. Операторы ОЦД обязаны регистрировать паспортные данные пользователей, более того, компьютеры пользователей настроены таким образом, что *делают скриншот каждые пять минут работы* и отсылают его в Государственную корпорацию развития информационных технологий. Кроме того, администрации интернет-кафе и ОЦД обязаны размещать компьютеры так, чтобы было видно содержимое экранов, и принять меры к тому, чтобы клиенты могли пользоваться только государственными почтовыми сервисами. Доступ к политическим сайтам категорически запрещен [24].

4. Политика сегрегации Интернета и продвижения национального интранета. В рамках этой политики создается внутренняя национальная компьютерная сеть преимущественно академического характера с ограниченным набором фиксированных функций и информационных ресурсов, жестко контролируемых государственными контент-провайдерами (НИИ, университетами, библиотеками, ведомствами). Подобная сеть призвана компенсировать недостаток доступа к глобальной сети у занятых интеллектуальным трудом граждан страны. Доступ к ней может быть либо бесплатным (служебным), либо существенно более дешевым, чем доступ к Интернету.

Такого рода политика проводится на Кубе и в КНДР. На Кубе интранет состоит из почтового сервиса, так называемой Кубинской энциклопедии и сайтов, находящихся на государственном содержании. Доступ к этому ресурсу стоит 1,5 долл. США, т.е. он как минимум в 4 раза дешевле, чем доступ к Интернету [25]. Подобная сеть, известная как «Квангмьёнг» [26], создана в КНДР. Есть сведения, что Иран и Мьянма также намерены создать аналогичные национальные сети, существующие практически автономно от глобальной сети [27].

Для всех перечисленных режимов, за исключением четвертого типа, ограничения свободного доступа граждан к Интернету, очевидно, можно рассматривать как нарушение основных гражданских прав и прав человека.

Страны, заинтересованные в свободном доступе граждан к Интернету предпочитают регулировать использование его ресурсов с помощью механизмов фильтрации контента. Важно иметь в виду, что «враги Интернета» помимо мер по ограничению доступа к Интернету вообще непременно вводят режим фильтрации контента. Однако вследствие крайне низких скоростей и небольшого количества пользователей в таких странах не возникает необходимости обширной фильтрации, поскольку почти все мультимедиаресурсы оказываются недоступными. Таким образом, государственные способы регулирования правоотношений в информационной среде можно классифицировать по критерию *характера фильтрации*.

1. *Тотальная фильтрация* (Иран, Китай). Характеризуется как *глубиной* (режим блокировки, при котором блокируются большие порции целевого контента в данной категории), так и *широтой* (режим блокировки включает фильтрацию множества категорий в данное время).

2. *Существенная фильтрация* (Саудовская Аравия, ОАЭ, Южная Корея, Йемен, Мьянма, Вьетнам, Пакистан, Оман, Узбекистан, Сирия, Тунис, Бахрейн).

3. *Постоянная выборочная фильтрация* (многие страны СНГ, в частности Беларусь, Азербайджан, Казахстан, Таджикистан, а также Индия, Сингапур, Германия, Франция, Австралия, Малайзия). Характеризуется *глубиной* или *широтой:* несколько категорий фильтруются на среднем уровне или множество категорий фильтруются слабым образом.

4. *Гибкая тактическая фильтрация* (Беларусь). Существует набор заготовленных планов обеспечения информационной безопасности, включающих шаблоны фильтрации, которые активируются исходя из конкретной военной и политической обстановки. Профили могут быстро модифицироваться и настраиваться на конкретный контент.

5. *Отсутствие фильтрации* (США, Великобритания, Дания, Финляндия, Венесуэла). Отсутствуют какие бы то ни было режимы фильтрации на государственном уровне или на уровне провайдера. Поощряется саморегуляция на уровне конечного пользователя.

Приведенный выше список категорий достаточно детально отображает ситуацию и касается практически всех видов общественной деятельности. Анализ этих категорий позволяет выделить на их основании определенные *классы (сферы)* фильтрации (табл. 1).

