ОРИГИНАЛЬНАЯ СТАТЬЯ

DOI: 10.26794/2226-7867-2022-12-2-153-158
УДК 323(045)

Формирование института «суверенного интернета» в Российской Федерации

Д.Э. Ковригин
Финансовый университет, Москва, Россия

АННОТАЦИЯ

В статье рассматриваются меры, обусловленные геополитическими вызовами, предпринимаемые государствами и ограничивающие формирование глобального цифрового пространства. Для противостояния новым угрозам страны создают институты, устанавливающие национальные границы киберпространства. Государства стремятся создать системы регулирования цифрового пространства для сохранения своего суверенитета, и этот процесс является современной общемировой тенденцией. Развитие института «суверенного интернета» в России выступает элементом государственной политики для ограничения внешнего влияния при дестабилизации политической ситуации.

Ключевые слова: глобализация; информационное пространство; цифровые коммуникации; «суверенный интернет»; государственная политика

Для цитирования: **Ковригин Д.Э. Формирование института «суверенного интернета» в Российской Федерации. *Гуманитарные науки. Вестник Финансового университета.* 2022;12(2):153-158. DOI: 10.26794/2226-7867-2022-12-2-153-158**

ORIGINAL PAPER

Formation of the Institution of "Sovereign Internet" in the Russian Federation

D.E. Kovrigin
Financial University, Moscow, Russia

ABSTRACT

The article discusses measures caused by geopolitical challenges, taken by states, and limiting the formation of a global digital space. With the aim to counter new threats to the country, institutions are being created that establish national boundaries of cyberspace. States are striving to create systems for regulating the digital space to preserve their sovereignty, and this process is a modern global trend. The development of the "sovereign Internet" institution in Russia is an element of state policy to limit external influence while destabilizing the political situation.

Keywords: globalization; information space; digital communications; "sovereign Internet"; public policy

For citation: **Kovrigin D.E. Formation of the institution of "sovereign Internet" in the Russian Federation. *Gumanitarnye Nauki. Vestnik Finasovogo Universiteta = Humanities and Social Sciences. Bulletin of the Financial University.* 2022;12(2):153-158. DOI: 10.26794/2226-7867-2022-12-2-153-158**

ГЕОПОЛИТИКА ЦИФРОВОГО МИРА

Информационное пространство стало новой сферой геополитического противостояния государств. В соответствии с информационной парадигмой геополитики отношения между государствами в современном мире в первую очередь определяются посредством превосходства в информационном пространстве. В своих работах Дж. О'Тоал утверждает, что информационное пространство стало «третьей природой» геополитики [1]. Территориальность постепенно заменяется телеметричностью, а государства уступают место сетям. В конце XX в. появилось большое количество теорий, в соответствии с которыми вследствие экстерриториального характера интернета и невозможности контроля формирующегося киберпространства произойдет постепенное отмирание национальных государств. М.М. Лебедева понимает глобализацию как «процесс размывания межгосударственных границ вследствие развития информационных и коммуникативных технологий, экономических связей и отношений» [2].

В соответствии с концепцией В.Л. Иноземцева, глобализация — это скрытый процесс замены прямого контроля над миром на косвенный, избавляющий контролера от всякой ответственности [3]. Основная проблема современного мира состоит в отставании политической глобализации от информационной, социальной и экономической. У США на данный момент наибольшее количество элементов влияния на глобальное интернет- пространство: так,

социальная сеть Facebook и поисковик Google, созданный на территории США, регулируется местным законодательством, а также активно сотрудничают со спецслужбами, став инструментом политического влияния США. В свою очередь, политика Российской Федерации по суверенизации киберпространства направлена на защиту своих граждан от влияния извне.

