DOI: 10.17976/jpps/2022.02.02

ФОРМИРОВАНИЕ ЦИФРОВЫХ ГРАНИЦ И ИНФОРМАЦИОННАЯ ГЛОБАЛИЗАЦИЯ: АНАЛИЗ С ПОЗИЦИЙ КРИТИЧЕСКОЙ ГЕОГРАФИИ

Е.С. Зиновьева

ЗИНОВЬЕВА Елена Сергеевна, доктор политических наук, профессор кафедры мировых политических процессов, МГИМО МИД России; профессор департамента международных отношений, Национальный исследовательский университет "Высшая школа экономики", Москва, email: elena.zinovjeva@gmail.com

Зиновьева Е.С. 2022. Формирование цифровых границ и информационная глобализация: анализ с позиций критической географии. *Полис. Политические исследования*. № 2. С. 8-21. https://doi.org/10.17976/2022.02.02

Статья опубликована в рамках проекта "Посткризисное мироустройство: вызовы и технологии, конкуренция и сотрудничество" по гранту № 2020-1902-01-372.

Статья поступила в редакцию: 05.04.2021. Принята к публикации: 11.12.2021

Аннотация. В последние годы заметно усилилось внимание ученых к фрагментации интернета, появились специализированные термины "балканизация интернета" и "разделенный интернет", описывающие новое состояние деглобализированного информационного пространства. Как правило, этот процесс связывают с появлением цифровых границ в интернете. Объем данных, пересекающих границы государств, продолжает возрастать. Таким образом, информационная глобализация на уровне данных сосуществует с усилением цифровых границ и практикой укрепления цифрового суверенитета. Критическая география позволяет изучить цифровые границы не только как материальные объекты, но и как социальные конструкты, дискурсивные практики, которые отражают характер властных отношений на международной арене и являются источником власти для тех, кто их создает и контролирует. Согласно критической географии, цифровые границы в силу своей социальной природы не могут быть непроницаемыми, их возведение не означает конца информационной глобализации. В статье выделено два уровня цифровых границ – дискурсивный и онтологический. На дискурсивном уровне они отражают секьюритизацию информационной сферы и трансформацию баланса сил, формирование многополярности, а на онтологическом призваны прежде всего защищать от угроз информационной безопасности. При этом государства заинтересованы в выгодах, предоставляемых глобальным интернетом. Его связность обеспечивает бизнес, который выступает субъектом формирования новых глобальных цифровых пространств, содействуя глобализации рынка в целях увеличения прибыли.

Ключевые слова: интернет, глобализация, критическая география, международная информационная безопасность, цифровой суверенитет, цифровые границы, цифровая география.

ВВЕДЕНИЕ

В 1990-х годах, на начальном этапе развития интернета, в научной литературе преобладал подход, согласно которому интернет считался так называемой ничьей землей (лат. *terra nullis* – пространство, в котором социальные отношения и нормы не опираются на исторический опыт и должны быть выработаны заново). При таком подходе нормы международной политики не действовали в киберпространстве, в нем не было государственных границ и к нему не

применялась категория государственного суверенитета. Информационное пространство рассматривалось как один из двигателей глобализации, доминирующей темы в академической литературе того периода, широко использовался также термин "информационная глобализация", призванный подчеркнуть растущий объем трансграничных потоков информации в интернете.

В настоящее время подобный подход оспаривается представителями различных областей знания – политической науки, международных исследований и др. В научной литературе, российской и зарубежной, публикуется значительное число работ, посвященных фрагментации интернета и усиливающейся роли государств в информационной сфере [Drezner 2004; Кучерявый 2015], а также ее нарастающей конфликтности [Diebert, Rohozinski 2010]. При этом научных материалов, посвященных глобализации интернета, становится существенно меньше.

И хотя проблематика фрагментации интернета находит свое отражение не только в значительном количестве научных публикаций, но и в докладах международных организаций (например, в докладе ВЭФ "Фрагментация интернета: обзор"[1]), она вступает в противоречие со статистическими данными, согласно которым на протяжении последних лет объем трансгранично передаваемых данных возрастает[2].

Настоящая статья ставит своей задачей ответить на исследовательский вопрос: почему наряду с усилением дискурса о цифровых границах и фрагментации интернета не сокращается объем трансгранично передаваемых данных и правомерно ли в этих условиях говорить о конце информационной глобализации?

В качестве теоретической основы исследования выбраны социальный конструктивизм, исследующий взаимосвязь материальных и идеальных факторов мировой политики, и подход критической географии, который рассматривает цифровые границы как социальные конструкты, отражающие властные отношения на международной арене.

Использование выбранной методологии позволило сформулировать следующую гипотезу. Цифровые границы, разделяющие глобальное информационное пространство, представляют собой социальные конструкты, в которых можно выделить дискурсивный (являющийся отражением властных отношений и дискурса на международной арене) и онтологический уровни (под онтологическим уровнем понимается инфраструктура, программное обеспечение и цифровой контент). Эти два уровня не совпадают, но находятся в сложной взаимозависимости. На дискурсивном уровне субъектами формирования цифровых границ выступают государства, заинтересованные в укреплении своего суверенитета и защите от угроз информационной безопасности. В силу секьюритизации информационного пространства дискурс о цифровых границах прежде всего ориентирован на обеспечение безопасности, поэтому в нем доминируют государства, однако это не означает конец информационной глобализации.

Государства, как и глобальные интернет-компании[3], заинтересованы в экономическом росте и получении экономической выгоды от связного глобального

[1] Internet fragmentation: an overview. world economic forum. 2016. https://www.weforum.org/reports/internet-fragmentation-an-overview (accessed 12.01.2022).

