УДК 32.019.5 DOI: 10.17506/18179568_2024_21_4_26

СУВЕРЕНИЗАЦИЯ ЦИФРОВЫХ ОБЩЕСТВЕННО-ПОЛИТИЧЕСКИХ КОММУНИКАЦИЙ: АНАЛИЗ АКАДЕМИЧЕСКОГО ДИСКУРСА

Сергей Владимирович Володенков,

Государственный академический университет гуманитарных наук, Московский государственный университет имени М.В. Ломоносова, Москва, Россия
s.v.cyber@gmail.com

Сергей Николаевич Федорченко,

Государственный академический университет гуманитарных наук, Московский государственный университет имени М.В. Ломоносова, Москва, Россия,
s.n.fedorchenko@mail.ru

Получена 02.10.2024.
Поступила после рецензирования 20.11.2024.
Принята к публикации 11.12.2024.

Для цитирования: Володенков С.В., Федорченко С.Н. Суверенизация цифровых общественно-политических коммуникаций: анализ академического дискурса // Дискурс-Пи. 2024. Т. 21. № 4. С. 26–47. https://doi.org/10.17506/18179568_2024_21_4_26

Аннотация

В условиях кризиса однополярного порядка и возросшей в связи с этим геополитической турбулентности на фоне одновременно происходящих в мире глобальных цифровых технологических трансформаций актуализируются процессы формирования, усиления и защиты нового типа государственного суверенитета – цифрового. Такие процессы создают запрос на активизацию академического дискурса и проведение дополнительных исследований в сфере существующих предпосылок, препятствий, экономических, политических и ценностно-цивилизационных особенностей трансформации существующих и формирования новых суверенных моделей цифровых общественно-политических коммуникаций, обеспечивающих реализацию национальных интересов. В связи с этим целью настоящей работы стало выявление специфики современного академического дискурса, посвященного проблеме суверенизации цифровых общественно-политических коммуникаций. Методологическая оптика критического дискурс-анализа научных работ была в основном сфокусирована на двух исследовательских критериях: (1) поиске существующих теоретических попыток объяснения причин суверенизации цифровых коммуникаций и (2) выявлении условных складывающихся моделей суверенизации цифровых коммуникаций. В ходе исследования был выявлен рост популярности в современном академическом дискурсе категорий цифрового суверенитета, кибербезопасности, суверенитета данных, цифровых границ, цифровой балканизации. По итогам работы делается вывод о том, что теории цифрового колониализма, колониализма данных, платформенного империализма и вепонизации Интернета не противоречат друг другу, но, напротив, дополняют существующую научную картину происходящих трансформаций в цифровом пространстве. Вместе с тем сопоставление существующих теоретических концептов позволило обнаружить их содержательные различия. Также по итогам проведенного анализа академических исследований был выявлен спектр формирующихся моделей суверенизации цифровых общественно-политических коммуникаций, появление и развитие которых во многом было обусловлено несогласием ряда государств с господством американоцентричной глобальной модели управления цифровым пространством. По итогам исследования авторы делают вывод о необходимости формирования российской модели суверенизации цифровых коммуникаций, формулируя ее ключевые характеристики, определяющие ее уникальность в сравнении со складывающимися аналогичными моделями в других странах и регионах мира.

Ключевые слова:

цифровой суверенитет, цифровые общественно-политические коммуникации, цифровая колонизация, платформенный империализм, суверенизация коммуникаций

Источники финансирования:

исследование выполнено в рамках проекта «FZNF-2024–0006 – Суверенная модель стратегического развития цифровых общественно-политических коммуникаций в современной России: ключевые потенциалы и сценарии формирования» при поддержке Министерства науки и высшего образования Российской Федерации и Экспертного института социальных исследований.

UDC 32.019.5 DOI: 10.17506/18179568_2024_21_4_26

SOVEREIGNIZATION OF DIGITAL COMMUNICATIONS IN THE SOCIO-POLITICAL SPHERE: AN ANALYSIS OF ACADEMIC DISCOURSE

Sergey V. Volodenkov,

State Academic University of Humanities,
Lomonosov Moscow State University,
Moscow, Russia,
s.v.cyber@gmail.com

Sergey N. Fedorchenko,

State Academic University of Humanities,
Lomonosov Moscow State University,
Moscow, Russia,
s.n.fedorchenko@mail.ru

Received 02.10.2024.
Revised 20.11.2024.
Accepted 11.12.2024.

For citation: Volodenkov, S.V., Fedorchenko, S.N. (2024). Sovereignization of Digital Communications in the Socio-Political Sphere: An Analysis of Academic Discourse. *Discourse-P, 21*(4), 26–47. (In Russ.). https://doi.org/10.17506/18179568_2024_21_4_26

Abstract

Amid the crisis of the unipolar order and the ensuring geopolitical turbulence, which are further intensified by global digital technological transformations, the establishment, reinforcement, and protection of a new form of state sovereignty – digital sovereignty – has become increasingly pertinent. This situation necessitates further academic research into the existing prerequisites, obstacles, challenges, as well as the civilizational characteristics influencing the transformation of current sovereignty models. It also requires development of new sovereign frameworks for digital communications in the socio-political sphere that would effectively safeguard national interests. This study aims to identify the specifics of contemporary academic discourse surrounding the issue of sovereignization in terms of digital communication in the socio-political context. Employing a methodological framework of critical discourse analysis, the research focuses on two primary criteria: (1) exploring theoretical frameworks that explain the motivations behind the sovereignization of digital communications, and (2) identifying sovereignization models that emerge these days in relation to digital communication. The findings indicate a rising emphasis on such concepts *as digital sovereignty, cybersecurity, data sovereignty, digital borders, and digital balkanization* within current academic discussions. The study concludes that the theories of digital colonialism, data colonialism, platform imperialism, and the weaponization of the Internet are not mutually exclusive; rather they complement the existing scholarly understanding of the ongoing transformations in the digital realm. A comparative analysis of these concepts and theories reveals nuanced distinctions between them. Furthermore, the examination of academic literature has uncovered a range of emerging sovereignization models of digital communications in the socio-political sphere, largely driven by the discontent of various states with the prevailing US-centric global governance in the digital realm. Consequently, the authors advocate for the development of a Russian sovereignization model of digital communication, outlining its key characteristics that distinguish it from similar emerging models in other countries and regions of the world.

Keywords:

digital sovereignty, digital communications, sovereignization, socio-political sphere, digital colonization, platform imperialism, sovereignization models of digital communications

Funding:

The study was conducted as part of the project "FZNF-2024–0006 – Sovereign Model of Strategic Development of Digital Socio-Political Communications in Contemporary Russia: Key Potentials and Formation Scenarios". The project received financial support of the Ministry of Science and Higher Education of the Russian Federation and the Expert Institute of Social Research.