Государства и компании борются за контроль над самым крупным нерегулируемым социальным пространством — киберпространством. На протяжении долгого времени государства не оказывали на данную сферу существенного влияния, что позволило компаниям получить в ней регулирующие функции. Установление корпоративного контроля над определенными зонами, где не действуют законы государства, привело к формированию системы, которую американский ученый Шошана Зубофф назвала «капитализм надзора». Это экономическая система, которая базируется на коммерциализации персональных данных с целью получения прибыли. В связи с этим можно вспомнить скандал 2004 г., когда выяснилось, что почтовый сервис Gmail сканирует переписку для предоставления данных рекламодателям, или ситуацию 2007 г. с системой Beacon от Facebook, которая отслеживала деятельность пользователей на сторонних сайтах. Во многих государствах есть законы о неприкосновенности частной жизни и тайне переписки (в нашей стране это п. 1, 2 ст. 23 Конституции РФ[1]). Однако компании нарушали и продолжают нарушать подобные законы.

Возможность слежки за своими пользователями и предоставление им той информации, которая выгодна компаниям, позволяет манипулировать людьми. На современном этапе развития общества власть не у того, кто владеет информацией, а у того, кто имеет возможность регулировать информационные потоки. В данных условиях особое место занимает угроза гибридной и информационной войны.

С появлением «цифрового мира» возникла принципиально новая сфера человеческих взаимоотношений. Киберпространство представляет угрозу, так как через него происходит бесконтрольное формирование сознания граждан. Противодействуя данным вызовам, государства изобретают институты, которые регулируют принципиально новые отношения, выстраивая свои виртуальные границы.

[1] URL: http://www.consultant.ru/document/cons_doc_LAW_28399/2573feee1caecac37c442734e00215bbf1c85248/

МЕТОДОЛОГИЯ ИССЛЕДОВАНИЯ

В качестве методологии данного исследования используется неоинституционализм. Основными представителями этого направления являются Р. Коуз, М. Олсон, Г. Саймон, О. Уильямсон и Д. Норт. Дугласу Норту принадлежит наиболее известное определение института — «правила игры в обществе» — т.е. создаваемые людьми ограничительные рамки, регулирующие человеческое взаимодействие [4]. Другое необходимое в данной статье понятие — «трансакционные издержки», которые Р. Коуз определяет как «издержки сбора и обработки информации, издержки проведения переговоров и принятия решения, издержки контроля и юридической защиты выполнения контракта» [5].

В рамках теории институционального изменения в настоящей работе проводится анализ развития новых отношений, складывающихся внутри современных государств. В соответствии с положениями теории основными функциями институтов общества являются сдерживание оппортунистического поведения человека и минимизация трансакционных издержек. По мнению Д. Норта, при рассмотрении процесса трансформации институтов общества важно учитывать такие важные факторы, как идеология, культура и исторические особенности государства.

Государства Запада активно разрабатывают способы ведения борьбы в информационном пространстве и методы его регулирования. Для этого необходимо изучение процессов развития интернет-пространства и аудитории. В Российской Федерации исследования в данной сфере становятся все более востребованными. Основой исследований являются научные работы С.В. Володенкова [6], Л.В. Сморгунова, Р.В. Пырмы, Е.В. Бродовской, Е.С. Зиновьева [7], Ю.А. Кабанова [8] и А.В. Даниленкова [9].

ИНСТИТУЦИОНАЛИЗАЦИЯ КИБЕРПРОСТРАНСТВА

Государство всегда находится перед дилеммой: сохранить старые институты или заменить их новыми. Если старые институты больше не способны регулировать различные процессы, то возрастают трансакционные издержки и наступает время для изменения или замены институтов. Институты призваны обеспечить объединение общества в государство, а также не допустить распада последнего, особенно в новую информационную эпоху. При изучении трансформации отдельных институтов или всего общества в целом необходимо выявить эндогенные факторы, способствующие данным процессам, а именно, трансформации отношений