[2] UNCTAD digital economy report 2021. https://unctad.org/webflyer/digital-economy-report-2021 (accessed 12.01.2022).

[3] Под интернет-компаниями понимаются компании, получающие большую часть прибыли в результате работы в интернете (см., например, Forbes назвал 30 самых дорогих интернет-компаний в России в 2021 году. *VC.ru*. https://vc.ru/finance/212746-forbes-nazval-30-samyh-dorogih-internet-kompaniy-v-rossii-

интернета. Крупные интернет-компании стремятся к глобализации рынков сбыта и росту прибыли, в результате их деятельности наблюдается рост объема данных, пересекающих границы государств. Дискурсивный и онтологический уровни тесно связаны: на первом принимаются решения и формируются институты, которые управляют последующим развитием технологий на втором.

Согласно критической географии, границы – это прежде всего социальные объекты, а территориализация интернета не означает формирование "непроницаемых" границ, т.е. не уничтожает его как связную глобальную систему. Укрепление цифровых границ не приводит к деглобализации, но говорит о растущем влиянии на информационное пространство международной политики, характеризующейся возрастающей конфликтностью.

Статья состоит из пяти частей. В первой представлен исторический обзор исследовательской литературы о глобализации и фрагментации интернета. Во второй части описывается теоретико-методологическая база исследования – критическая география и социальный конструктивизм. В третьей части дается анализ процессов глобализации интернета и информационной глобализации в 1990-е – начале 2000-х годов с позиций критической географии, показывается, что дискурс об информационной глобализации и об интернете как о "глобальном общественном благе" был призван продвигать интересы США, закрепляя их лидирующее положение в данной области. В четвертой части рассмотрена роль государств в дискурсивном формировании цифровых границ на современном этапе, что отражает секьюритизацию информационного пространства и изменение баланса сил в глобальной информационной сфере. Последняя часть статьи посвящена изучению роли негосударственных акторов в территориализации интернета и создании новых цифровых пространств.

ЭВОЛЮЦИЯ АКАДЕМИЧЕСКОГО ДИСКУРСА О ГЛОБАЛИЗАЦИИ ИНТЕРНЕТА

На начальных этапах развития интернета в 1990-х – начале 2000-х годов российские и зарубежные ученые публиковали работы, посвященные особенностям его влияния на мировую политику [Mueller 2010], причем интернет рассматривался как основной двигатель глобализации [Nye, Keohane 2000], способствовал возрастающей роли неправительственных акторов, усилению взаимозависимости и размыванию государственного суверенитета [Михеев 2009]. Большинство исследователей противопоставляли сетевую природу интернета и территориальную природу политической географии [Mueller 2010].

Подобный подход получил название "цифровая исключительность" – пространство интернета рассматривалось как самостоятельная область, на которую не распространяются законы реальной политики и географии, но которая оказывает существенное влияние на международную политику, усиливая глобализацию [Rosenau, Singh 2002].

Начиная с середины 2000-х годов акценты начали смещаться: подобная точка зрения рассматривается как утопичная трактовка не только самой природы интернета, но и характера его взаимоотношений с мировой политикой [Herrera 2008]. Исследователи полагают, что международная политика, в том числе "откат глобализации", сильно влияет на природу информационного

v-2021-godu). Наиболее влиятельные из них – это компании, владеющие крупными интернет-площадками, в том числе социальными сетевыми сервисами. В результате их деятельности, согласно докладу ЮНКТАД за 2019 г., наметилась тенденция к платформизации мировой экономики, см. UNCTAD Digital Economy Report 2021. https://unctad.org/webflyer/digital-economy-report-2021 (accessed 12.01.2022).

пространства [Drezner 2004], его нарастающую конфликтность, укрепление государственных границ и цифрового суверенитета в условиях растущего количества цифровых угроз безопасности, набирающей силу тенденции фрагментации интернета [Mueller 2020][4].

Американский исследователь М. Мюллер доказывает, что государства стремятся обозначить границы своей юрисдикции в информационном пространстве, что является двигателем информационной фрагментации мира [ibidem]. Как отмечает швейцарский ученый М. Данн-Кавелти, подобная политика обусловлена секьюритизацией данной сферы, так как по мере увеличения количества цифровых угроз правительства рассматривают ИТ через призму безопасности [Dunn Cavelty 2013].

Российский политолог М.М. Кучерявый пишет о необходимости укрепления государственного суверенитета в информационной сфере в условиях нарастающего количества угроз международной информационной безопасности [Кучерявый 2015]. А.А. Стрельцов исследует проблематику определения суверенитета и юрисдикции государства в информационной сфере, отмечая, что по мере роста угроз информационной безопасности разрешение соответствующих правовых коллизий становится все более насущной задачей [Стрельцов 2017]. О популярности подобной концептуализации в российской научной литературе говорит появление термина "информационная геополитика" [Быков 2008], который показывает растущее влияние государств в глобальном информационном пространстве [Buchanan 2020].

Смену исследовательской парадигмы подтверждает и растущее количество статей в публицистических изданиях. В 2016 г. журнал *Economist* предложил термин "балканизация интернета", в 2019 г. появился термин "сплинтернет", оба они отражают снижающуюся связность национальных сегментов интернета. Специальный представитель президента РФ по вопросам цифрового и технологического развития Д.Н. Песков также отмечает тенденцию к "островизации" интернета вследствие укрепления суверенитета государств и возведения границ в цифровом пространстве[5].