Введение

Развитие глобальных технологических корпораций, рост их цифровых экосистем, претензии цифровых платформ на роль нового социального клея в условиях кризиса прежнего однополярного порядка, возросшей геополитической турбулентности и вызванного ею увеличения интенсивности информационных войн между странами определили вызовы для формирования, усиления и защиты нового типа суверенитета государства – цифрового. Такие вызовы создают запрос на активизацию академического дискурса и проведение дополнительных исследований в сфере существующих предпосылок, препятствий, экономических, политических и ценностно-цивилизационных особенностей для трансформации различных моделей цифровых общественно-политических коммуникаций.

Следует подчеркнуть, что под общественно-политическими коммуникациями мы понимаем совокупность базовых коммуникативных площадок, каналов, арен взаимодействия общества, государства и человека по различным вопросам экономики, политики, культуры.

Особую стратегическую значимость таким коммуникациям придает их цифровой характер, определяющийся в связанности с цифровыми стандартами, алгоритмами, программным обеспечением, выпускаемыми конкретными разработчиками. Безусловно, базовую нагрузку в анализе цифровых общественно-политических коммуникаций должен нести Интернет, однако не стоит забывать и о связанных с ним платформах, веб-приложениях, Интернете вещей, нейронных сетях и разнообразных «сквозных технологиях», из которых может быть соткана метавселенная, дополненная реальность и другие цифровые экосистемы.

При этом общественно-политический спектр коммуникационного пространства выбран нами не случайно. Степень зависимости государства от технологических корпоративных гигантов, не являющихся его резидентами, влияет на уровень объективных угроз для выстраиваемой им системы обратной связи с обществом, без которой государственные служащие не могут объективно определить контур актуальных проблем граждан. Последние, в свою очередь, лишаются полноценной возможности своевременно сообщать о таких проблемах государству. В результате санкций, инициируемых и вводящихся технологическими корпорациями в интересах враждебных государств, страна может столкнуться со снижением собственной информационной безопасности, ухудшением качества коммуникации между гражданами, регулярными нарушениями конфиденциальности их данных. Определенные риски не стоит исключать и в плане навязывания искаженных, ложных моделей существующей политической реальности, генерируемых транснациональными корпорациями по договоренности с заказчиком и чреватых возникновением новых конфликтных ситуаций, конфликтов в области межнациональных, политических, социальных или межрелигиозных отношений.

Существование такого рода особенностей, рисков и трендов определяет в качестве цели настоящей работы выявление специфики современного академического дискурса, посвященного проблеме суверенизации цифровых общественно-политических коммуникаций.

Краткий обзор научной литературы

Обращаясь к обзору академической литературы по выбранной проблематике, для начала важно рассмотреть само явление суверенизации цифровых общественно-политических коммуникаций. Как отмечает российский политолог А.М. Ваховский, такая суверенизация подразумевает аспекты регулирования глобальной компьютерной сети в условиях санкций и угроз отключения государства от возможностей и ресурсов Интернета (Ваховский, 2019, с. 12). Согласно такой позиции, можно разделять внутреннюю и внешнюю суверенизацию цифровых коммуникаций. Если внутренняя суверенизация в большей мере сосредоточена на развитии и обретении независимости национального коммуникационного сегмента государства от внешних акторов, то внешняя суверенизация, как правило, обусловлена ответами на дополнительные вызовы со стороны иных государств. Такой подход позволяет изучать суверенизацию коммуникаций в качестве ответа на вызов десуверенизации.

Суверенизация цифровых общественно-политических коммуникаций означает достижение важных качественных показателей государства в сфере киберпространства. Сначала в отечественной политической науке не обращались к цифровому суверенитету, предпочитая говорить о коммуникационном суверенитете. При этом подобные термины часто бывают схожи по своей сути, касаясь одних и тех же явлений, процессов, феноменов. Так, И.Н. Панарин под коммуникационным суверенитетом России понимал не только защищенность личности, государства, общества от коммуникационной агрессии, но и «состояние безопасности коммуникационного пространства страны». Примечательно, что в коммуникационный суверенитет Панарин включает духовный суверенитет, информационный суверенитет (доминирование в информационном поле страны позитивного контента о национальных ценностях, героях, истории), а также киберсуверенитет (кибербезопасность страны) (Панарин, 2013, с. 13). Вместе с тем, категория цифрового суверенитета, все чаще встречаясь в современных отечественных политологических трудах, вовсе не отменяет термин коммуникационный суверенитет, а, скорее, дополняет его, учитывая фактор технологических конфликтов между политически мотивированными корпоративными техногигантами (Ромашкина, Киричук, 2023, с. 853). В зарубежной политической науке не существует однозначного ответа на то, что такое цифровой суверенитет. Хотя трехлетнее исследование на базе Лундского университета показало, что цифровой суверенитет связан с инициативой государственных служащих, недовольством их в существующем наборе цифровых артефактов, веб-приложений, а не только с желанием государства контролировать данные и разработку программного обеспечения (Paulsson, Fred, 2024).

Ярким проявлением суверенизации цифровых общественно-политических коммуникаций выступает зарождение в киберпространстве так называемых «цифровых границ» (Zhang, Morris, 2023). Скорее, это можно считать не причинами, а последствиями суверенизации. К этому феномену авторы серьезно стали обращаться сравнительно недавно, отталкиваясь от кейса КНР,

в котором пользователи разделяют контент, распространяемый внутри границ китайской коммуникационной сферы (neiwang), и контент, циркулирующий за ее пределами (waiwang). Между тем эта тема только на первый взгляд может показаться совершенно новой: ранее до нее уже появились осторожные размышления (Weichselbaum et al., 2016) по поводу эффекта цифровой балканизации или кибербалканизации (cyberbalkanization), понимаемой в виде событий, способствующих фрагментации не только Интернета, но и любой коммуникационной деятельности в цифровом пространстве. Изначально такая балканизация объяснялась ростом интернет-пользователей за пределами Соединенных Штатов. Другие авторы (Rinesi, 2018), допуская употребление такой неоднозначной категории, использовали для описания происходящей фрагментации киберпространства термин «выравнивание» (alignment). Это означало, что государства не столько пытались создать собственный локальный Интернет, сколько начать играть более активную роль в управлении цифровыми общественно-политическими коммуникациями.

На первый взгляд проблему суверенизации цифровых общественно-политических коммуникации можно и нужно рассматривать через призму суверенитета данных (data sovereignty), так как явление Big Data больше связано именно с цифровыми, а не традиционными коммуникационными каналами. По оценке исследователей из Университета Эрлангена – Нюрнберга, дискуссия вокруг суверенитета данных сосредоточена вокруг аспектов власти над данными и проектирования IT-архитектуры (Hummel et al., 2021). Научные труды других авторов показывают, что суверенитет данных невозможен без суверенитета платформ, концепт которых также начал сравнительно недавно разрабатываться в связи с попытками корпоративных техногигантов (особенно американских Google, Apple, Amazon и др.) полностью контролировать собственные цифровые инфраструктуры, используя практику властных отношений, повторения, создания иллюзии выбора для граждан. Отмечаемая демонстрация платформами своего технического превосходства над правительствами, возможно, является одной из причин актуализации темы цифрового суверенитета в разных государствах (Heylen, 2023). Различные причины суверенизации цифровых коммуникаций (информационная политика США и их геополитических союзников, политизация деятельности технологических корпораций, риски санкций) позволили начать говорить некоторым ученым об ответной реакции – зарождении моделей суверенизации цифровых общественно-политических коммуникаций (Eko, 2001).

