

КАТЕГОРИЯ «ЦИФРОВОГО СУВЕРЕНИТЕТА» В СОВРЕМЕННОЙ МИРОВОЙ ПОЛИТИКЕ

ВЫЗОВЫ И ВОЗМОЖНОСТИ ДЛЯ РОССИИ

ОЛЬГА РЕБРО
АНАСТАСИЯ ГЛАДЫШЕВА
МАКСИМ СУЧКОВ
АНДРЕЙ СУШЕНЦОВ
МГИМО МИД России, Москва, Россия

Резюме

Глобальная цифровая революция привела к трансформации технологического и экономического укладов, общественных отношений и самой философии жизни человека. Трансграничный характер цифровой среды обусловил возникновение новых, глобальных угроз и вывел на повестку дня вопросы функционирования государств в условиях новой цифровой реальности, границ между национальным и международным, правил взаимодействия в Интернете и понимания «суверенитета» государства в цифровую эпоху. Настоящее исследование направлено на концептуализацию понятия «цифровой суверенитет». Кроме того, в статье мы рассматриваем эволюцию двух конкурирующих взглядов на интернет-пространство и обозначаем пути обеспечения суверенитета в условиях тотальной цифровизации. «Цифровая вседозволенность» последних трёх десятилетий существенным образом стимулировала инновации, экономическое освоение новой среды и улучшение качества жизни населения. Вместе с тем она привела к размыванию регулирующей роли государства и осложнила выполнение такой ключевой функции, как обеспечение безопасности граждан. Сегодня перед государствами стоит непростая задача: найти эффективные механизмы обеспечения суверенитета в цифровом пространстве без ущерба для положительных аспектов цифровой революции, а также выработать оптимальную глобальную архитектуру, в рамках которой будет гарантировано равноправие и безопасность всех вовлечённых сторон. В современном мире сформировались несколько подходов к определению понятия «кибербезопасность» и вариантов интерпретации категории «суверенитета», что лишь усугубляет набирающее обороты межгосударственное противостояние. Таким образом, рассматриваемая в этой работе проблема актуальна как с теоретической, так и с практической точки зрения. Цифровой технологический суверенитет государства представляет собой не только основу «цифрового лидерства», но является также необходимым условием суверенитета политического и его национальной независимости. Выбор модели организации и управления киберпространством

Исследование выполнено при финансовой поддержке РФФИ и ЗИСИ в рамках научного проекта №21-011-31278 «Компоненты лидерства в цифровой среде и стратегические приоритеты России».

Дата поступления рукописи в редакцию: 29.09.2021

Дата принятия к публикации: 29.11.2021

Для связи с авторами / Corresponding author:

Email: max.suchkov@gmail.com

в будущем будет оказывать существенное влияние на облик всей международной системы. В этой работе рассматриваются основные теоретические подходы к явлению «цифрового суверенитета»; анализируется эмпирический опыт ключевых государств и международных институтов, занятых разработкой этой проблематики, а также обосновывается необходимость создания двухуровневой системы управления глобальным киберпространством как оптимального для текущего этапа развития информационных технологий механизма разрешения проблемы цифрового суверенитета.

Ключевые слова:

цифровая среда; цифровой суверенитет; глобальное управление; цифровая конкуренция; стратегия; кибербезопасность; Россия; США; коллегиальное управление Интернетом.

Вступление мира в новый технологический уклад приводит к кардинальным трансформациям во всех сферах человеческой жизни. В то время как практическое проявление данных трансформаций мы наблюдаем в повседневности, их теоретическое осмысление пока значительно отстаёт. Сложность концептуализации происходящих изменений связана с их фундаментальным характером, отражающимся в таких наблюдениях, как «мир перестал быть человекомерным»¹ или «четырёхмерный человек» [Scott 2015]. Появление «нового измерения» или «новой реальности» обуславливает актуальность изучения меняющейся в условиях нарастающей цифровизации [Kissinger 2014; Hanelt et al. 2021; Verhoef et al. 2021] роли государства в международных отношениях, начальным прин-

ципом которых на протяжении веков выступал суверенитет.