Большая часть исследователей в области фрагментации интернета в качестве субъектов фрагментации выделяет государства, которые стремятся обеспечить свой суверенитет, укрепляя "цифровые границы" [Lambach 2020: 487], что может быть обозначено как территориализация интернета, по аналогии с колонизацией и территориализацией государствами других новых пространств, например Арктики или Нового Света [Herrera 2008]. Приобретает популярность метафора "цифровой фронтир" [Плотичкина, Довбыш 2017].

КРИТИЧЕСКАЯ ГЕОГРАФИЯ И СОЦИАЛЬНЫЙ КОНСТРУКТИВИЗМ О ЦИФРОВЫХ ГРАНИЦАХ

В качестве теоретической основы исследования была использована критическая география. В российской научной литературе известность получило ее частное направление – подход критической геополитики. Как отмечает

[4] См. например, Capri A. Techno-Nationalism: What Is It And How Will It Change Global Commerce? *Forbes*. 20.12.2019. https://www.forbes.com/sites/alexcapri/2019/12/20/techno-nationalism-what-is-it-and-how-will-it-change-global-commerce/?sh=77705a7c710f (accessed 12.01.2022).

[5] Безопасность в интернете достигается не запретами. *Россия сегодня*. 05.06.2019. https://1prime.ru/telecommunications_and_technologies/20190605/830039744.html (accessed 12.01.2022).

директор Центра пространственных исследований МГИМО МИД России И.Ю. Окунев, критическая геополитика отходит от традиционного понимания концептов "политического" и "географического", выйдя за рамки исследовательских задач, принимающих во внимание лишь физические границы. К сфере ее интересов относятся социальные науки, вопросы глобализации, идентификации и суверенитета [Окунев 2014].

Согласно подходу критической географии, границы и территории – это продукты властных отношений, формируемые дискурсивно. Границы и территории – не просто материальные объекты, они обретают форму и смысл только в результате социальной активности групп или отдельных индивидов. Таким образом, "территории – это всегда манифестации властных отношений, и они нуждаются в публичных действиях для их создания и поддержания" [Paasi 2003: 111].

В работах западных ученых пространственный анализ интернета получил популярность достаточно давно, но критическая география до недавнего времени в нем не использовалась. Один из наиболее авторитетных центров в данной сфере, Оксфордский институт исследований интернета, составляет "карты интернета", отражающие популярность социальных сетей в мире, маршруты трансгранично и трансконтинентально передаваемых данных, общее число доменов или количество пользователей по странам. Однако сама схема построения подобных "карт интернета" была призвана подчеркнуть различия между физическим и киберпространством и неприменимость к нему простых географических аналогий.

Одним из первых подход критической географии использовал немецкий исследователь Д. Ламбах, который отметил, что субъекты территориализации не только обозначают границы и пределы своей юрисдикции, но и создают новые территории в глобальном киберпространстве. При этом в роли субъектов территориализации интернета Ламбах выделяет государства, крупные интернет-компании и сообщества пользователей интернета. Вслед за Ламбахом в настоящей статье в качестве субъектов формирования интернет-границ выделяются сообщества, государства, крупные интернет-компании и сообщества интернет-пользователей.

В критической географии в формировании территории и границ важная роль отводится дискурсу, при этом дискурс всегда является отражением властных отношений. Отталкиваясь от работ в области критической географии, в настоящем исследовании выделено две главных дискурсивных практики в области формирования и поддержания цифровых границ:

1) публичное обозначение границ (например, заявления официальных лиц государства о государственных границах в интернете);

2) регулярная публичная демонстрация власти и контроля границ (принятие законодательных инициатив, направленных на обозначение цифровых границ на национальном уровне, закрепление соответствующих формулировок в итоговых документах международных организаций, ограничение доступа иностранных IT-компаний).

Особенностью киберпространства является рукотворный характер, что отличает его от предшествующих пространств, таких как земля и воздушное пространство. Поэтому кибертерритории нуждаются в "овеществлении", создании на онтологическом уровне и лишь потом происходит делимитация границ и определение властных отношений в цифровом пространстве. При

этом онтологический и дискурсивный уровни цифровых границ тесно связаны между собой, но не совпадают.

На онтологическом уровне глобальное информационное пространство интернета состоит из инфраструктуры, программного обеспечения и контента, информации и данных [Eriksson, Giacomello 2009]. Такой подход позволяет сформулировать онтологическую составляющую цифровых границ:

1) контроль доступа (контроль над инфраструктурой, посредством которой осуществляется доступ в интернет);

2) контроль функциональности (контроль над программным обеспечением, при помощи которого и реализуется основной функционал информационных ресурсов сети);

3) контроль данных (также предполагает контроль поведения пользователей интернета, создающих данные и информацию, в том числе в контексте информационной безопасности, предотвращение незаконной деятельности на уровне отдельного государства и международного сообщества) [ibid.: 206-207].

Ввиду взаимозависимости дискурса и онтологии цифровых границ многие решения одновременно влияют на оба уровня. Например, законодательные инициативы в области локализации персональных данных граждан, с одной стороны, имеют дискурсивное значение, поскольку являются демонстрацией контроля государства над своими цифровыми границами, а также изменяют сетевую онтологию, так как предполагают создание инфраструктуры и разработку программных решений, позволяющих хранить персональные данные внутри определенной юрисдикции.

Согласно конструктивистскому подходу, интернет тесно вписан в политику, в том числе международную, так как характеристики технологии являются предметом политических противоречий, а институты, управляющие использованием и развитием технологии, отражают баланс сил в обществе и международной политике [Herrera 2012]. Чем более развита технология, тем большее влияние на нее оказывают международно-политические процессы, что мы и наблюдаем в отношении интернет-пространства.