Итак, краткий обзор научных работ показывает, что наиболее важные аспекты выбранной для анализа темы касаются причин суверенизации и ее последствий, а также проявлений суверенизации цифровых общественно-политических коммуникаций. Отталкиваясь от этой стартовой дихотомии, методологическая оптика критического дискурс-анализа научных работ была в основном сфокусирована на двух исследовательских критериях: (1) поиске существующих теоретических попыток объяснения причин суверенизации цифровых коммуникаций и (2) выявлении условных складывающихся моделей суверенизации цифровых коммуникаций.

Попытки объяснения причин цифровой суверенизации

Крах биполярной системы международных отношений и возникновение периода однополярного мирового порядка с ключевой геополитической ролью Соединенных Штатов создали условия для неолиберальной экономической и цифровой глобализации, в процессе которой сформировалась модель многостороннего управления глобальными цифровыми коммуникациями на основе международных организаций. Данный глобальный порядок отвергал создание государствами альтернативных моделей в виде национальных сегментов суверенного киберпространства (Barrinha, Christou, 2022). Тем не менее, продвижение одной американоцентричной глобальной модели управления киберсредой не остановило другие государства от попыток разработки иных принципов цифровых коммуникационных экосистем, отвечающих их политическим интересам. Критическое отношение формировалось и в отношении созданной при участии американского правительства корпорации ICANN, ответственной за управление IP-адресами и доменными именами. Свою роль сыграли и разоблачения Эдварда Сноудена, экономические противоречия стран.

Одной из причин суверенизации цифровых общественно-политических коммуникаций выступает цифровая колонизация, соответственно, появилась целая *теория цифрового колониализма*, которая пытается объяснить этот тренд. На примере Канады имеются свидетельства, что цифровые корпорации способны разрушать саму социальную ткань, традиционные ценности и нормы общественной коммуникации (Young, 2019). Крупнейший специалист в области исследования проблем цифровой колонизации, сотрудник Йельского университета М. Квет полагает, что в современное время появились три формы новой цифровой власти, связанные с контролем над сетевым подключением, оборудованием и программным обеспечением (Kwet, 2019, p. 6). Контроль над сетевым подключением включает совокупность стандартов, протоколов, отношение интернет-провайдеров к контенту, трафику, проходящему через поддерживаемые ими коммуникации (например, встречается практика замедления подключения до минимальных значений). Если пользователи не могут изменить код, а предоставляемый интерфейс разрабатывается на стороннем оборудовании (компьютерах, облачных сервисах корпорации, где осуществляются вычисления), то мы сталкиваемся с рисками и угрозами контроля над оборудованием (аппаратным обеспечением). В случае если инструкциями ограничивается пользовательский опыт, посредством программ определяются правила публикационной политики, то можно говорить о контроле над программным обеспечением.

Квет подчеркивает, что цифровая колонизация осуществляется в режиме капитализма слежения, реализуемого крупными технологическими корпорациями (big teach), которые наделяют США в странах глобального Юга большой политической, социальной и экономической властью (имперским государственным надзором) через практики этих видов цифрового контроля. Ученый считает, что цифровые формы контроля являются результатом эволюции прежней модели вмешательства американских властей в политику Южной

Африки (практики наблюдения за работой шахтеров в XIX в., использование перфокарт IBM для создания системы апартеида по четырем расовым категориям в XX в.) (Kwet, 2019, p. 13). Другие же исследования позволяют изучать такие цифровые процессы не только с точки зрения цифровой колонизации, односторонней информационной активности и агрессии Соединенных Штатов, но и посмотреть на эту проблему через призму американо-китайского соперничества, проявляющегося в возникновении двух конкурирующих цифровых пространств, специфических форм государственного платформенного капитализма, разных типов взаимодействия государства и технологических корпораций (Rolf, Schindler, 2023). Данное обстоятельство вызывает необходимость рассмотреть дополнительные доказательства существования цифрового колониализма.

Примечательно, что некоторые исследования по перспективам деколонизации цифровых коммуникаций, по сути, выходят на проблемный фон суверенизации. Например, М. Манн (Университет Виктории в Веллингтоне) и А. Дэйли (Университет Данди) в своей довольно интересной работе утверждают, что современная Австралия, являясь страной Глобального Севера в регионе Глобального Юга (Global-North-in-South), осуществляет типичные практики цифрового колониализма и информационного империализма в отношении иных государств, входя в разведывательный альянс Five Eyes (вместе с США, Великобританией, Новой Зеландией и Канадой) и собирая для него информацию о странах Азиатско-Тихоокеанского региона. Манн и Дэйли считают, что примером цифровых колониальных практик Австралии можно считать установление подслушивающих устройств в новом суверенном государстве Тиморе-Лешти (Mann, Daly, 2019). Как можно заметить, в рамках теории цифрового колониализма часто в качестве основных бенефициаров таких форм технологического контроля рассматриваются политически и экономически влиятельные государства.

Еще одной причиной суверенизации общественно-политических коммуникаций, как ответной реакции некоторых государств, можно назвать датификацию, глубокие трансформации самого капитализма, которые привели к возникновению капитализма слежения (или капитализма платформ). Одним из проявлений таких метаморфоз ученые называют зарождение рыночного сектора социальной квантификации, состоящего из крупных и мелких разработчиков программного обеспечения и производителей оборудования, связанного с анализом больших данных и брокерской активностью. На деле практически нерегулируемый рынок брокеров данных занимается алгоритмическим сбором данных, их упаковкой и продажей (рекламодателям, правительствам). Существование такого сектора пытаются объяснить с помощью *теории колониализма данных* (Couldry, Mejias, 2018), согласно которой на эволюцию исторических форм колониализма и капитализма нужно смотреть в совокупности. Колониализм данных меняет само общество, переводя социальные отношения на уровень отношений данных, преобразуя любую деятельность человека в новую абстрактную форму для бесконечного присвоения данных крупными корпорациями и их цифровыми платформами, что, безусловно, представляет непосредственную угрозу для цифрового суверенитета страны.

Теория колониализма данных выступает против тотальной датификации и схожа с теорией цифровой колонизации, но в основном сосредоточена на корпоративной угрозе и секторе социальной квантификации.