Формирование нового технологического уклада, запущенное с появлением Интернета, до сих пор происходило под влиянием доминировавших в мире процессов глобализации². Если до середины 2010-х годов они представлялись безальтернативными, то в последующие годы динамика изменилась, что повлекло за собой переосмысление подходов к концептуализации цифрового пространства. Отсутствие государственного контроля стимулировало экономическое освоение новой среды и инновации, которые легли в основу технологий, качественно изменивших современную жизнь [Naughton 2016]. Вместе с тем она также привела к размыванию роли государства и осложнила выполнение такой ключевой

¹ «Мир перестал быть человекомерным». Татьяна Черниговская о проблемах развития искусственного интеллекта // Snob.ru. 26 февраля 2020. [Электронный ресурс]. URL: <https://snob.ru/entry/189353/> (дата обращения: 20.09.2021).

² Научное объяснение концепции технологических укладов как общественно-экономической формации происходило одновременно сразу в нескольких предметных областях, преимущественно в экономике и технологии производства (см.: Perez C. (2010). *Technological revolutions and technoeconomic paradigms*. Cambridge journal of economics, 34(1), 185–202; *Потеев А.Т.* Технологический уклад: методология оценки уровня технологического уклада отрасли / А.Т. Потеев, Т.С. Мешкова // Предприятия, отрасли и регионы: генезис, формирование, развитие и прогнозирование: Сб. научных трудов по материалам III Международной научно-практической конференции. Пермь, 31 марта 2017 года. Пермь: Научная общественная организация «Профессиональная наука», 2017. С. 161–169; *Ковальчук М.В.* Природоподобные технологии: новые возможности и новые вызовы / М.В. Ковальчук, О.С. Нарайкин, Е. Б. Яцишина // Вестник Российской академии наук. 2019. Т. 89. № 5. С. 455–465; *Косакян Н.Л.* Аддитивная технологическая совокупность 6-го технологического уклада / Н.Л. Косакян // Экономика и управление: проблемы, решения. 2021. Т. 1. № 2(110). С. 4–8; *Усков В.С.* Научно-технологическое развитие российской экономики в условиях перехода к новому технологическому укладу / В.С. Усков // Экономические и социальные перемены: факты, тенденции, прогноз. 2020. Т. 13. № 1. С. 70–86 и др.), но также и в гуманитарной сфере (см.: *Золотарёва О.А.* Гуманитарно-технологическая революция: оценка состояния готовности перехода в новый технологический уклад / О.А. Золотарёва, Е.С. Дарда, А.В. Тихомирова // Вестник НГУЭУ. 2021. № 4. С. 55–66; *Härnmarcorpi V., Haikonen A., & Kauranen I.* (2003). *The Shift of Techno-Economic Paradigm and Its Effects on Regional Disparities*).

функции, как обеспечение безопасности граждан³ [Bierwisch et al. 2015; Rainie et al. 2017]. Сегодня перед государствами стоит непростая задача: найти эффективные механизмы обеспечения суверенитета в цифровом пространстве без ущерба для положительных аспектов цифровой революции. Решением этой задачи могло бы стать сочетание принципа коллегиальности, предполагающего привлечение национальных экспертов, общественных организаций и бизнеса при разработке национального законодательства и запуск равноправного межгосударственного диалога для определения универсальных принципов взаимодействия «суверенных интернет-пространств». Формирование нового технологического уклада, запущенное с появлением Интернета, привело к утверждению тезиса об отсутствии границ в цифровом пространстве, воспринимавшемуся как аксиома. В работе данная догма переформулирована в гипотезу, состоятельность которой авторы предлагают проверить через анализ национальных подходов к использованию понятия «цифровой суверенитет», трансформаций бытовых практик использования цифровых технологий, геополитического контекста распространения Интернета и дискуссий в международных институтах о выработке общих правил межгосударственного взаимодействия в цифровом пространстве.

Настоящая статья опирается на проведённый авторами анализ научной литературы и программных документов; при этом источники структурированы в соответствии со смысловым наполнением четырёх основ-

ных блоков. В первом даётся краткая характеристика современных подходов к определению цифрового суверенитета и выявляются препятствия на пути выработки единого определения. Второй и третий разделы рассматривают два конкурирующих подхода к осмыслению Интернета и киберпространства⁴. С одной стороны, выход за рамки осязаемой реальности и глубина происходящих в результате этого социально-политических изменений породили тезис об исключительности киберпространства, которая требует кардинально новых подходов к межгосударственному взаимодействию (раздел 2). С другой — по мере повсеместного распространения Интернета, под влиянием бытовых практик жизнедеятельности человека, в большинстве своём имеющих географическую привязку, изменились и механизмы его использования, что привело к естественному появлению границ в цифровом пространстве (раздел 3). В завершающей части статьи разбираются вызовы суверенитету, характерные для цифрового пространства, с учётом двойственной природы категории «суверенитета»: как независимости государства от внешнего вмешательства и как монопольной власти на определение принципов внутреннего устройства [Jackson 1990].