Информационная глобализация интернета на ранних этапах его развития

В 1990-е годы, когда интернет только набирал популярность в глобальном масштабе, политические деятели США, стран ЕС и представители международных организаций заявляли о нем как о пространстве вне суверенитета[6]. Кроме того, было популярно представление об интернете как о всеобщем благе [Introna, Nissenbaum 1999], к которому все люди имеют доступ вне зависимости от национальной или территориальной принадлежности.

Однако и в этом случае мы можем говорить о расхождении дискурсивного и онтологического уровней цифрового пространства. С момента создания сети в силу исторических причин США обладали уникальными возможностями трансграничного контроля инфраструктуры и функциональных систем интернета, которые обеспечивали его связность в глобальном масштабе – а именно пространства имен и адресов интернета. В силу того, что

[6] См., например, International Strategy for cyberspace. prosperity, security and openness in a networked world. *US White House*. 2011. https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf (accessed 12.01.2022).

распределением доменов и IP-адресов[7] в интернете изначально занималась ICANN, действовавшая по контракту с правительством США (сейчас этим занимается ее дочерняя структура – PTI), государства (за исключением США) не имели возможности осуществлять контроль в данной области в полной мере. Подобная ситуация в области международного управления техническими ресурсами интернета сохраняется до сих пор.

Даже на ранних этапах развития сети контроль США над интернетом все же не был абсолютным. Аппаратное обеспечение и серверы, на которых хранится информация, линии передачи данных, посредством которых она передается, всегда находились в границах юрисдикции отдельных государств и имели географическую принадлежность, это было характерно для всех этапов его исторического развития. В рамках этой же логики программное обеспечение, установленное на этих устройствах, также подпадает под юрисдикцию той страны, на чьей территории они размещены. Таким образом, на ранних этапах развития интернета государства имели возможность осуществлять ограниченный контроль на уровне инфраструктуры и программного обеспечения (однако не абсолютный, в силу того что США сохраняли контроль над пространством имен и адресов). Кроме того, на тот период программные средства не всегда позволяли определить территориальную принадлежность данных и пользователей и контролировать данные и информацию, пересекающие границы.

Критическая география рассматривает глобализацию как экстратерриториальный формат глобального управления, который пришел на смену традиционным форматам территориальной организации социальных и политических отношений и отражал интересы наиболее влиятельных стран, прежде всего США и их союзников [Ruggie 1993]. Иными словами, глобализация и дискурс о "конце географии" легитимировали стремление стран Запада и крупных компаний контролировать процессы, выходящие за пределы их юрисдикции. Схожие выводы настоящее направление позволяет сделать и относительно информационной глобализации. Формат ICANN представлял собой экстратерриториальную форму управления интернетом, попытку расширить границы юрисдикции США на уровень международной системы интернета в целом. Поддержка США дискурса об экстратерриториальной природе интернета, который концептуализировался как всеобщее благо, с этой позиции представляет собой попытку перестроить властные отношения в новом информационном пространстве, закрепив свои лидирующие позиции и ограничив суверенитет других стран.

Вместе с тем можно утверждать, что дискурс об информационной глобализации имел определенное влияние на тенденции развития сети – количество пользователей во всем мире и объем передаваемых данных в интернете возрастали. В 2000 г. в США почти половина граждан имела доступ к интернету, но в Азии, Африке и Тихоокеанском регионе у более чем 90% доступа не было. Уже к 2005 г. число пользователей интернета в других частях света возросло, в основном за счет Азии и особенно Китая[8]. Рост числа пользователей, став-

[7] IP-адрес – уникальный адрес, которым должно обладать каждое устройство, подключаемое к интернету. Текущая версия базового интернет-протокола IPv4 предполагает наличие ограниченного количества IP-адресов, что делает их потенциально оспариваемым ресурсом. Современные технологические решения в большинстве случаев позволяют обойти данное ограничение.

[8] На основании Internet World Stats. http://www.Internetworldstats.com (accessed 12.01.2022).

ший следствием информационной глобализации, оказался важным фактором, обусловившим растущий интерес к укреплению государственного влияния в информационном пространстве и формированию цифровых границ.

СТРЕМЛЕНИЕ ГОСУДАРСТВ К ЦИФРОВОМУ СУВЕРЕНИТЕТУ И ФОРМИРОВАНИЕ ИНФОРМАЦИОННЫХ ГРАНИЦ НА СОВРЕМЕННОМ ЭТАПЕ

По мере того, как увеличивалось количество пользователей интернета, возрастало и стремление большинства стран мира контролировать данную технологию. В середине 2000-х годов появились социальные сети, которые стали важнейшим фактором влияния интернета на политическую сферу, а также актуализировались угрозы информационной безопасности, что придало дополнительный импульс стремлению государств укрепить контроль в информационном пространстве.

На этот период пришлись первые шаги в области формирования международно-политического дискурса о границах в интернете. В 2003 и 2005 гг. по инициативе России в документы Всемирной встречи на высшем уровне по вопросам информационного общества, которая прошла под эгидой ООН, был внесен пункт о том, что на национальный сегмент интернета распространяется суверенитет государств[9]. Позднее под влиянием протестов Арабской весны в 2011 г., в ходе которых информационные технологии сыграли роль катализаторов [Зиновьева 2013; Farrell 2012], вопрос о цифровом суверенитете стал активнее обсуждаться на международном уровне, в частности в рамках ШОС и ОДКБ [Зиновьева 2013][10]. В докладах Группы правительственных экспертов ООН от 2013 и 2015 гг. по международной информационной безопасности было зафиксировано признание суверенитета государств над национальным сегментом интернета[11]. С позиций критической географии это можно рассматривать как дискурсивное закрепление границ государств в интернете. Одновременно с этим принимались инициативы по контролю границ, которые не только имели политическое измерение, но и воплощались в технологические решения, влияющие на онтологию сети.