Однако теория колониализма данных поддерживается не всеми учеными. Так, С. Кальцати из Делфтского технического университета критикует ее за гиперболизацию процесса датификации, «универсализм данных», недостаточную аргументацию выделения особых, противостоящих друг другу колониальных держав данных (к примеру, США и КНР), излишнее отождествление пользователей с пассивными субъектами данных (Calzati, 2020, p. 5–12). Кальцати считает, что ситуация является намного более сложной, предлагая в качестве альтернативы модель «федеративных систем данных» для изучения активности консорциумов, в которых субъекты заимствуют и обрабатывают данные из общей сети (к примеру, формируется сложное переплетение интересов западных, китайских и африканских корпораций). Автор обращает внимание на то, что китайские корпорации участвуют в сложных системах, консорциумах, контролирующих интернет-структуру, состоящую из подводных кабелей, автономных систем, сетей доставки контента, тогда как американские корпорации в основном сконцентрировались на контроле программного обеспечения и интернет-сервисов. В то же время модель Кальцати не отрицает саму возможность внешнего влияния на цифровые общественно-политические коммуникации суверенной страны. Не исключено, что те государства (африканские, латиноамериканские, постсоветские, южноазиатские и др.), которые не могут себе позволить выбрать стратегию суверенизации цифровых коммуникаций (как Китай, США и Россия), вынуждены участвовать своими корпорациями в таких сложных консорциумах, чтобы не допустить доминирования в своем сегменте киберпространства какой-либо одной страны и ее технологических гигантов.

Риски десуверинизации современных государств также просчитываются рядом ученых в рамках *теории платформенного империализма*, одним из авторов которой является ученый Университета Саймона Фрезера Д. Джин (Jin, 2013). С. Баннерман из Макмастерского университета описывает ряд признаков, которые сближают эту концептуальную модель с теорией цифрового колониализма и теорией колониализма данных. Но в качестве специфики она отмечает, что теоретическая рамка платформенного империализма пытается объяснить, каким образом платформы (суверены платформ) наделяются полномочиями государств, а государства, наоборот, наделяются полномочиями платформ. Порядок платформенного империализма складывается не только на базе цифровых технологий, но и на основе глобальной системы интеллектуальной собственности, защищающей эти технологии с помощью патентного права. Платформенный империализм угрожает традиционному суверенитету государств, так как, с одной стороны, использует международные структуры власти, а, с другой стороны, пользуется принципами диффамации, практикуемой в период существования администрации Британской империи и запрещающей абсолютно любую критику колониальных практик (Bannerman, 2024). Теоретическая схема

платформенного империализма исходит из того, что цифровые платформы, так же как и государства, пытаются контролировать посредством властных приемов население, территории и общественно-политические коммуникации.

Справедливости ради стоит заметить, что ничего принципиально нового в идее осмысления такой формы империализма нет. Предшественницей данной теории является концепция медиа-империализма (медиатизированного империализма) О. Бойд-Барретта, оттолкнувшегося от трудов Г. Инниса, К. Бейли, Г. Шиллера, Э. Хермана, Н. Хомского, А. Маккоя и раскрывшего в своей монографии, каким образом крупные медиа-конгломераты могут становиться агентами империалистической деятельности (Бойд-Барретт, 2018, с. 29, 99–101). Бойд-Барретт также отметил зарождающиеся тренды сопротивления такой форме империализма на примере активизации российских, китайских, арабских и других национальных информационных агентств. Однако модель медиа-империализма хотя и пыталась связать действия медиа-олигополий с политическими интересами США и их западных союзников, практически обходила стороной феномен цифрового капитализма и рост значимости алгоритмов платформ, искусственного интеллекта.

В последнее время перспективной концепцией становится *вепонизация Интернета*. Вепонизация (от *weapon* – оружие, *weaponization* – оснащение оружием) в данном смысле означает использование в конфликтных, военных целях сфер, изначально не предназначенных для этого, внедрение в практику противоборства новейших типов информационного оружия, в том числе и на основе искусственного интеллекта, превращение пространств цифровых общественно-политических коммуникаций суверенных государств в арену геополитических войн нового типа. Согласно концепции вепонизации цифровых коммуникаций, сокращение пользовательской базы Соединенных Штатов относительно интернет-пользователей в других странах, неспособность США утвердить односторонний контроль над цифровыми коммуникациями в мире, сложность их централизации привели к тому, что американские власти изменили свою киберстратегию и стали добиваться сокращения доступа стран-противников к критически значимой интернет-инфраструктуре посредством односторонних киберсанкций и блокировок со стороны крупных технологических корпораций (Ortiz Freuler, 2023). В рамках такой цифровой вепонизации американские власти устанавливают режим массированной слежки по всему миру, стремясь уже не подчинять своим интересам все мировые коммуникации, а способствовать расколу мирового киберпространства и одновременному формированию новой глобальной цифровой топографии из контролируемых ими пространств из цифровых узлов в зависимых государствах и блокируемых пространств из цифровых узлов стран-изгоев (Ирана, Китая, России и др.).

В результате проводимая Соединенными Штатами вепонизация киберпространства провоцирует в качестве ответной меры суверенизацию общественно-политических коммуникаций в разных странах. Однако необходимо заметить, что теоретическая схема вепонизации Интернета нуждается в более серьезной концептуальной проработке, тем более что факты

ведения алгоритмических войн, применения киберармий, информационного оружия, хакерских атак в политических целях существуют и требуют своего дальнейшего теоретического осмысления.

И здесь нам представляется необходимым перейти от теоретического осмысления к рассмотрению и анализу формирующихся сегодня моделей суверенизации цифровых общественно-политических коммуникаций, являющихся ответной реакцией государств на сложившиеся в настоящее время обстоятельства.

Намечающиеся модели цифровой суверенизации

Анализ научной литературы демонстрирует, что в мире складывается несколько условных моделей суверенизации цифровых общественно-политических коммуникаций. К примеру, в ответ на вызовы десуверенизации, связанные с цифровой колонизацией, платформенным империализмом и вепонизацией Интернета уже развивается отдельная *китайская модель* цифровой суверенизации. Китайская модель предполагает, с одной стороны, регулирование национального рынка цифровых коммуникаций и, с другой стороны, постепенное проникновение собственных крупных технологических корпораций на внешние рынки других стран. При этом регуляция общественно-политических коммуникаций обладает многоуровневым и комплексным характером. Речь идет о фильтрации информации посредством программного обеспечения, функционировании ответственных цензоров, системы наказания и наблюдения за потребителями и поставщиками контента с целью сохранения контроля государства за цифровыми коммуникациями и предупреждения негативного влияния информации на граждан. Интернет-шлюзы, созданные для контроля трафика информации, разделены на несколько уровней (Мельникова, 2022): локальный (коммуникационная система городов), основной (Сиань, Нанкин, Шэньян, Чанчжоу, Ухань, Чунцин, Чунцин) и национальный (Пекин, Гуанчжоу, Шанхай, подключенные к международным каналам). Но КНР не только сосредотачивается на внутренней регуляции киберпространства. Поддерживаемые властями крупные китайские технологические корпорации (например, Huawei, ZTE Corporation и др.) активно продвигают новые цифровые технологии в других государствах. Поэтому этот подход в научной литературе иногда называется моделью «развития двойной циркуляции» (Becerra, Waisbord, 2021).