Фундаментальность поставленной проблемы предполагает использование широкого набора методов. Понятие «цифровой суверенитет» рассматривается через призму конструктивистских подходов и фокусируется на различии существующих интерпретаций в зависимости от культурно-исторических традиций. Рассмотрение

³ Проблема обеспечения безопасности граждан в новую технологическую эру заботит не только исследователей и самих граждан, но также и правительства ведущих государств мира. Спектр угроз приводимых последними при этом широкий, как и само понятие «безопасность»: от расширения возможностей террористов проводить вербовку и координировать свою деятельность через социальные сети и финансирования нелегальных организаций через криптовалютные механизмы до похищения хакерами денег с личных счетов граждан и «зловредного» (malign) — в разных смыслах — контента в Интернете, доступ к которому, в частности, у детей теперь свободнее, чем прежде. Подробнее см.: (National Security Through Technology: Technology, Equipment, and Support for UK Defence and Security // UK Ministry of Defence. URL: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/27390/cm8278.pdf (дата обращения: 20.09.2021)).

⁴ В настоящей работе понятия «цифровая среда», «киберпространство» и «интернет-пространство» используются как взаимозаменяемые.

каждого из двух подходов к осмыслению цифрового пространства построено по хронологическому принципу. Методология исследования включает использование методов сравнения на основе логико-интуитивного подхода с опорой на ряд страновых доктринальных документов и документов, затрагивающих вопросы правоприменительной практики в цифровой среде. Для достижения поставленной цели был дополнительно применён метод экспертных оценок⁵, который позволил определить степень адекватности и применимости первичных гипотез авторов исследования. Последняя часть также опирается на изучение отдельных случаев (case study) для иллюстрации вызовов, стоящих перед государствами, и содержит анализ практик, используемых правительствами и уполномоченными властными органами ряда стран для разрешения проблемы регулирования цифровой среды.

Понятие «суверенитет» в цифровом пространстве

Понятие «цифровой суверенитет» прочно вошло в современный политический лексикон. Несмотря на широкое признание значимости цифрового суверенитета для функционирования современного государства, не сформировано единого подхода к определению его содержания [Никонов и др. 2021], а сам термин обладает свойством «риторической перформативности»⁶ [Кутюр, Тоупин 2020]. С одной стороны, трудности выработки единого подхода связаны с невозможностью применения традиционных инструментов, использовавшихся до сих пор для определения суверенитета: цифровое пространство не имеет географических характеристик и

в нём одновременно «соприкасаются» все государства, то есть в нём происходит бесконечная коллизия всех национальных правовых пространств одновременно. С другой — они обусловлены возрастающим влиянием цифровизации на все сферы социально-политической и экономической жизни государства. В отсутствие универсального подхода термин «цифровой суверенитет» наполняется смыслом, наиболее соответствующим традициям и национальным приоритетам различных государств. В этой связи обеспечение независимости в научных разработках, определении стандартов, безопасности физической инфраструктуры связи относится к понятию «технологический суверенитет», привлёкшему внимание исследователей ещё до распространения Интернета [Globerman 1978, Grant 1983]. Столь же повсеместно интерес исследователей привлекает силовой компонент или защита государств в информационной среде — кибербезопасность [Tikk, Kerttunen 2020].

При этом вычленяются различные акценты в понимании цифрового суверенитета в зависимости от культурно-исторических традиций отдельных регионов. Право на защиту персональных данных, собираемых и обрабатываемых с помощью цифровых технологий, определяется как «суверенитет личности в цифровом пространстве» и особенно часто упоминается применительно к дискурсу Европейского Союза [Floridi 2020; Pohle, Thiel 2020]. С подачи Пекина в оборот было введено понятие «интернет-суверенитет» — права государства устанавливать собственные правила функционирования интернет-пространства, отвечающие национальным интересам и традициям [Jiang 2010; Shen 2016].

⁵ Экспертный опрос проводился для целей настоящего исследования через Интернет в период с 15 июля до 20 августа. Участие в опросе приняли представители 5 ведущих профильных школ (преимущественно специализированные консалтинговые агентства и исследовательские университеты), которым было предложено ответить на 6 тематических вопросов о категории «цифрового суверенитета» и практиках регулирования цифровой среды.