КНР первой предложила новую практику определения государственного суверенитета не только на уровне инфраструктуры и программного обеспечения, но и на уровне контента – информационного содержимого всемирной сети: “Великий китайский файрвол” был запущен в 2003 г. при участии компании IBM [Бухарин 2016: 78]. Подобная практика получила широкое распространение. Россия со второй половины 2010-х годов укрепляет собственный информационный суверенитет, причем наибольший прогресс достигнут в таких областях, как российские поисковые системы, социальные сети, а также навигационная система [там же: 76]. Как отмечают исследователи, в настоящее время во всех государствах мира принимаются инициативы, направленные на укрепление су-

[9] См. WSIS-03/GENEVA/DOC/5-R. Всемирная встреча на высшем уровне по вопросам информационного общества. План действий. 12.12.2003. http://www.itu.int/dms_pub/itu-s/md/03/wsis/doc/S03-WSIS-DOC-0005!!PDF-R.pdf (accessed 12.01.2022).

[10] Заявление Совета глав государств – членов Шанхайской организации сотрудничества о сотрудничестве в области обеспечения международной информационной безопасности. 10.11.2020. https://www.fmprc.gov.cn/rus/zxxx/t1831178.shtml (accessed 12.01.2022).

[11] A/70/174 ‘Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security’. 22.07.2015. https://daccess-ods.un.org/TMP/6949319.83947754.html (accessed 12.01.2022).

верenитета и цифровых границ[12], хотя трактовки и используемая терминология и различаются, смысловое ядро дискурса сводится к обозначению легитимных властных притязаний государств на контроль цифровых границ.

Во второй половине 2010-х годов по мере развития технологий сложился целый ряд решений и политических практик, направленных на контроль цифровых границ (инфраструктуры, программного обеспечения и данных).

1) Отключение / ограничение доступа к интернету внутри государственных границ. Хотя это, как правило, крайнее средство, оно весьма эффективно демонстрирует полноту власти государства, как показал опыт Эстонии в 2007 г., Египта в ходе Арабской весны в 2011 г.[13] и Ирана в 2019 г., Казахстана 2022 г.[14]

2) Геолокационное программное обеспечение, которое устанавливает связи информационного пространства и реального мира, разделенного государственными границами, для пользователей и устройств, подключенных к интернету.

3) Законодательно закрепленное регулирование трансграничной передачи данных за счет программных средств (только в наименее развитых странах отсутствует регулирование данной области [Casalini, Gonzales 2019]).

4) Локализация персональных данных граждан (определенные виды данных граждан собираются, хранятся и обрабатываются только на территории страны, причем зачастую список компаний, управляющих данными, также формируется на основании того, подпадают ли они под юрисдикцию государства). Согласно данным ОЭСР за 2020 г., в 40% государствах – членах ОЭСР действует соответствующее регулирование[15].

Эти технологические решения дают возможность государствам контролировать цифровые границы даже в условиях сохранения монополии американской компании PTI на управление пространством имен и адресов в интернете, существенно укрепляя цифровой суверенитет. При этом преследуется цель обеспечения безопасности и государственного суверенитета, поэтому, как правило, это не препятствует трансграничным потокам информации.

Таким образом, национальные сегменты информационного пространства аналогичны территориальным юрисдикциям в киберпространстве, которые удобны и понятны для лиц, принимающих решения в области государственной политики. Основной причиной возведения цифровых границ является секьюритизация информационного пространства, когда по мере роста угроз информационной безопасности актуализируются вопросы обеспечения безопасности, в принятии решений относительно которых государства играют

---

[12] В России вступил в силу "Закон о суверенном Рунете". РБК. 01.11.2019. https://www.rbc.ru/technology_and_media/01/11/2019/5dbb1cb49a7947777b009bd6; Global Initiative on Data Security. *Ministry of foreign affairs of the People's Republic of China*. 09.08.2020. https://www.fmprc.gov.cn/mfa_eng/zxxx_662805/t1812951.shtml; EU Data Strategy. *European Commission*. 2020. https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/european-data-strategy_en (accessed 12.01.2022).

[13] Ritchell M. Egypt cuts off most Internet and cell service. *NY Times*. 28.01.2011. https://www.nytimes.com/2011/01/29/technology/internet/29cutoff.html (accessed 12.01.2022).

[14] Baraniuk C. Iran's Internet blackout reaches four-day mark. *BBC News*. 20.11.2019. https://www.bbc.com/news/technology-50490898 (accessed 12.01.2022).

[15] OECD Digital Economy Indicators. 2020. https://www.oecd-ilibrary.org/sites/bb167041-en/index.html?itemId=/content/publication/bb167041-en&_csp_=509e10cb8ea8559b6f9cc53015e8814d&itemIGO=oecd&itemContentType=book#section-1 (accessed 12.01.2022).

главную роль. При этом государства заинтересованы в экономических выгодах, предоставляемых глобальным связным интернетом[16].

Критическая география позволяет рассматривать границы как отражения властных отношений на международной арене. Поэтому формирование дискурса о цифровых границах, который пришел на смену дискурсу об информационной глобализации и об интернете как о глобальном общественном благе, представляет собой перестройку пространственной организации информационной сферы на основании цифрового суверенитета путем создания новых дискурсивных и онтологических практик в условиях изменившихся властных отношений – снижения влияния США в международной политике и информационной сфере, формирования многополярности, растущего количества угроз международной информационной безопасности.