Существует мнение, что цифровой суверенитет важен и для институционализации кибервласти партии-государства. В некоторых работах (Becerra, Waisbord, 2021) на этом основании делают вывод о существовании в Китае, Иране и России некой схожей модели кибернационализма (cybernationalism), ставшей преемницей модели медианационализма (media nationalism) – государственной политики контроля над международными медиа XX в. Но такой тезис приравнивания кибернационализма к цифровой суверенизации весьма спорен, так как, во-первых, не учитывает политическую, цивилизационную, экономическую специфику цифровых коммуникаций трех стран,

во-вторых, соотносится с некими нелиберальными попытками восстановления суверенитета, одновременно не поясняя суть либеральных попыток суверенизации цифровых коммуникаций, и, в третьих, замалчивает роль в цифровой колонизации (Kwet, 2019) крупных западных технологических корпораций, ставших, по сути, проводниками политических и экономических интересов Соединенных Штатов и их союзников. Корректнее сказать, что китайское правительство заинтересовано в существовании альтернативных западным социальных сетей (WeChat, Weibo).

Китайские цифровые коммуникации действительно обретают признаки территоризации и цифровых границ, будучи зависимыми от национальной физической инфраструктуры и правовых практик (Zhang, Morris, 2023). Между тем Закон о кибербезопасности КНР, опубликованный в 2016 г., по мнению некоторых авторов, оговаривая китайскую власть над внутренней киберактивностью пользователей и трансграничными потоками данных, может спровоцировать ответные действия со стороны других стран. Конечно, китайская модель предусматривает проверку критически значимых сетевых услуг и продуктов, выпуск стандартов кибербезопасности, но некоторые стандарты местные власти вынуждены раскрывать ВТО, чтобы избежать негативной реакции, в том числе США (Hong, Goodnight, 2019). Таким образом, китайский суверенитет во внутренней цифровой сфере также ограничен существующими международными организациями. Более современные работы подтверждают эти наблюдения, ссылаясь на участие китайской стороны в работе проектной группы IETF по цифровым стандартам (Nanni, 2022).

С определенной степенью осторожности можно отметить функционирование *иранской модели* суверенизации цифровых общественно-политических коммуникаций. С китайской иранскую модель сближают присутствие цензуры, правительственный курс на развитие незападных, собственных цифровых коммуникаций и технологий. Иранские технологические корпорации стараются инициировать создание национальных операционных систем, собственных социальных сетей, приложений для обмена сообщениями (Soroush, iGap), видеохостингов (Aparat). *Telecommonication Company of Iran* является крупнейшим оператором сотовой связи, учитывающим государственную медиаполитику. Принципиальным отличием иранской модели цифровой суверенизации от китайской является сосредоточенность местных технологических корпораций на внутренней аудитории. Иранские корпорации не могут активно работать в других странах, в том числе и из-за серьезных американских санкций, наложенных на страну.

Санкции препятствуют развитию национальной цифровой экономики, хотя существуют и приемы их обхода, и серый рынок. Цензура цифровых коммуникаций оправдывается иранскими властями необходимостью обеспечения национальной безопасности на фоне угроз государственного переворота, в котором заинтересованы Соединенные Штаты. С этой целью власти Ирана фильтруют западный контент, платформы и сервисы, противоречащие местным религиозным ценностям (Hashemzadegan, Gholami, 2022).

В свое время иранским государством были созданы Верховный совет по киберпространству, Центр национальной кибербезопасности, Совет по кибербезопасности, кибер-полиция.

Ученые фиксируют и особую *латиноамериканскую модель* суверенизации цифровых общественно-политических коммуникаций, которая означает постепенный переход от политики медианационализма (media nationalism) 1960–1970 гг. к более прагматичной цифровой политике XXI в. Развитие медианационализма Перу (1968–1975 гг.) и Венесуэлы (1974–1975 гг.) исследователи поясняли не только желанием их политических элит контролировать потоки международных новостей посредством нормативных инструментов, но и необходимостью защиты от угрозы американского медиа-империализма. Однако в 1980–1990-х гг. государственная медиаполитика латиноамериканских стран переориентировалась на рост иностранных инвестиций, дерегуляцию и сокращение значения государства в развитии медиаиндустрии (Becerra, Waisbord, 2021). Государственный контроль над медиа в основном сохранялся на Кубе.

С начала 2000-х гг. фиксируется очередная попытка некоторых латиноамериканских стран (Венесуэлы, Бразилии, Аргентины, Боливии, Эквадора, Уругвая) пересмотреть политику дерегуляции коммуникаций, уйдя от неолиберального рыночного подхода к политике диверсификации собственности на медиа. Трансформация медиаполитики возникла из-за конфликта между государством и крупными корпорациями в латиноамериканских странах (Becerra, Wagner, 2018). Власти этих государств серьезно опасались влияния крупных корпораций на суверенный политический процесс и общественные дискуссии из-за конструирования узкого предложения новостных программ. Тем не менее, современный латиноамериканский вариант суверенизации цифровых коммуникаций не включает существования некого наднационального законодательства и регулятора, как в случае с ЕС.

Латиноамериканская модель обладает колебательным характером, зависит от внутриполитической конъюнктуры и внешнеполитического давления. В основе такой модели лежит прагматизм, так как цифровая экономика стран Латинской Америки уступает по объему экономикам стран Запада или Азии, среди латиноамериканских государств пока не наблюдается геополитических игроков, сопоставимых с великими державами наподобие России, США и КНР. Напротив, местные правительства в основном вынуждены допускать доминирующую роль крупных американских технологических корпораций, привлекают инвестиции от китайских корпораций и стремятся адаптироваться к технологической конкуренции между Китаем и Соединенными Штатами, так как не могут противопоставить им активность своих компаний. Балансирование между американскими и китайскими технологическими корпорациями объясняется тем, что латиноамериканские правительства не пошли по пути «цифрового девелопментализма» – развития местных цифровых промышленных комплексов, рынков цифровых коммуникаций с важной ролью государства как регулятора их отношений (Becerra, Waisbord, 2021).

На основании реальных кейсов и нормативной практики также можно выделить *европейскую модель* суверенизации цифровых общественно-политических коммуникаций, действующую в государствах – членах Европейского союза. В отличие от латиноамериканского варианта, европейская модель предполагает наличие регулятора в области киберпространства (в виде общеевропейских органов власти и законодательства ЕС), функция которого менялась с 1995 по 2021 гг. (Flonk, Jachtenfuchs, Obendiek, 2024). Стратегия кибербезопасности ЕС (2020 г.) уже упоминает факторы лидерства, технологического суверенитета, устойчивости к киберугрозам, формирования производственных мощностей. Президент Европейского совета Ш. Мишель отмечал важность цифрового рынка, предполагающего европейские цифровые решения и определяющего правила. ЕС, как и латиноамериканские страны, выступает за установление двухсторонних и многосторонних отношений формирования киберпространства. Вместе с тем европейская модель цифровых коммуникаций означает суверенизацию, предполагающую защиту от цифрового влияния иных государств, купирование рисков со стороны американских и китайских крупных технологических корпораций, присваивающих и монетизирующих данные европейских пользователей (Barrinha, Christou, 2022). ЕС продвигает идею достижения устойчивой, безопасной технологической инфраструктуры.