Таблица 1

Сферы фильтрации	**Содержание класса**	**Тип политического режима или политической культуры, форма правления**	**Страны, фильтрующие данную сферу**
Политическая	Оппозиционная политическая пропаганда, запрещенные судом или конституцией идеологические учения, права человека, свобода слова, права меньшинств	Особенно характерно для азиатских деспотий, диктатур, военных хунт и абсолютных монархий, однако, встречается и в демократических странах (государствах)	Китай, Иран, Саудовская Аравия, Германия, Франция, Россия
Религиозная	Учения сект и конфессий, враждебных или считающихся властями враждебными официальной или домини-	Характерно для теократических политических режимов и стран с официальной государственной религией. Также	Саудовская Аравия, Иран, Ирак, Китай

	рующей религии, или светской идеологии	имеет место в некоторых странах, запрещающих деструктивные культы или религиозный экстремизм согласно решениям суда или актам правительства	
Социальная	Сексуальный контент (эротика, порнография, сексуальное просвещение), азартные онлайн-игры, запрещенные наркотики, вредные для общества течения и массовые увлечения	Встречается практически во всех странах в форме фильтрации детской порнографии. Особенно характерно для стран с сильными религиозными традициями, влиятельными консервативными партиями	Германия, Франция, Южная Корея, Малайзия, Сингапур, Иран, Саудовская Аравия
Конфликтная	Контент, имеющий отношение к вооруженным конфликтам, пограничным спорам, сепаратистским движениям, незаконным вооруженным формированиям и т.п.	Характерно для федеративных республик с нерешенными сепаратистскими конфликтами, для стран, находящихся в состоянии перманентных гражданских войн и длительных пограничных конфликтов	Китай, Иран, КНДР, Куба
Авторское право и др. невещное право	Мультимедиа материалы и книги, содержащиеся в открытом доступе с нарушением авторских прав, а также ссылки на такие материалы	Характерно для западных стран с сильным лобби владельцев авторских прав	Франция
Интернет-сервисы и приложения	Почта, хостинг, поиск, перевод, телефонные сервисы VoIP, клиенты P2P, хакерские сайты	Характерно для «врагов Интернета», деспотических режимов	КНДР, Куба, Йемен, Мьянма, Франция

Также следует обратить внимание на критерий *степени прозрачности правил фильтрации* контента. Предлагаемая классификация представлена в табл. 1.

Таблица 2

Скрытый режим глубокой фильтрации. Факты фильтрации определенных категорий контента скрываются от своих граждан и не признаются перед международным сообществом с целью сохранения видимости декларируемой свободы слова)	Фильтрация глубокая, законодательная регламентация слабая	Китай, КНДР, Куба, Беларусь, Туркменистан, Узбекистан, Эфиопия, Бахрейн
Скрытый режим поверхностной фильтрации	Фильтрация поверхностная, законодательная регламентация слабая	Мьянма, Узбекистан, Судан, Йемен
Частично скрытый фильтрационный режим. Факт фильтрации признается, но скрываются его детали	Фильтрация любого уровня, законодательная регламентация средняя	Сирия, Вьетнам, Тунис, Индия
Режим полностью открытых правил фильтрации	Сильная законодательная регламентация	Саудовская Аравия, Сингапур, Израиль, Германия, Франция

Одним из важных признаков, характеризующих отношение государства к праву доступа в Интернет, является *признание* или *непризнание* этого права неотъемлемым правом человека. Таких стран совсем немного, и все они признали указанное право относительно недавно. В первую очередь это Финляндия, Греция и Эстония.

В Финляндии каждый гражданин имеет право доступа к Интернету как минимум по мегабитному каналу. В стране к глобальной сети не подключено всего 4 тыс. домов в труднодоступной местности, однако новый закон обязывает провайдеров проложить линии таким образом, чтобы каждое домохозяйство находилось на расстоянии не более 2 км от точки широкополосного доступа. Исключение сделано только для 2 тыс. домов, расположенных в крайне труднодоступной местности; Интернет этим домам не гарантирован. Правительство также уже составило план, по которому к 2015 г. граждане Финляндии по закону смогут требовать подключения к Сети со скоростью 100 Мбит/с. Пресс-секретарь Министерства телекоммуникаций и транспорта Л. Викконен отметила важ-

ность расширения доступа к глобальной сети: «Мы полагаем, что без него (Интернета – *Д.В.*) невозможно жить в современном обществе. Как в банковском обслуживании, воде или электричестве, вы нуждаетесь в Сети. Универсальный сервис – это индивидуальное право каждого гражданина» [28].