РОЛЬ НЕГОСУДАРСТВЕННЫХ АКТОРОВ В ГЛОБАЛИЗАЦИИ ИНТЕРНЕТА

Глобальное информационное пространство – это яркий пример нового с точки зрения территориальности пространства, в рамках которого государственные границы и границы государственной власти проходят стадии возникновения, изменения и борьбы. В отличие от других пространств, территориализация интернета предполагает первоначально "овеществление", создание территории, так как кибертерритория не является данностью. В этом процессе ведущую роль играют негосударственные акторы – представители бизнеса и интернет-сообщества. Как отмечает М. Финнемор, 95% всей инфраструктуры интернета находится в частной собственности [Финнемор 2018]. Именно в результате деятельности бизнеса формируются новые форматы использования интернета, новые площадки для взаимодействия пользователей, причем следует отметить высокий динамизм бизнес-активности на этом направлении.

Важную роль играют и сами пользователи, которые либо поддерживают существующие цифровые площадки, либо создают новые. Показателен пример массированного перехода пользователей социальной сети *Twitter* на площадку *Telegram* после блокировки аккаунта действовавшего на тот момент президента США Д. Трампа в *Twitter* – таким образом, пространство для цифровой дипломатии, центром которого первоначально был *Twitter*[17], существенно расширилось. Цели, преследуемые сообществами пользователей, как правило, лежат в ценностной плоскости – чаще всего это свобода доступа к информации (в качестве примера можно привести движение "Пиратский интернационал", которое ставит задачу свободного доступа ко всей информации, защищенной авторским правом). Ценности носят трансграничный характер, поэтому на онтологическом уровне новые цифровые территории, создаваемые пользователями, необязательно совпадают с государственными границами. Однако сообщества пользователей все же обладают меньшим влиянием по сравнению с бизнес-структурами, в силу того что у них нет возможности влияния ни на инфраструктурном, ни на функциональном уровнях; их главный ресурс – это данные, которые в результате их деятельности агрегируют цифровые плат-

[16] См., например, Доктрина информационной безопасности Российской Федерации. https://rg.ru/2016/12/06/doktrina-infobezobasnost-site-dok.html; Global Initiative on Data Security. *Ministry of Foreign Affairs of the Peoples Republic of China*. 2020. https://www.fmprc.gov.cn/mfa_eng/zxxx_662805/t1812951.shtml; EU Data Strategy. *European Commission*. 2020. https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/european-data-strategy_en (accessed 12.01.2022).

[17] См., Twiplomacy. www.twiplomacy.com (accessed 12.01.2022).

формы. Пользователи вынуждены выбирать между интернет-площадками, созданными бизнес-структурами.

В свою очередь крупные компании, владеющие цифровыми платформами, имеют возможности создания цифровых границ информационных экосистем на всех уровнях – контроль инфраструктуры, программного обеспечения и контента, а также возможность управлять предпочтениями и поведением пользователей информационных услуг. Тем не менее в политической области у них нет влияния, сопоставимого с государствами, и поэтому они практически не принимают участия в дискурсе о границах в интернете. Доминирующее положение государств в дискурсе объясняется растущим количеством угроз информационной безопасности, в силу того, государства обладают монополией на легитимное насилие и таким образом могут гарантировать безопасность цифровых границ.

Бизнес преследует цели получения выгоды, поэтому заинтересован в расширении рынков сбыта, т.е. в информационной глобализации. Именно бизнес-активность играет существенную роль в увеличении объема трансгранично передаваемых данных – прежде всего, речь идет о деятельности глобальных цифровых платформ (таких как компании группы *GAFAM – Google*, *Apple*, *Facebook*, *Amazon* и *BATX – Baidu*, *Alibaba*, *Tascent*, *Xiaomi*). Как отмечают авторы Доклада ЮНКТАД о цифровой экономике за 2021 г., крупные IT-компании имеют возможность управлять огромными цифровыми экосистемами, зачастую ставя под вопрос возможности суверенного контроля отдельных государств над потоками данных, которые пересекают их границы[18].

В 2019-2020 гг. в связи с ограничительными мерами, принятыми США в отношении китайской компании *Huawei*, китайских социальных медиа *TikTok* и *WeChat*[19], наметился новый виток фрагментации интернета, обусловленный конкуренцией между двумя наиболее технологически развитыми странами – США и Китаем[20]. Это в очередной раз продемонстрировало сложный и неоднозначный характер отношений крупных государств с IT-компаниями. Французский исследователь Ж. Носетти полагает, что "роль этих частных предпринимателей напоминает роль, которую в Европе XVII и XVIII вв. играли ост-индские компании: они то объединялись, то соперничали с европейскими государствами, а иногда и полностью игнорировали законодательство последних"[21].

При этом наиболее крупные компании базируются в США и Китае. Согласно статистике ЮНКТАД, на компании, штаб-квартиры которых находятся в этих двух странах, в 2019 г. приходилось 90% рыночной капитализации всех цифровых платформ. Как отмечает Д. Фаррелл, "государства используют крупные IT-компании как "точки контроля" над поведением пользователей или других негосударственных акторов" [Farrell 2012: 361], таким непрямым образом укрепляя свое влияние внутри цифровых границ. Компании соглашаются на это, опасаясь коммерческих издержек, связанных с конфронтацией

[18] UNTAD digital economy report 2021. https://unctad.org/webflyer/digital-economy-report-2021 (accessed 12.01.2022).

[19] См., например, Trump's TikTok battle heralds the ugly birth of a new splinternet. *Wired*. 21.09.2020. https://www.wired.co.uk/article/tiktok-china-trump (accessed 12.01.2022).