Последние исследования трансформации законодательства ЕС свидетельствуют, что европейская модель суверенизации цифровых коммуникаций постепенно смещается с приоритетов открытости Интернета, свободного доступа к коммуникациям, расширения и укрепления прав пользователей на приоритеты поддержания общественного порядка (public order), защиты от вредоносного контента, дезинформации, диффамации, терроризма, враждебных иностранных субъектов. Усиливаются акценты борьбы с разжиганием ненависти, защиты либерально-демократического порядка. Такие категории, как контроль и власть, становятся все более актуальными в европейском дискурсе. В связи с этим некоторые авторы отмечают, что усиление контроля ЕС над контентом в европейских цифровых коммуникациях может иметь глобальные последствия, так как влияние европейского регулятора способно распространяться и на другие страны (Flonk, Jachtenfuchs, Obendiek, 2024).

Другие же авторы, напротив, полагают, что ЕС запоздал с регулированием цифровых коммуникаций, называя среди причин этого изначально слабое финансирование европейских программ в области конструирования киберпространства (например, существовавший в 1980–1984 гг. проект *Euronet* финансировался в меньшей степени по сравнению с американским проектом ARPANET), доминирование в мире американских и китайских крупных технологических корпораций (с которыми европейским компаниям сложно конкурировать), влияющих на социальную и экономическую жизнь в ЕС и находящихся вне его правового поля (Nieminen, Padovani, Sousa, 2023). Хотя следует отметить, что европейский уровень управления региональным киберпространством все-таки существует, будучи представленным ETSI (Европейским институтом стандартов телекоммуникаций), ENISA (Агентством Европейского союза по кибербезопасности) и другими структурами.

Выводы

Подводя итоги проведенного критического дискурс-анализа академических работ, важно сформулировать несколько выводов.

Во-первых, изучение современной научной литературы показало, что появилось несколько теоретических конструктов, в рамках которых предпринимается попытка выявления каузальных механизмов суверенизации цифровых общественно-политических коммуникаций в ряде стран и регионов мира. В целом, фиксируемые концептуальные схемы вовсе не противоречат друг другу, а, напротив, дополняют нашу научную картину происходящих трансформаций в киберпространстве. Так, особенность теории цифрового колониализма заключается в ее интересе к бенефициарам технологического контроля – экономически и политически влиятельным государствам. В отличие от нее, концепция колониализма данных опирается на идею развития исторических форм капитализма и колониализма, акцентируя внимание исследователей на возрастании роли корпоративной власти, а также рынка социальной квантификации. В свою очередь, теория платформенного империализма во многом является развитием концепции медиа-империализма и фокусируется на рисках десуверенизации современных государств в связи с проникновением крупных технологических корпораций в социально-политическую и экономическую жизнь стран. Наконец, теория вепонизации Интернета пытается объяснить, каким образом частная корпоративная структура начинает играть роль нового типа оружия Соединенных Штатов, используемого ими против их геополитических конкурентов.

Во-вторых, на основе анализа научных работ были выявлены несколько формирующихся моделей суверенизации цифровых общественно-политических коммуникаций, развитие которых во многом было обусловлено несогласием ряда государств с господством американоцентричной глобальной модели управления киберсредой. Китайская модель сочетает регулирование внутреннего рынка цифровых коммуникаций с одновременным постепенным проникновением собственных крупных технологических корпораций на внешние рынки. Фактор цензуры внутреннего интернет-трафика во многом сближает иранскую модель с китайской. Однако принципиальными отличиями иранской модели остаются нахождение страны под сильными американскими санкциями и сосредоточенность местных технологических корпораций на внутренней аудитории. Европейская модель суверенизации цифровых коммуникаций схожа с латиноамериканской моделью тем, что в ней практикуются многосторонние отношения формирования киберпространства, присутствует лавирование между различными крупными технологическими корпорациями. При этом важным отличием европейской модели можно назвать наличие наднационального регулятора цифровых коммуникаций.

На данный момент сложно однозначно определить четкие признаки отдельной *российской модели* суверенизации цифровых общественно-политических коммуникаций, хотя запрос на ее создание есть как у общества, так и российского государства. Однако появление подобной модели объективно назрело из-за

серьезного конфликта США и стран коллективного Запада с Россией, формирования в этой связи существенных рисков информационных и алгоритмических войн, хакерских атак, угроз отсечения граждан от жизненно важной цифровой инфраструктуры. Об этом свидетельствует целый корпус работ российских ученых, посвященных теме цифрового суверенитета.

Между тем, по нашему мнению, российская модель суверенизации цифровых коммуникаций не должна просто копировать уже намечающиеся (и в основном условные) модели. Отечественная модель цифровых общественно-политических коммуникаций может задействовать возможности использования потенциалов таких международных организаций, как БРИКС и ШОС, параллельно развивая собственные суверенные решения в области опорных компонентов цифровой власти – программного обеспечения, компьютерного оборудования и сетевого подключения. Такая модель не должна означать некую замкнутость на собственном рынке цифровых коммуникаций, но предполагать активную поддержку российских технологических корпораций, проникающих и на цифровые рынки других стран и регионов. В рамках формирования российской модели суверенизации цифровых коммуникаций также важно учитывать и угрозы, риски, вызовы трансформации американской модели развития цифровых коммуникации, которая означает смещение от глобального варианта управления Интернетом к использованию санкций и провоцированию цифровой балканизации, информационных конфликтов между странами и регионами. Так или иначе, представляется очевидным, что сегодня перед нашей страной стоит серьезный вызов, заключающийся в стратегическом выборе того пути, по которому будет развиваться отечественное пространство цифровых общественно-политических коммуникаций, и в том, в какой степени будет достигнута его суверенизация, являющаяся, по нашему глубокому убеждению, одним из важнейших факторов развития сильного, независимого и конкурентноспособного в геополитическом смысле российского государства.