Франция только задекларировала концепцию предоставления гарантированного доступа к веб-ресурсам.

В Германии в январе 2013 г. Федеральный суд г. Карлсруэ, рассматривая иск гражданина, по техническим причинам лишенного провайдером возможности выходить в Интернет, удовлетворил этот иск. Как заявил представитель суда, «Интернет сегодня играет очень важную роль и влияет на частную жизнь каждого, позволяя принимать существенные решения. Поэтому потеря возможности использовать Интернет сравнима с потерей возможности использовать автомобиль» [29]. Кроме того, в интервью «Дойче Велле» министр юстиции ФРГ С. Летюссер-Шнаренбергер заявила: «Решение (суда. – *Д.В.*) демонстрирует то, насколько фундаментальную роль стал играть Интернет в информированной жизни. Использование Интернета начинает осознаваться как гражданское право» [30].

Можно сделать вывод, что хотя и существует некоторая зависимость между степенью демократичности политического режима в той или иной стране и свободой доступа к Интернету, подобная зависимость не носит жесткого характера. Единственное, что можно сказать достоверно, – это то, что для деспотических режимов восточного типа ограничение свободы доступа к Интернету и цензура являются органически присущими. А в странах с авторитарными режимами и военными хунтами особый акцент сделан на фильтрации политического контента и выявлении гражданских конфликтов, непосредственно угрожающих режиму. В теократиях, по понятным соображениям, развита фильтрация морального и религиозного контента, но поскольку религиозный контент в этих странах часто неотличим от политико-идеологического, политическая фильтрация также активно осуществляется. Для реальных демократических режимов характерна фильтрация социального контента, однако антифашистское законодательство некоторых стран позволяет говорить и о политической фильтрации. С формой правления и типом политического устройства права доступа к Интернету вообще не коррелирует. В республиках как президентского, так и парламентского типа с равным успехом принимаются законодательные акты по фильтрации социально вредного контента и по фильтрации ресурсов, нарушающих

права пользователей. На что следует обратить внимание, так это на то, что в странах с сильной президентской властью легче вводятся технические системы надзора за Интернетом.

Примечания

1. См.: *China* creates stern Internet, e-mail rules // USA Today. – 2002. – 18 Jan.
2. См.: Новая китайская секта «Фалуньгун». – URL: http://iriney.ru/sects/falun/001.htm. – Дата обращения 28.12.2013 г.
3. URL: https://www.btg-bestellservice.de/pdf/80201000.pdf. – Дата обращения 09.11.2013 г.
4. См.: *Strafgesetzbuch* [German Criminal Code], Section 130. – URL: http://bundesrecht.juris.de/stgb/__130.html. – Дата обращения 10.09.2013 г.
5. См.: *Telemediengesetz*. – URL: http://www.gesetze-im-internet.de/tmg/ – Дата обращения. 25.09.2013 г
6. См.: *Telemediengesetz*. – URL: http://www.gesetze-im-internet.de/tmg/8.html. – Дата обращения 10.10.2013 г..
7. См.: *Sperrungsverfьgung* [Blocking Order]. – URL: http://www.odem.org/material/verfuegung/ – Дата обращения 11.10.2013 г..
8. См.: *Cracking* Down on Digital Communication and Political Organizing in Iran. – URL: http://opennet.net/blog/2009/06/cracking-down-digital-communication-and-political-organizing-iran. – Дата обращения 10.01.2014 г..
9. См.: *A Report* on the Status of the Internet in Iran. – URL: http://www.genderit.org/upload/ad6d215b74e2a8613f0cf5416c9f3865/A_Report_on_Internet_Access_in_Iran_2_.pdf. – Дата обращения 14.02.2014 г.
10. URL: http://www.isu.net.sa/saudi-internet/contenet-filtring/filtring.htm. – Дата обращения. 20.03.2014 г.
11. URL: http://www.tgdaily.com/business-and-law-features/53403-saudi-arabia-bans-blogging-without-a-licence. – Дата обращения 16.02.2014 г.
12. URL: http://newsru.co.il/rest/03dec2009/aviva_ziyi_111.html. – Дата обращения 16.02.2014 г.
13. См.: *Tor* partially blocked in China. – URL: https://blog.torproject.org/blog/tor-partially-blocked-china. – Дата обращения 30.01.2014 г.
14. См.: *China's* Green Dam: The Implications of Government Control Encroaching on the Home PC. – URL: http://opennet.net/sites/opennet.net/files/GreenDam_bulletin.pdf. – Дата обращения.18.12.2013 г.
15. См.: *Bandurski D*. China's Guerrilla War for the Web // Far Eastern Economic Review. – 2008. – URL: http://testfeer.wsj-asia.com/essays/2008/august/chinas-guerrilla-war-for-the-web. – Дата обращения 22.09.2013 г.
16. См.: *Turkmenistan* Helsinki Foundation for Human Rights. – URL: http://www.tmhelsinki.org/en/modules/news/article.php?storyid=3310. – Дата обращения 12.01.2014 г.
17. URL: http://www.electroname.com/story/4665. – Дата обращения 14.01.2014 г.
18. См.: *Kim Hyung-eun.* Do new Internet regulations curb free speech? – URL: http://joongangdaily.joins.com/article/view.asp?aid=2893577. – Дата обращения. 16.02.2014 г.
19. URL: http://online.tm/vydelennaya-liniya. – Дата обращения. 16.02.2014 г.
20. URL: https://opennet.net/research/profiles/cuba.. – Дата обращения 22.02.2014 г..