[20] The splinternet of things threatens 5G's potential. *The Economist*. 25.12.2019. https://www.economist.com/the-world-in/2019/12/25/the-splinternet-of-things-threatens-5gs-potential (accessed 12.01.2022).

[21] Носетти Ж. Жизнь после Эдварда Сноудена: будущее управления интернетом. *Коммерсантъ*. 09.04.2014. https://www.kommersant.ru/doc/2448799 (accessed 12.01.2022).

с правительствами стран. Однако интересы государств и бизнеса все же лежат в различной плоскости, что во многом объясняет расхождение дискурсивного и онтологического уровней цифровых границ. Важнейшим элементом формирования цифровых границ является легитимация власти государства над определенной "цифровой территорией", при этом важным легитимирующим фактором на дискурсивном уровне выступает секьюритизация глобального информационного пространства и рост угроз информационной безопасности. На уровнях данных и инфраструктуры, а также программного обеспечения главным субъектом глобализации выступает бизнес.

Заключение

Территории в киберпространстве обладают характеристиками географической территории: они определяют, что является "внутренним" и "внешним". Однако особенностью цифровых территорий и цифровых границ является их динамизм – они постоянно изменяются и перестраиваются, причем создание новых территорий и новых измерений киберпространства происходит в результате деятельности государств и негосударственных акторов.

На уровне дискурса укрепление цифровых границ связывается с необходимостью защиты от угроз информационной безопасности, которые носят преимущественно транснациональный характер. Тенденции развития информационного пространства многогранные и нелинейные, они характеризуются участием множества акторов, мотивы которых лежат не только в политической, но и в экономической, ценностной и иных плоскостях. Так что возведение цифровых границ не означает конца информационной глобализации.

Развитие интернета на современном этапе характеризуется одновременным протеканием разнонаправленных процессов глобализации и деглобализации – феномен, который американский ученый Д. Розенау обозначил как "глокализация" [Rosenau 1997: 121]. Причем если на дискурсивном уровне мы наблюдаем усиление фрагментации, то онтология "цифровых границ" в интернете и "цифровой географии" тяготеет скорее к глобализации.

DOI: 10.17976/jpps/2022.02.02

INTERNET FRAGMENTATION AND THE FORMATION OF DIGITAL BORDERS: AN ANALYSIS FROM THE STANDPOINT OF CRITICAL GEOGRAPHY

E.S. Zinovieva[1, 2]

[1] *MGIMO University. Moscow, Russia*

[2] *HSE University. Moscow, Russia*

ZINOVIEVA, Elena Sergeyevna, Cand. Sci. (Polit. Sci.), Professor, World Political Processes Department, MGIMO University; Professor, School of International Affairs, HSE University, email: elena.zinovjeva@gmail.com

Zinovieva, E.S. (2022) Internet fragmentation and the formation of digital borders: an analysis from the standpoint of critical geography. *Polis. Political Studies,* 2, 8-21. (In Russ.) https://doi.org/10.17976/jpps/2022.02.02

Acknowledgements. The article was published as part of the project "Post-crisis world order: challenges and technologies, competition and cooperation" grant No. 2020-1902-01-372.

Received: 05.04.2021. Accepted: 11.12.2021

Abstract. In recent years, the number of scientific publications devoted to the fragmentation of the Internet has been increasing; specialized terms such as "Internet Balkanization" and "Divided Internet"

have appeared to describe the new state of the de-globalized information space. As a rule, this process is associated with the emergence of digital boundaries on the Internet. At the same time, according to statistics, the volume of data crossing the borders of states continues to grow. Thus, information globalization at the data level coexists with the strengthening of digital boundaries and attempts to strengthen digital sovereignty. Critical geography allows us to study digital boundaries not only as material objects, but also as social constructs, discursive practices that reflect the nature of power relations in the international arena and are a source of power for those who create and control them. According to critical geography, digital borders, due to their social nature, are not impenetrable and the construction of digital borders, therefore, does not mean the end of information globalization. The article identifies two levels of digital boundaries – discursive and ontological. At the discursive level, they reflect the securitization of the information sphere and the transformation of the balance of power, the formation of multipolarity, and at the ontological level, they are designed primarily to protect against threats to information security. At the same time, states are interested in the benefits that the global connected Internet provides. Its connectivity is boosted by businesses, which act as the subject of the formation of new global digital spaces, contributing to the globalization of the market in order to increase profits.

Keywords: Internet, globalization, de-globalization, critical geography, international information security, digital sovereignty, digital borders, digital geography.

References

Buchanan, B. (2020). The hacker and the state: cyber attacks and the new normal of geopolitics. Cambridge, MA: Harvard University Press.

Casalini, F., & González, J.L. (2019). Trade and cross-border data flows. *OECD Trade Policy Papers*, 220. Paris: OECD Publishing. https://doi.org/10.1787/b2023a47-en

Deibert, R., & Rohozinski, R. (2010). Liberation vs. control: the future of cyberspace. *Journal of Democracy*, 4, 43-57.

Drezner, D.W. (2004). The global governance of the Internet: bringing the state back in. *Political Science Quarterly*, 119(3), 477-498.

Dunn Cavelty, M. (2013). From cyber-bombs to political fallout: threat representations with an impact in the cyber-security discourse. *International Studies Review*, 15(1), 105-122.