Список литературы

1. Бойд-Баррет, О. (2018). *Медиа-империализм*. Харьков: Гуманит. Центр.
2. Ваховский, А.М. (2019). Суверенизация Интернета как проблема современного политического процесса. *Известия Тульского государственного университета. Гуманитарные науки*, (1), 11–18. https://doi.org/10.24411/2071-6141-2019-10101
3. Мельникова, О. (2022). Опыт Китая в защите национального киберсуверенитета. *Международная жизнь*, (12), 106–119.
4. Панарин, И.Н. (2013). Коммуникационный суверенитет России. *Обзор*. НЦПТИ, (2), 8–13.
5. Ромашкина, А.Б., Киричук, Д.А. (2023). Политическая субъектность цифровых актантов в контексте обеспечения цифрового суверенитета. *Вестник Российского университета дружбы народов. Серия: Политология, 25*(4), 848–861. https://doi.org/10.22363/2313-1438-2023-25-4-848-861

6. Bannerman, S. (2024). Platform imperialism, communications law and relational sovereignty. *New Media & Society, 26*(4), 1816–1833. https://doi.org/10.1177/14614448221077284

7. Barrinha, A., & Christou, G. (2022). Speaking sovereignty: the EU in the cyber domain. *European Security, 31*(3), 356–376. https://doi.org/10.1080/09662839.2022.2102895#d1e284

8. Becerra, M., & Wagner, C.M. (2018). Crisis of representation and new media policies in Latin America. *Latin American Perspectives, 45*(3), 86–102. https://doi.org/10.1177/0094582X18766895

9. Becerra, M., & Waisbord, S.R. (2021). The curious absence of cybernationalism in Latin America: Lessons for the study of digital sovereignty and governance. *Communication and the Public, 6*(1–4), 67–79. https://doi.org/10.1177/20570473211046730

10. Calzati, S. (2020). Decolonising "Data Colonialism" Propositions for Investigating the Realpolitik of Today's Networked Ecology. *Television & New Media*, 152747642095726. https://doi.org/10.1177/1527476420957267

11. Couldry, N., & Mejias, U.A. (2018). Data Colonialism: Rethinking Big Data's Relation to the Contemporary Subject. *Television & New Media*, 152747641879663. https://doi.org/10.1177/1527476418796632

12. Eko, L. (2001). Many Spiders, One Worldwide Web: Towards a Typology of Internet Regulation. *Communication Law and Policy, 6*(3), 445–484. https://doi.org/10.1207/s15326926clp0603_0

13. Flonk, D., Jachtenfuchs, M., & Obendiek, A. (2024). Controlling internet content in the EU: towards digital sovereignty. *Journal of European Public Policy, 31*(8), 2316–2342. https://doi.org/10.1080/13501763.2024.2309179

14. Hashemzadegan, A., & Gholami, A. (2022). Internet Censorship in Iran: An Inside Look. *Journal of Cyberspace Studies, 6(*2), 183–204. https://doi.org/10.22059/jcss.2022.349715.1080

15. Heylen, K. (2023). Enforcing platform sovereignty: A case study of platform responses to Australia's News Media Bargaining Code. *New Media & Society, 26*(2). https://doi.org/10.1177/14614448231166057

16. Hong, Y., & Goodnight, G.T. (2019). How to think about cyber sovereignty: the case of China. *Chinese Journal of Communication*, (13), 1–19. https://doi.org/10.1080/17544750.2019.1687536

17. Jin, D.Y. (2013). The construction of platform imperialism in the globalization era. Triplec: *Communication, Capitalism & Critique. Open Access Journal for a Global Sustainable Information Society, 11*(1), 145–172. https://doi.org/10.31269/triplec.v11i1.458

18. Kwet, M. (2019). Digital colonialism: US empire and the new imperialism in the Global South. *Race & Class, 60*(4), 3–26. https://doi.org/10.1177/0306396818823172

19. Mann, M., & Daly, A. (2019). (Big) Data and the North-in-South: Australia's Informational Imperialism and Digital Colonialism. *Television and New Media, 20*(4), 379–395, https://doi.org/10.1177/1527476418806091

20. Nanni, R. (2022). Digital sovereignty and Internet standards: normative

implications of public-private relations among Chinese stakeholders in the Internet Engineering Task Force. *Information, Communication & Society, 25*(16), 2342–2362. https://doi.org/10.1080/1369118X.2022.2129270

21. Nieminen, H., Padovani, C., & Sousa, H. (2023). Why Has the EU Been Late in Regulating Social Media Platforms? *Javnost – The Public, 30*(2), 174–196. https://doi.org/10.1080/13183222.2023.2200717

22. Ortiz Freuler, J. (2023). The weaponization of private corporate infrastructure: Internet fragmentation and coercive diplomacy in the 21st century. *Global Media and China, 8*(1), 6–23. https://doi.org/10.1177/20594364221139729

23. Hummel, P., Braun, M., Tretter, M., & Dabrock, P. (2021). Data sovereignty: A review. *Big Data & Society, 8*(1), https://doi.org/10.1177/2053951720982012

24. Paulsson, A., & Fred, M. (2024). Making apps, owning data: Digital sovereignty and public authorities' arrangements to "byte" back. *Organization*. https://doi.org/10.1177/13505084241246073

25. Rinesi, M. (2018). Will the Internet fragment?: *Sovereignty, globalization and cyberspace. Prometheus*, (1–2), https://doi.org/10.1080/08109028.2018.1505

26. Rolf, S., & Schindler, S. (2023). The US-China rivalry and the emergence of state platform capitalism. *Environment and Planning A: Economy and Space, 55*(5), 1255–1280. https://doi.org/10.1177/0308518X221146545

27. Weichselbaum, L., Spagnuolo, M., Lekies, S., & Janc, A. (2016). CSP is dead, long live CSP! On the insecurity of whitelists and the future of Content Security Policy. *In Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security* (pp. 1376–1387).

28. Young, J.C. (2019). The new knowledge politics of digital colonialism. *Environment and Planning A: Economy and Space, 51*(7), 1424–1441. https://doi.org/10.1177/0308518X19858998

29. Zhang, C., & Morris, C. (2023). Borders, bordering and sovereignty in digital space. Territory, Politics. *Governance, 11*(6), 1051–1058. https://doi.org/10.1080/21622671.2023.2216737

References

1. Bannerman, S. (2024). Platform imperialism, communications law and relational sovereignty. *New Media & Society*, 26(4), 1816–1833. https://doi.org/10.1177/14614448221077284

2. Barrinha, A., & Christou, G. (2022). Speaking sovereignty: the EU in the cyber domain. *European Security*, 31(3), 356–376. https://doi.org/10.1080/09662839.2022.2102895#d1e284

3. Becerra, M., & Wagner, C.M. (2018). Crisis of representation and new media policies in Latin America. *Latin American Perspectives*, 45(3), 86–102. https://doi.org/10.1177/0094582X18766895

4. Becerra, M., & Waisbord, S.R. (2021). The curious absence of cybernationalism in Latin America: Lessons for the study of digital sovereignty

and governance. *Communication and the Public*, *6*(1–4), 67–79. https://doi.org/10.1177/20570473211046730

5. Boyd-Barrett, O. (2018). *Media-imperializm* [Media imperialism]. Kharkov: Gumanit. Tsentr.

6. Calzati, S. (2020). Decolonising "Data Colonialism" Propositions for Investigating the Realpolitik of Today's Networked Ecology. *Television & New Media*, 152747642095726. https://doi.org/10.1177/1527476420957267

7. Couldry, N., & Mejias, U.A. (2018). Data Colonialism: Rethinking Big Data's Relation to the Contemporary Subject. *Television & New Media*, 152747641879663. https://doi.org/10.1177/1527476418796632