⁶ То есть его использование обусловлено не объективным содержанием понятия, но субъективными задачами говорящего: если стратегическая задача государства — защита прав человека, то термин интерпретируется через призму «суверенитета личности», если защита от внешнего нападения — через призму кибербезопасности и суверенитета технологий и др.

В российских исследованиях значительное внимание уделяется «информационно-му суверенитету» [Ромашкина 2019; Виноградова, Полякова 2021]. При этом отличительной особенностью подхода России в международной дискуссии о цифровой среде является более широкое, чем у её контрагентов, восприятие цифровых угроз и рисков. Наряду с постулированием информационного суверенитета Россия предпочитает термин «информационная безопасность» (information security) устоявшемуся в англоязычном дискурсе понятию «кибербезопасность» (cybersecurity). Принципиальное отличие заключается в том, что информационная безопасность включает в себя не только практику защиты соответствующей инфраструктуры, технологий и данных, но также и регулирование международных информационных потоков и интернет-контента [Батуева 2014; Шариков 2018; Макарычева 2015]. Доктрина информационной безопасности Российской Федерации 2016 г. определяет, среди прочего, в качестве угроз «информационное воздействие, направленное на размывание традиционных российских духовно-нравственных ценностей» и «применение информационных технологий в целях нанесения ущерба суверенитету, территориальной целостности, политической и социальной стабильности» государства⁷. Аналогичный подход Россия использует при отстаивании своего видения проблемы цифровой безопасности на международной арене. Пример тому даёт выдвинутый в рамках ООН про-

ект Конвенции об обеспечении международной информационной безопасности⁸. Столь широкий подход Москвы к определению явления «цифровой безопасности» и «цифрового суверенитета» вызывает опасения других участников международного диалога⁹. Концептуальные различия между понятиями «кибербезопасность» и «информационная безопасность», с учётом различий в интерпретации, объясняют критику ряда государств по отношению к российским инициативам и действиям российского правительства по регулированию внутренней цифровой среды [Kozzak 2021].

На фоне сохраняющегося многообразия взглядов выделяются подходы, представляющие цифровой суверенитет не как статичный конструкт, но как продукт постоянного переосмысления в ходе взаимодействия государства и цифрового общества. В России, например, группа исследователей Московского государственного университета определила цифровой суверенитет как «эмерджентное свойство современного государства как сложной системы», возникающее в результате «сочетания технологических возможностей государства (цифровые технологии и цифровая инфраструктура) и цифровых компетенций, способностей и навыков его граждан, организаций, институтов в сфере использования цифровых ресурсов» [Володенков и др. 2021]. Эксперты из Германии отрицают возможность строгой детерминации понятия «цифровой суверенитет» с последующим законодательным закреплением норм и правил его реализа-

⁷ Доктрина информационной безопасности Российской Федерации от 5 декабря 2016 г. [Электронный ресурс]. URL: <http://static.kremlin.ru/media/acts/files/0001201612060002.pdf> (дата обращения: 20.09.2021).

⁸ Convention on International Information Security. The Ministry of Foreign Affairs of the Russian Federation. 2011. [Электронный ресурс]. URL: https://www.mid.ru/en/foreign_policy/official_documents/-/asset_publisher/CptlCkBBZ29/content/id/191666 (дата обращения: 20.09.2021).

⁹ В качестве примера можно привести принятие ГА ООН российской резолюции «Противодействие использованию информационно-коммуникационных технологий в преступных целях», в ходе голосования по которой против высказались США и страны ЕС. Российская резолюция стала альтернативой продвигавшейся до этого момента западными странами Будапештской конвенции Совета Европы в качестве ключевого инструмента противодействия преступности с использованием информационных технологий. Россия не присоединилась к Будапештской конвенции, так как согласно статье 32 данного документа в целях противодействия киберпреступности государства-участники получают возможность «трансграничного доступа к компьютерным данным», что с российской точки зрения противоречит принципу государственного суверенитета.

ции, равно как и необходимость подобного закрепления, и в этой связи руководствуются тезисом о необходимости выработки адекватных моделей взаимодействия государств и акторов в цифровой среде — удобной и приемлемой для всех вовлечённых сторон [Pohle, Thiel 2020].

Сложности в выработке единого подхода при осмыслении государства в цифровом пространстве связаны с характеристиками самой среды.