в обществе под влиянием новых информационных технологий. Информационная эпоха привела не к отмене института суверенитета государства, а к развитию его новых видов: цифрового и информационного суверенитета, суверенитета киберпространства, личного цифрового суверенитета и т.д. Под «цифровым суверенитетом» следует понимать возможность власти устанавливать порядок информационной коммуникации внутри государства. Также это понятие подразумевает право государства на производство, распространение и использование информации без вмешательства извне [10]. Под «государственным суверенитетом» в сети Интернет следует понимать систему, в которой государство является главным администратором национального информационного пространства и телекоммуникационной инфраструктуры [9]. Но данные концепции в современных условиях не реализованы в большинстве государств из-за отсутствия как технической, так и законодательной базы. Однако возрастание угроз для государства со стороны киберпространства привело к тому, что начался процесс формирования институтов, направленных на реализацию данных положений. Государства формируют новые институты, исходя из своего исторического опыта и идеологии. Так, интернет-пространство в Китае является наиболее закрытым и регулируемым в мире, а США, наоборот, обладает крайне слабым суверенитетом.

Введение новых институтов регулирования в киберпространстве приводит не только к изменению институциональной среды на уровне одного государства, но и на общемировом уровне. Постепенно в едином и глобальном информационном пространстве начинают функционировать самостоятельные подсистемы национальных интернет-пространств, которые становятся все более автономными. Это происходит не только из-за действий государств, направленных на обеспечения своей безопасности, но и потому, что люди объединяются в локальные сетевые сообщества в рамках национального сегмента интернета. Так появляются отечественные социальные сети и платформы, которые активно функционируют в рамках одного конкретного государства. Тенденции по усилению контроля за деятельностью людей и компаний прослеживаются во всем мире. Даже США, обладающие наибольшими возможностями в сфере регулирования глобального киберпространства, усиливают контроль за социальными сетями. Подтверждением этому служат многочисленные судебные дела против Facebook, в частности обвинения в разжигании конфликтов в обществе и ослаблении демократии, выдвинутые против сети в 2021 г. Также можно привести в качестве примера запрет на скачивание TikTok и WeChat в США в 2020 г.

НОРМАТИВНОЕ РЕГУЛИРОВАНИЕ

Российская Федерация, проводя свою политику, стремится сохранить суверенитет в сфере киберпространства, ограничив свободу деятельности международных социальных сетей, минимизировав возможность иностранного влияния на граждан, а также понизив криминальную активность в российском сегменте интернета. Для достижения этих целей разрабатывается система суверенного интернета и другие институты, направленные на регулирование данной сферы. Наиболее важными документами в сфере регулирования интернет- коммуникаций, принятыми в период с 2019 по 2021 г., являются:

- Закон о «суверенном интернете»[2], принятый 1 мая 2019 г., направленный на обеспечение бесперебойной работы российского сегмента интернета. Для достижения данной цели необходимо: создание реестра точек обмена трафиком и национальной системы доменных имен; участие поставщиков рынка IT-услуг в учениях и т.д.
- Закон об измерении объема интернет-аудитории[3] 2021 г., предназначенный для проведения кроссмедийных исследований аудитории в сети Интернет.
- Закон о «приземлении» иностранных IT-компаний[4] 2021 г., в соответствии с которым социальные сети, чья российская аудитория составляет более 500 тыс. чел. в сутки, обязаны открыть свои представительства на территории Российской Федерации, разместить на своем сайте систему приема сообщений от граждан, а также соблюдать законы государства и оперативно реагировать на обращения Роскомнадзора.
- Законопроект № 1057337–7[5], в соответствии с которым запрещается использование общедо-

[2] Федеральный закон от 01.05.2019 № 90-ФЗ «О внесении изменений в Федеральный закон «О связи» и Федеральный закон «Об информации, информационных технологиях и о защите информации»». URL: http://publication.pravo.gov.ru/Document/View/0001201905010025

[3] Законопроект № 1175409–7 «О внесении изменений в отдельные законодательные акты Российской Федерации». URL: https://sozd.duma.gov.ru/bill/1175409–7

[4] Законопроект № 1176731–7 «О деятельности иностранных лиц в информационно-телекоммуникационной сети "Интернет" на территории Российской Федерации». URL: https://sozd.duma.gov.ru/bill/1176731–7

[5] Законопроект № 1057337–7 «О внесении изменений в Федеральный закон "О персональных данных"». URL: https://sozd.duma.gov.ru/bill/1057337–7

ступных персональных данных без согласия владельца.