8. Eko, L. (2001). Many Spiders, One Worldwide Web: Towards a Typology of Internet Regulation. *Communication Law and Policy*, 6(3), 445–484. https://doi.org/10.1207/s15326926clp0603_0

9. Flonk, D., Jachtenfuchs, M., & Obendiek, A. (2024). Controlling internet content in the EU: towards digital sovereignty. *Journal of European Public Policy*, 31(8), 2316–2342. https://doi.org/10.1080/13501763.2024.2309179

10. Hashemzadegan, A., & Gholami, A. (2022). Internet Censorship in Iran: An Inside Look. *Journal of Cyberspace Studies*, *6*(2), 183–204. https://doi.org/10.22059/jcss.2022.349715.1080

11. Heylen, K. (2023). Enforcing platform sovereignty: A case study of platform responses to Australia's News Media Bargaining Code. *New Media & Society*, *26*(2). https://doi.org/10.1177/14614448231166057

12. Hong, Y., & Goodnight, G.T. (2019). How to think about cyber sovereignty: the case of China. *Chinese Journal of Communication*, (13), 1–19. https://doi.org/10.1080/17544750.2019.1687536

13. Hummel, P., Braun, M., Tretter, M., & Dabrock, P. (2021). Data sovereignty: A review. *Big Data & Society*, *8*(1), https://doi.org/10.1177/2053951720982012

14. Jin, D.Y. (2013). The construction of platform imperialism in the globalization era. Triplec: *Communication, Capitalism & Critique. Open Access Journal for a Global Sustainable Information Society*, *11*(1), 145–172. https://doi.org/10.31269/triplec.v11i1.458

15. Kwet, M. (2019). Digital colonialism: US empire and the new imperialism in the Global South. *Race & Class*, *60*(4), 3–26. https://doi.org/10.1177/0306396818823172

16. Mann, M., & Daly, A. (2019). (Big) Data and the North-in-South: Australia's Informational Imperialism and Digital Colonialism. *Television and New Media*, *20*(4), 379–395, https://doi.org/10.1177/1527476418806091

17. Melnikova, O. (2022). Opyt Kitaya v zashchite natsional'nogo kibersuvereniteta [China's experience in protecting national cyber sovereignty]. *Mezhdunarodnaya zhizn'*, (12), 106–119.

18. Nanni, R. (2022). Digital sovereignty and Internet standards: normative implications of public-private relations among Chinese stakeholders in the Internet Engineering Task Force. *Information, Communication & Society*, *25*(16), 2342–2362. https://doi.org/10.1080/1369118X.2022.2129270

19. Nieminen, H., Padovani, C., & Sousa, H. (2023). Why Has the EU Been Late in Regulating Social Media Platforms? *Javnost – The Public*, *30*(2), 174–196. https://doi.org/10.1080/13183222.2023.2200717

20. Ortiz Freuler, J. (2023). The weaponization of private corporate infrastructure: Internet fragmentation and coercive diplomacy in the 21st century. *Global Media and China*, *8*(1), 6–23. https://doi.org/10.1177/20594364221139729

21. Panarin, I. N. (2013). Kommunikatsionnyy suverenitet Rossii [Communication sovereignty of Russia]. *Obzor*. NTsPTI, (2), 8–13.

22. Paulsson, A., & Fred, M. (2024). Making apps, owning data: Digital sovereignty and public authorities' arrangements to "byte" back. *Organization*. https://doi.org/10.1177/13505084241246073

23. Rinesi, M. (2018). Will the Internet fragment?: Sovereignty, globalization and cyberspace. *Prometheus*, (1–2), https://doi.org/10.1080/08109028.2018.1505

24. Rolf, S., & Schindler, S. (2023). The US-China rivalry and the emergence of state platform capitalism. *Environment and Planning A: Economy and Space*, *55*(5), 1255–1280. https://doi.org/10.1177/0308518X221146545

25. Romashkina, A.B., & Kirichuk, D.A. (2023). Politicheskaya sub»ektnost' tsifrovykh aktantov v kontekste obespecheniya tsifrovogo suvereniteta [The political subjectivity of digital actors in the context of ensuring digital sovereignty]. *Vestnik Rossiyskogo universiteta druzhby narodov. Seriya: Politologiya*, 25(4), 848–861. https://doi.org/10.22363/2313-1438-2023-25-4-848-861

26. Vakhovskiy, A.M. (2019). Suverenizatsiya Interneta kak problema sovremennogo politicheskogo protsessa [Sovereignization of the internet as a problem modern political process]. *Izvestiya Tul'skogo gosudarstvennogo universiteta. Gumanitarnye nauki*, (1), 11–18. https://doi.org/10.24411/2071-6141-2019-10101

27. Weichselbaum, L., Spagnuolo, M., Lekies, S., & Janc, A. (2016). CSP is dead, long live CSP! On the insecurity of whitelists and the future of Content Security Policy. *In Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security* (pp. 1376–1387).

28. Young, J.C. (2019). The new knowledge politics of digital colonialism. *Environment and Planning A: Economy and Space*, *51*(7), 1424–1441. https://doi.org/10.1177/0308518X19858998

29. Zhang, C., & Morris, C. (2023). Borders, bordering and sovereignty in digital space. Territory, Politics. *Governance*, *11*(6), 1051–1058. https://doi.org/10.1080/21622671.2023.2216737

Информация об авторах

Сергей Владимирович Володенков, доктор политических наук, главный научный сотрудник научно-проектного отдела Научно-инновационного управления Государственного академического университета гуманитарных наук, профессор кафедры государственной политики факультета политологии Московского государственного университета имени М.В. Ломоносова, Москва, Россия, ORCID: https://orcid.org/0000-0003-2928-6068, e-mail: s.v.cyber@gmail.com

Сергей Николаевич Федорченко, доктор политических наук, главный научный сотрудник научно-проектного отдела Научно-инновационного управления Государственного академического университета гуманитарных наук, доцент кафедры истории и теории политики факультета политологии Московского государственного университета имени М.В. Ломоносова, Москва, Россия, ORCID: https://orcid.org/0000-0001-6563-044X, e-mail: s.n.fedorchenko@mail.ru

Information about the authors

Sergey Vladimirovich Volodenkov, Doctor of Sciences (Political Sciences), Chief Researcher at the Research and Design Department of the Scientific and Innovation Department, State Academic University for the Humanities; Professor of the Department of Public Policy, Faculty of Political Science, Lomonosov Moscow State University, Moscow, Russia, ORCID: https://orcid.org/0000-0003-2928-6068, e-mail: s.v.cyber@gmail.com

Sergey Nikolaevich Fedorchenko, Doctor of Sciences (Political Sciences), Chief Researcher at the Research and Design Department of the Scientific and Innovation Department, State Academic University for the Humanities; Associate Professor of the Department of History and Theory of Politics, Faculty of Political Science, Lomonosov Moscow State University, Moscow, Russia, ORCID: https://orcid.org/0000-0001-6563-044X, e-mail: s.n.fedorchenko@mail.ru