Eriksson, J., & Giacomello, G. (2009). Who controls the internet? Beyond the obstinacy or obsolescence of the State. *International Studies Review*, 11(1), 205-230. https://doi.org/10.1111/j.1468-2486.2008.01841.x

Farrell, H. (2012). The consequences of the internet for politics. *Annual Review of Political Science*, 15, 35-52. https://doi.org/10.1146/annurev-polisci-030810-110815

Finnemore M. (2019) Talking Past Each Other: Government, Business and Civil Society Discussing Cyber Security. *MGIMO Review of International Relations*;12(5), 7-11. https://doi.org/10.24833/2071-8160-2019-5-68-7-11

Herrera, G. (2008). Cyberspace and sovereignty: thoughts on physical spapce and digital space. In M.D. Cavelty, & V. Mauer (Ed.), *Power and Security in the Information Age: Investigating the Role of the State in Cyberspace* (67-93). London: Routlege.

Herrera, G.L. (2012). Technology and international transformation: the railroad, the atom bomb, and the politics of technological change. SUNY Press, 265 p.

Introna, L., & Nisselbaum, H. (1999). Sustaining the public good vision of the Internet: the politics of search engines. *Center for the Arts and Cultural Policy Studies, Working Paper,* 9.

Keohane, R. O., & Nye, Jr. J.S. (2000). Globalization: What's new? What's not? (And so what?). *Foreign Policy*, 118, 104-119.

Lambach, D. (2020). The territorialization of cyberspace. *International Studies Review*, 22(3), 482-506.

Mueller, M.L. (2010). Networks and states: The global politics of Internet governance. Cambridge, MA: MIT Press.

Mueller, M.L. (2020). Against sovereignty in cyberspace. *International Studies Review*, 22(4), 779-801.

Rosenau, J.N. (1997). Along the domestic-foreign frontier: exploring governance in a turbulent world. Cambridge: Cambridge University Press. https://doi.org/10.1017/CBO9780511549472

Rosenau, J.N., & Singh J.P. (Ed.) (2002*).* Information technologies and global politics: the changing scope of power and governance. Albany, NY: State University of New York.

Paasi, A. (2003). Territory. In J. Agnew, K. Mitchell, & G. Ó Tuathail (Ed.), *A Companion to Political Geography* (109-122). Malden: Blackwell. https://doi.org/10.1108/09504120310503764

Ruggie, J.G. (1993). Territoriality and beyond: problematizing modernity in international relations. *International organization,* 47(1), 139-174.

Buharin V.V. (2016). Components of the digital sovereignty of the Russian Federation as a technical basis for information security. *MGIMO Review of International Relations*, 6(51), 76-91. https://doi.org/10.24833/2071-8160-2016-6-51-76-91 (in Russ)

Bykov, A.Yu. (2008). Informational nature of the geopolitics. *Cosmopolis*, 3, 24-31. (In Russ.)

Kucherjavyj, M.M. (2015). State policy of the information sovereignty of Russia in the multipolar world. *Upravlencheskoe konsul'tirovanie,* 2, P. 8-15. (In Russ.)

Miheev, A.N. (2009). Informacionno-kommunikacionnye tehnologii: global'nye problemy i/ili global'nye vozmozhnosti? [ICT: global threats or global possibilities?]. In M. Lebedeva (ed.), *Sovremennye global'nye problemy mirovoj politiki* [Contemporary Global Problems] (121-135). Moscow: Aspect Press. (In Russ.)

Okunev, I.Yu. (2014). Critical geopolitics and post-critical shift in the geopolitical research paradigm. Comparative Politics, 5(4), 6-14. (In Russ.) https://doi.org/10.18611/2221-3279-2014-5-4-6-14

Plotichkina N.V., & Dovbysh E.G. (2017). Network frontier as a metaphor and myth. *RUDN Journal of Sociology*, 17(1), 51-62. https://doi.org/10.22363/2313-2272-2017-17-1-51-62

Strel'cov, A.A. (2017). Sovereignty and Jurisdiction in the ICT sphere in the context of international security. *International Affairs,* 2. (In Russ.) https://interaffairs.ru/jauthor/material/1806

Zinov'eva, E.S. (2013). US digital diplomacy: opportunities and threats for international security. *Security Index*, 1, 213-228. (In Russ.)

Литература на русском языке

Бухарин В.В. 2016. Компоненты цифрового суверенитета российской федерации как техническая основа информационной безопасности. *Вестник МГИМО-Университета*. № 6(51). С. 76-91. https://doi.org/10.24833/2071-8160-2016-6-51-76-91

Быков А.Ю. 2008. Информационная сущность геополитики. *Космополис*. № 3. С. 24-31.

Зиновьева Е.С. 2013. Цифровая дипломатия США: возможности и угрозы для международной безопасности. *Индекс Безопасности*. № 1. С. 213-228.

Кучерявый М.М. 2015. Государственная политика информационного суверенитета России в условиях современного глобального мира. *Управленческое консультирование*. № 2. С. 8-15.

Михеев А.Н. 2009. Информационно-коммуникационные технологии: глобальные проблемы и/или глобальные возможности? *Современные глобальные проблемы мировой политики*. Под ред. М.М. Лебедевой. М.: Аспект Пресс.

Окунев И.Ю. 2014. Критическая геополитика и посткритический сдвиг в исследовательской парадигме геополитики. *Сравнительная политика*. Т. 5. № 4. С. 6-14. https://doi.org/10.18611/2221-3279-2014-5-4-6-14

Плотичкина Н.В., Довбыш Е.Г. 2017. Сетевой фронтир как метафора и миф. *Вестник Российского университета дружбы народов. Серия: Социология*. Т. 17. № 1. С. 51-62. https://doi.org/10.22363/2313-2272-2017-17-1-51-62

Стрельцов А.А. 2017. Суверенитет и юрисдикция государства в среде информационно-коммуникационных технологий в контексте международной безопасности. *Международная жизнь*. № 2. https://interaffairs.ru/jauthor/material/1806