Во-первых, впервые новое пространство межгосударственных взаимодействий появилось не в результате получения человеком возможностей по его освоению, а было создано самим человеком [Касенова, Демидов 2013]. В отличие от морской, воздушной и космической среды цифровое пространство не статично, но развивается вместе с технологическим прогрессом и под влиянием социально-экономических и политических процессов.

Во-вторых, привычные социально-политические процессы происходят в нём по другим законам [Choucri 2012]. В киберпространстве информация распространяется мгновенно, географические и физические преграды отсутствуют, равно как не существуют такие политические конструкторы, как юрисдикции и государственные границы. Субъектами в нём выступают не физические люди, а их «цифровые аналоги» или «цифровые личности» [Vesali Naesh 2016], логика взаимодействия которых, в условиях сложности атрибуции действий и привлечения к ответственности за совершённое, отличается от реального мира. Это, в свою очередь, снижает барьеры для политического участия, а также ломает привычную иерархию, уравнивая индивидов, компа-

нии, общественные организации, неформальные группы и государственные институты. Если предыдущее освоение новых сред сопровождалось адаптацией существующих принципов взаимодействия под новые условия, то создание кардинально нового пространства увеличило соблазн переосмысления данных принципов.

В-третьих, цифровая среда — это относительно новое явление. Появившаяся и получившая широкое распространение только в последние тридцать лет, она развивалась в регулятивной среде, где доминировали идеи экономического либерализма и глобализации, а правила устанавливала единственная сверхдержава — Соединённые Штаты. В этом плане показательным, что в США понятие «цифровой суверенитет» зачастую имеет негативную коннотацию [Кутюр, Тоупин 2020] и ассоциируется с авторитаризмом¹⁰, даже несмотря на то, что необходимость регулирования цифрового пространства начали осознавать и американские законодатели¹¹. С этой точки зрения подходы к осмыслению проблематики цифрового суверенитета нельзя рассматривать в отрыве от процессов мирового развития, где попытки стран заявить о своей независимости в интернет-среде выражают отказ от легитимизации американской гегемонии [Mainwaring 2020].

От киберисключительности к коллегиальному управлению Интернетом

Трансформации социальных взаимодействий, вызванных появлением Интернета, стимулировали спекуляции о появлении качественно новой среды, существующей по особым законам. Наиболее ярко тезис киберисключительности¹² был заявлен

¹⁰ Knake R.K. The Beginning of the End of the Open Internet Era // Council on Foreign Relations. January 6, 2020. URL: <https://www.cfr.org/blog/2019-beginning-end-open-internet-era> (дата обращения: 20.09.2021).

¹¹ Bartz D. Breaking up Big Tech in focus as new U.S. antitrust bills introduced // Reuters. June 11, 2021. URL: <https://www.reuters.com/technology/us-house-lawmakers-introduce-bipartisan-bills-target-big-tech-2021-06-11/> (дата обращения: 20.09.2021).

¹² Термин «киберисключительность» широко используется в научной литературе и исследованиях по тематике киберпространства. В данной статье авторы рассматривают его в увязке с проблемой цифрового суверенитета. Соответственно, под киберисключительностью подразумевается подход, отрицающий право государств на установление порядка в цифровом пространстве.

в Декларации независимости киберпространства, выдвинутой Джоном Барлоу в 1996 году. Документ призвал лидеров индустриального мира «оставить в покое» новое «глобальное социальное пространство», в котором нет суверенитета и авторитетов, а у государств «нет ни морального права, ни методов для принуждения»¹³. Эта идея получила широкое распространение среди теоретиков международного права, указавших, что применение национального законодательства к «внегеографическим» действиям либо не имеет смысла, либо ведёт к бесконечному количеству правовых коллизий [Hardy 1994; Johnson and Post 1996]. Исследователями-международниками новая среда трактовалась как ещё одно проявление процессов глобализации, ускоряющее уже наметившееся размывание суверенитета, укрепление неправительственных институтов и актуализацию запроса на межгосударственное взаимодействие [Perritt 1998; Scholte 2000].

Постепенно идея киберисключительности, отказывавшая государствам в праве установления порядков в цифровом пространстве, трансформировалась в менее конфронтационный подход коллегиального управления Интернетом (multi-stakeholder internet governance). Он предполагал развитие регулирования на базе международного форума, где «государства, частный сектор и гражданское общество» выступали бы на равных¹⁴. При этом концепция коллегиального управления Интернетом

основывалась на тезисе об особом характере цифрового пространства, в котором ни один игрок не обладает монополией на установление правил [Doria 2013]. Тем не менее история становления основных институтов, воплощающих эту коллегиальность — Корпорации по управлению доменными именами и IP-адресами (ICANN), Инженерного совета Интернета (IETF) и Форума по управлению Интернетом (IGF) — представляет собой скорее «медленную и молчаливую капитуляцию международного режима» перед «глобальным управлением», правила которого устанавливались единственной на тот момент сверхдержавой [Hill 2014].