• Закон о предустановке российского софта[6] от 1 июля 2020 г., направленный на защиту прав потребителей и продвижение российских программ на рынке информационных технологий.

• Приказ Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций[7] от 24.02.2021 № 18 «Об утверждении требований к содержанию согласия на обработку персональных данных, разрешенных субъектом персональных данных для распространения», в соответствии с которым третье лицо может получить доступ к персональным данным другого человека только при наличии его согласия.

• Приказ Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций от 31.07.2019 № 229 о национальной системе доменных имен, порядке ее создания и требованиях к ней[8].

Развитие системы регулирования интернет-коммуникаций на территории Российской Федерации прошло несколько условных этапов. Первый — с момента появления интернета на территории Российской Федерации (7 апреля 1994 г.) до 2014 г. В данный период киберпространство подвергалось крайне слабому регулированию со стороны государства, и активно развивались неформальные институты поведения граждан России в данной среде. В 2014 г. по поручению Президента Владимира Путина были проведены учения, направленные на проверку возможности продолжения работы российского интернета в случае сбоев в DNS, в ходе которых необходимость развития законодательной и технической систем для поддержания стабильного функционирования интернет-пространства Российской Федерации стала очевидной. Далее начался этап постепенного развития данной сферы, завершением которого можно считать принятие в 2019 г. закона «о суверенном интернете». С момента принятия данного закона идет третий этап, характеризующийся крайне бурным развитием институтов суверенного интернета Российской Федерации, что приводит к радикальному пересмотру системы взаимодействия государства, граждан и международных компаний в киберпространстве России.

Здесь просматривается очевидная закономерность в развитии институтов. Государство обнаружило сферу, в которой оно уязвимо из-за недостатка эффективности формальных институтов, и предприняло активные действия для ликвидации данной уязвимости. Ведущими направлениями этого процесса выступают: регламентация виртуальной жизни граждан, контроль за деятельностью социальных сетей, создание дублирующих систем киберпространства, регулирование потоков информации, распространение российского ПО, развитие IT-сектора экономики, развитие систем противодействия процессам цифрового проникновения со стороны субъектов внешнего политического противоборства, создание отечественных альтернатив зарубежной IT-продукции и платформам, сокращение приступной и террористической активности в киберпространстве.

Российское государство активно развивает институты, через которые оно осуществляет свои функции в новом типе пространства — киберпространстве. Вслед за введением новых формальных правил регулирования киберпространства происходит активное развитие механизмов принуждения. Но для достижения стабильности новой системы институтов необходимо параллельное развитие российского сегмента IT-технологий, а также приложений для удовлетворения потребностей национального сегмента потребителей. Особенно это касается социальных сетей.

На современном этапе становится очевидным, что социальные сети активно задействованы в политическом процессе. Так, 10 сентября 2021 г. МИД Российской Федерации вызвал посла США в Москве Джона Салливана в связи с вмешательством американских IT-компаний в процесс выборов в Госдуму. И это только один из множества аналогичных случаев вмешательства платформ в политическую и экономическую жизнь государств, вследствие чего появилась необходимость обязать такие компании подчиняться законам государства, на территории

[6] Законопроект № 757423–7 «О внесении изменения в статью 4 Закона Российской Федерации “О защите прав потребителей”». URL: https://sozd.duma.gov.ru/bill/757423–7

[7] Приказ Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций от 24.02.2021 № 18 «Об утверждении требований к содержанию согласия на обработку персональных данных, разрешенных субъектом персональных данных для распространения». URL: http://publication.pravo.gov.ru/Document/View/0001202104210039

[8] Приказ Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций от 31.07.2019 № 229 «Об утверждении Положения о национальной системе доменных имен, требований к ней, порядка её создания, в том числе формирования информации, содержащейся в ней, а также правил её использования, включая условия и порядок предоставления доступа к информации». URL: http://publication.pravo.gov.ru/Document/View/0001201911080052

которого они действуют, а также создавать их отечественные аналоги.