21. См.: *Terms* and conditions for Y.Net Service. – URL: http://www.y.net.ye/support/rules.htm. – Дата обращения 09.10.2013 г.

22. См.: *Symmes P.* Che is dead. – URL: http://www.wired.com/wired/archive/6.02/cuba.html. – Дата обращения. 08.11.2013 г.

23. См.: *Going* online in Cuba: Internet under surveillance. – URL: http://www.rsf.org/IMG/pdf/rapport_gb_md_1.pdf. – Дата обращения 15.09.2013 г.

24. См.: *Burmese* Regulations for Cybercafйs Stringent as Expected. – URL: http://opennet.net/blog/2008/07/burmese-regulations-cybercafes-stringent-expected. – Дата обращения 30.09.2013 г.

25. URL: https://opennet.net/research/profiles/cuba/ – Дата обращения 12.12.2013 г.

26. См.: *Lintner B.* North Korea's IT revolution Asia Times 2007. – URL: http://www.nkeconwatch.com/category/dprk-organizations/companies/korea-computer-center-kcc/kwangmyong-computer-network/ – Дата обращения 03.01.2014 г.

27. См.: *Rhoads C., Fassihi F.* Iran Vows to Unplug Internet. – URL: http://online.wsj.com/article/SB10001424052748704889404576277391449002016.html. – Дата обращения 05.02.2014 г.

28. См.: *Интернет* гарантирован каждому жителю Финляндии. – URL: http://www.igotofin.ru/news/news81/ – Дата обращения 03.12.2013 г.

29. См.: *Internet* access is «essential» human right, rules German court. – URL: http://www.globalpost.com/dispatch/news/business/technology/130128/internet-access-essential-rules-german-court. – Дата обращения 03.12.2013 г.

30. См.: *Wünsch S.* Internet access declared a basic right in Germany // URL: http://www.dw.de/internet-access-declared-a-basic-right-in-germany/a-16553916. – Дата обращения 04.02.2014 г .

Дата поступления 15.04.2014

Институт философии и права
СО РАН, г. Новосибирск
dvin@ngs.ru

Vinnik, D.V. **Digital sovereignty: political and legal regimes of data filtration**

The paper analyzes various state regimes used for censoring Internet and filtrating data in agreement with diverse purposes, viz. to maintain social order and control, to ensure political stability, state and social security, to keep up sovereignty, etc. The author suggests a classification of such regimes.

Keywords: Internet, content filtration, censor