По мере коммерциализации Интернета в первой половине 1990-х годов контроль над реестром доменных адресов, прежде реализуемый разработчиками-сотрудниками Стэнфордского исследовательского института, консолидировался в руках субподрядчика Пентагона и перешел к Networks Solution (NSI), позже приобретенной Science Application International Corporation [Mueller 2009]¹⁵.

Не желая допускать превращение Интернета из общественного блага в инструмент государственной власти и способ обогащения корпораций, техническая элита сформировала движение за независимое управление Интернетом с планами создания соответствующего международного органа со штаб-квартирой в Швейцарии¹⁶. Администрация Уильяма Клинтона опасалась,

¹³ Barlow J.P. A Declaration of the Independence of Cyberspace // Duke Law & Technology Review. 2019. No. 5(7). URL: <https://www EFF.org/cyberspace-independence> (accessed: 20.09.2021).

¹⁴ Report of the Working Group on Internet Governance. Château de Bossey: Working Group on Internet Governance. 2005. [Электронный ресурс]. URL: <http://www.wgig.org/docs/WGIGREPORT.pdf> (accessed: 20.09.2021).

¹⁵ 'The cooperative agreement between the National Science Foundation and Network Solutions (NSI) for registration services was concluded just months before the Web's sudden transformation of domain names. Neither party to the transaction had any idea of what was in store for them... NSF held consultative discussions on charging for domain names, and an expert advisory panel brought in to evaluate the performance of the InterNIC contractors concluded in a December 1994 report that Network Solutions should "begin charging for .COM domain name registrations, and later charge for name registrations in all domains". Shortly after the decision to charge was made, a multibillion-dollar Washington-area defense contractor, Science Applications International Corporation (SAIC), purchased Network Solutions'.

¹⁶ В 1997 г. по инициативе Общества Интернета была создана международная рабочая группа Международный чрезвычайный комитет (International Ad Hoc Committee — IAHC), куда была приглашена технологическая элита (ключевая фигура — Джон Постел), заинтересованные международные

что привлечённые к этому процессу международные организации, такие как Международный союз электросвязи, пойдут по пути ограничения свободы экономической деятельности, и в 1997–1998 годах Вашингтон фактически пресёк такие попытки, в том числе посредством прямых угроз лишения финансирования и уголовного преследования лидеру движения — Джону Постелу [Goldsmith, Wu 2006]. Подавив мятеж Дж. Постела в январе 1998 года, американская администрация пошла на создание ICANN. Формально коллегиальная и неправительственная корпорация по сей день находится в Калифорнии и подчиняется законодательству США. Хотя правительство Соединённых Штатов подчёркивает независимость организации, Вашингтон «имеет многочисленные каналы доступа и давления» и «выступает посредником между разрозненными интересами» участников управления Интернетом с целью «сокращения политических противоречий и недопущения передачи слишком большого контроля международным органам» [Mueller 2002].

Таким образом, чтобы закрепить либерально-экономические принципы при регулировании Интернета — что предполагает минимальный контроль со стороны государства, — власти США взяли на себя роль «гаранта свободы» цифрового пространства, фактически превратив коллегиальное управление Интернетом в один из институтов собственного мирового лидерства.

Впоследствии предпринимались неоднократные попытки вернуться к по-настоящему международному коллегиальному управлению. Например, в ходе тунисского этапа Всемирной встречи на высшем уровне по вопросам информационного обще-

ства (WSIS) в 2005 г. ряд государств выступили с инициативой увеличения интернационализации на межправительственной основе посредством создания международной платформы для разработки общих принципов, обязательных для ICANN. Эта инициатива не получила широкой поддержки из-за оппозиции США. В результате созданный по результатам тунисского процесса в рамках ООН Форум по управлению Интернетом (IGF) не получил мандата на принятие обязательных к исполнению документов [Касенова, Демидов 2013].