ОТНОШЕНИЕ ГРАЖДАН

Развитие института «суверенного интернета» затрагивает важнейшие сферы жизни современного российского общества и, как следствие, порождает активный дискурс. Поскольку неформальные институты общества, связанные с киберпространством, развивались в атмосфере крайне слабого контроля со стороны государства, его усиление было воспринято отрицательно. Негативные отклики на закон о «суверенном интернете» и на последующие реформы сводятся к трем основным проблемам:

- крупные затраты и со стороны государства, и со стороны новостных агентств и IT-компаний, которым необходимо установить новое оборудование и программное обеспечение (так, в период с 2022 по 2024 г. на поддержание функционирования российского сегмента интернета планируется выделить около 31 млрд руб.);
- возрастание риска попадания частной информации третьим лицам, а также страх перед слежкой со стороны спецслужб;
- проблемы с доступностью интернет-соединения у российских пользователей.

Также термин «суверенный интернет» имеет в российском обществе скорее негативный окрас из-за весьма распространенного опасения, что данный процесс приведет к тотальному контролю за информацией со стороны государства. Это связано с негативным опытом тоталитарного корнтроля периода СССР, а также с примером жесткой цензуры в современном КНР (проект «Золотой щит»). У граждан Российской Федерации не сформировалось понимание того, что суверенизация интернета — это не ограничение свободы, а в первую очередь процесс определения зоны правовых полномочий государства в сочетании с созданием дублирующих систем, направленных на защиту и поддержание стабильного функционирования национального киберпространства. Принятие реформ может сформироваться в процессе активного общественного дискурса, а также разъяснительной деятельности со стороны государства.

ВЫВОДЫ

Государству необходимо приспособиться к новым условиям — тому, что информационное пространство изменило геополитическую картину мира. Оно не может оставаться полностью открытым, ведь, чем более система открыта, тем больше она подвергается негативному воздействию. Однако полностью закрытой система тоже быть не может,— всегда найдутся способы обхода блокировок, как со стороны граждан, так и со стороны других государств. Р. Кларк указывает на парадокс: чем менее развито информационное пространство государства, тем больше устойчивость к угрозам и прочнее суверенитет [11]. Поэтому необходимо достичь такого состояния национального информационного и киберпространства, при котором система будет гомеостатичной. В ходе изменения глобальной ситуации в области информационных технологий, вызванной их экстерриториальным характером, существующие общественные институты стали неэффективными, и у государств появилась необходимость в развитии или замене таких институтов. Цифровой суверенитет стал новым вызовом для современных государств. Российская Федерация стремится развить институты регулирования, определив тем самым сферу своего суверенитета в информационном пространстве. Необходимо контролировать сферу IT-технологий и одновременно создавать альтернативы иностранным компаниям. Это является необходимым условием выживания государства в долгосрочной перспективе. По мере развития как законодательной, так и технологической базы процесс будет только ускоряться. С возникновением стабильных официальных институтов «суверенного интернет-пространства» должны появиться поддерживающие неформальные институты.

Деятельность Российской Федерации по развитию цифрового суверенитета направлена на защиту информации и противодействие иностранному вмешательству, а также на становление отечественного программного обеспечения. Российской Федерации как одному из крупнейших игроков на международной арене необходимо максимально оперативно реагировать на новые виды угроз и совершенствовать свой сегмент киберпространства.

СПИСОК ИСТОЧНИКОВ

1. Лебедева М.М. Мировая политика и международные отношения на пороге нового тысячелетия. М.: Московский общественный научный фонд; 2000.
2. Иноземцев В.Л. Современная глобализация и ее восприятие в мире. *Век глобализации*. 2008;(1):31–44.
3. Норт Д. Институты, институциональные изменения и функционирование экономики. М.: Фонд экономической книги «Начала»;1997.