Следующая серьёзная попытка реформы коллегиального управления была предпринята после разоблачений Эдварда Сноудена. Выступая на созванной по этому поводу конференции NETmundial в апреле 2014 года, президент принимающей страны Бразилии Дилма Русефф призвала уравнять все государства с тем, чтобы «ни одна страна не имела большего влияния по сравнению с другими»¹⁷. Хотя существенных реформ не последовало, этот призыв дал толчок для множественных национальных инициатив по регулированию Интернета.

Коллегиальное управление Интернетом по-прежнему является центральным принципом международных инициатив. Запущенный в 2019 г. процесс ООН по реформе текущей архитектуры управления Интернетом учитывает распространённую в экспертной среде критику [Carr 2015] и предлагает три варианта реформы: (a) IGF Plus: совершенствование Форума по управлению Интернетом за счёт увеличения представительства и большей интеграции в систему ООН; (b) распределённая архитектура управления: при централизации выработки единых норм их практическая реализация

организации (Всемирная организация интеллектуальной собственности, Международная ассоциация товарных знаков, а позже присоединился Международный союз электросвязи), представители американского правительства (им стал Джордж Строн из Национального научного фонда США) с целью разработки меморандума об управлении доменными адресами, который бы ограничил закрепившуюся к тому времени монополию Network Solutions.

¹⁷ Dilma Rouseff, Speech opening the NETmundial meeting in Brazil on 23 April 2014, pp. 7–8. [Электронный ресурс]. URL: <https://netmundial.br/wp-content/uploads/2014/04/NETMundial-23April2014-Dilma-Rousseff-Opening-Speech-en.pdf> (accessed: 20.09.2021).

и надзорные функции передаются национальным правительствам; и (с) архитектура общего цифрового пространства: распределение цифровой повестки между существующими организациями ООН и координация их деятельности на регулярной основе¹⁸.

Ориентация на привлечение экспертов, частных компаний и общественных организаций для определения правил функционирования цифрового пространства небезосновательна, учитывая техническую сложность и тотальное влияние цифровизации на все сферы человеческой жизни [Kello 2017]. Тем не менее делегирование отдельных направлений управления этой средой негосударственным игрокам должно быть осознанным решением правительств, в противном случае происходит ошибочное пренебрежение ролью государства. Это стимулирует обратный процесс: для реализации стратегических интересов государство начинает использовать имеющиеся у него инструменты национального регулирования и искать наиболее удобные форматы международного взаимодействия, что в итоге ведёт к дроблению единого интернет-пространства [Drezner 2004].

От киберобыденности к национальному регулированию¹⁹

Хотя идея киберисключительности по-прежнему обладает существенным весом в экспертной литературе [Mueller 2019; Bremmer 2021], с конца 1990-х годов последовательно утверждается альтернативный взгляд на цифровое пространство как очередной этап развития информационно-коммуникационных технологий: «подобно телефону, телеграфу, дымовым сигналам, Интернет является инструментом, с помощью которого реальные люди в определённом правовом пространстве общаются

с другими реальными людьми в другом правовом пространстве» [Goldsmith 1998]. При этом кибероружие, принуждая государства к изменению тактики войны и поиску ответа на новые вызовы, не привело к перераспределению баланса сил в мире и дополнило, но не заменило традиционную военную мощь [Kello 2017; Suchkov 2021]. Анархия цифровой среды в первой половине 1990-х годов в рамках этого подхода воспринимается как временное явление, вызванное инерционным характером государственного управления, которое только во второй половине десятилетия всерьёз озабочилось регулированием цифрового пространства [Wu 1997].

Со временем аргументы в пользу второй точки зрения добавила сама логика трансформации интернет-практик: частные компании-лидеры цифровой индустрии сами, без государственного вмешательства, пришли к необходимости локализации своей деятельности [Goldsmith, Wu 2006].

На ранних этапах развития Интернет использовал ограниченный круг людей по всему миру для коммуникации друг с другом. Он действительно стирал государственные границы и сокращал расстояния внутри этой узкой группы. По мере превращения глобальной сети в объект обыденной жизни и роста числа пользователей, бытовые нужды которых имеют географическую привязку, начала происходить и локализация интернет-услуг. На сайтах появились опции выбора языка, а указав географическое место, пользователь получал возможность посмотреть актуальный прогноз погоды, курсы обмена валюты его страны, адаптированные под конкретный регион новостные ленты. Эта тенденция проявилась и в языковой диверсификации Интернета. Если в конце 1990-х годов 80% размещённых материалов были на англий-

¹⁸ The Age of Digital Interdependence. Report of the UN Secretary-General's High-level Panel on Digital Cooperation. 2019. P. 24–26. [Электронный ресурс]. URL: <https://www.un.org/en/pdfs/DigitalCooperation-report-for%20web.pdf> (accessed: 20.09.2020).