4. Коуз Р. Фирма, рынок и право. М.: Дело; 1993.
5. Володенков С.В., Митева В.В. Сетевые информационные войны в современных условиях: основные акторы и стратегии. *PolitBook*. 2016;(3):18–35.
6. Зиновьева Е.С. Глобальное управление Интернетом: Российский подход и международная практика. *Вестник МГИМО*. 2015;4(43):111–181.
7. Кабанов Ю.А. Информационное пространство как новое (гео)политическое пространство: роль и место государств. *Сравнительная политика*. 2014;4(17):54–59.
8. Даниленков А.В. Государственный суверенитет Российской Федерации в информационно-телекоммуникационной сети «Интернет». *Lex Russica.* 2017;7(128):154–165.
9. Gong W. Information Sovereignty Reviewed. *Intercultural Communication Studies*. 2005; XIV(1):119–135.
10. Кларк Р. Третья мировая война: какой она будет?: высокие технологии на службе милитаризма. Пер. с англ. URL: https://coollib.com/b/168011-richard-klark-tretya-mirovaya-voyna-kakoy-ona-budet/read.
11. О'Тоал Дж. Геополитика постмодерна? Геополитические представлении модерна и за их пределами. *Политическая наука.* 2009;(1):188–223.

REFERENCES

1. Lebedeva M.M. World politics and international relations on the threshold of the new millennium. Moscow: Moscow public scientific fund; 2000. (In Russ.).
2. Inozemtsev V.L. Modern globalization and its perception in the world. *Age of globalization*. 2008;(1):31–44. (In Russ.).
3. North D. Institutions, institutional changes and the functioning of the economy. Moscow: Fund of the economic book "Nachala"; 1997. (In Russ.).
4. Coase R. Firm, market and law. Moscow: Delo; 1993. (In Russ.).
5. Volodenkov S.V., Miteva V.V. Network information wars in modern conditions: main actors and strategies. *PolitBook*. 2016;(3):18–35. (In Russ.).
6. Zinovieva E.S. Global Internet Governance: Russian Approach and International Practice. *Bulletin of MGIMO*. 2015;4(43):111–181. (In Russ.).
7. Kabanov Yu.A. Information space as a new (geo)political space: the role and place of states. *Comparative politics*. 2014;4(17):54–59. (In Russ.).
8. Danilenkov A.V. State sovereignty of the Russian Federation in the information and telecommunications network "Internet". *Lex Russica*. 2017;7(128):154–165. (In Russ.).
9. Gong W. Information Sovereignty Reviewed. *Intercultural Communication Studies.* 2005; XIV(1):119–135.
10. Clark R. The third world war: what will it be?: high technologies in the service of militarism. URL: https://coollib.com/b/168011-richard-klark-tretya-mirovaya-voyna-kakoy-ona-budet/read. (In Russ.).
11. O'Toal J. Postmodern geopolitics? Geopolitical representations of modernity and beyond. *Political science*. 2009;(1):188–223. (In Russ.).

ИНФОРМАЦИЯ ОБ АВТОРЕ

Дмитрий Эльдарович Ковригин — бакалавр, магистрант 2-го курса факультета социальных наук и массовых коммуникаций, Финансовый университет, Москва, Россия
https://orcid.org/0000-0001-9880-1137
dmitrykovr@gmail.com

ABOUT THE AUTHOR

Dmitry E. Kovrigin — Bachelor, 2nd-year Master student, Faculty of Social Sciences and Mass Communications, Financial University, Moscow, Russia
https://orcid.org/0000-0001-9880-1137
dmitrykovr@gmail.com

Конфликт интересов: автор заявляет об отсутствии конфликта интересов.
Conflicts of Interest Statement: The author has no conflicts of interest to declare.

Статья поступила 20.01.2022; принята к публикации 12.02.2022.
Автор прочитал и одобрил окончательный вариант рукописи.
The article was received on 20.01.2022; accepted for publication on 12.02.2022.
The author read and approved the final version of the manuscript.