¹⁹ Термин «киберобыденность» в данном контексте используется как антоним концепции «киберисключительности». Если последняя предполагает отсутствие у государств права установления порядка в цифровом пространстве ввиду «исключительного» характера данного пространства, то «киберобыденность» рассматривает цифровую среду как сферу, подверженную регулированию.

ском²⁰, то в 2002 г. этот показатель опустился ниже 50% [Crystal 2004]. В 2020 г. английский был родным только для 25,9% пользователей, а по распространённости его почти догнал китайский (19,4%)²¹. К тому же исследования географии интернет-трафика ещё в начале 2000-х показывали обратную зависимость плотности информационных обменов от расстояния, а также их концентрацию вокруг урбанистических центров [Goodchild 2001].

Аналогичная динамика наблюдается во всех новых отраслях цифровой экономики. Интернет-торговля, позиционируемая как возможность покупать товары у производителя в любой части света, эволюционировала в сторону размещения складов вблизи потребителей, что отчётливо демонстрирует эволюция стратегии компании Amazon²². Бизнес-логика телекоммуникационных компаний стимулирует инвестиции в регионы с большей концентрацией потребителей, что, в свою очередь, привлекает в мегаполисы предприятия, функционирование которых напрямую зависит от стабильности подключения и скорости передачи данных. То есть качество подключения также имеет географическую привязку. Рост таргетированной рекламы как способа монетизации интернет-платформ стимулировал развитие технологии определения геолокации, и современные интернет-сайты автоматически выдают контент в зависимости от расположения пользователя.

Такая нормализация и географическая привязанность Интернета позволяет использовать уже разработанные принципы международного регулирования экономи-

ческой деятельности и борьбы с преступностью в цифровом пространстве. Например, отталкиваясь от опыта борьбы национальных государств с контрафактной продукцией, Дж. Голдсмит и Т. Ву отмечают, что, подобно цепочке сбыта такого товара, состоящей из производителя подделки, продавца и потребителя, использование Интернета также можно разделить на «источник» (функционирующий в соответствии с международными нормами, а значит, наднациональный), «посредника» (компании, предоставляющие услуги связи, а также транснациональные интернет-платформы и технологические гиганты) и «потребителя» (конкретных людей, привязанных к территории и правовому полю конкретного государства). В то время как государство может в теории таргетировать все три элемента, на практике борьба с производителем (источником) и потребителем, с одной стороны, слишком ресурсоёмка, с другой — юридически спорна. В таких условиях наиболее эффективным методом является ограничение деятельности посредников [Goldsmith, Wu 2006].

В случае с Интернетом посредников можно разделить на два типа: глобальные и национальные. Последние уже вынуждены подчиняться национальному регулированию. В частности, именно на это был направлен так называемый закон «о суверенном Интернете» 2019 г. в России, предписывающий операторам связи установить специальные устройства для маршрутизации интернет-трафика²³. С первыми ситуация обстоит несколько сложнее. Учитывая трансграничный характер интернет-среды, цифровой продукт транснациональной

²⁰ Wallraff B. What Global Language? // The Atlantic. November 2000. URL: <https://www.theatlantic.com/magazine/archive/2000/11/what-global-language/378425/> (accessed: 20.09.2021).

²¹ Internet World Users by Language. Internet World Stats. [Электронный ресурс]. URL: <https://www.internetworldstats.com/stats7.htm> (accessed: 20.09.2021).

²² Leonard M. 5 Charts Show Amazon's Growing Logistics Network as It Puts Inventory Closer to Consumers // Supply Chain Dive. August 2, 2021. URL: <https://www.supplychaindive.com/news/amazon-ecommerce-warehouse-fulfillment-capital-investment/603731/> (accessed: 20.09.2021).

²³ Федеральный закон от 1 мая 2019 г. № 90-ФЗ «О внесении изменений в Федеральный закон «О связи» и Федеральный закон «Об информации, информационных технологиях и о защите информации» // Российская газета. URL: <https://rg.ru/2019/05/07/fz90-dok.html> (дата обращения: 20.09.2021).

компания становится объектом регулирования всех стран одновременно. Чтобы избежать возможных юридических осложнений, у корпорации есть два варианта действий: либо выполнять все требования — что отразится на качестве продукта, — либо использовать технологии геолокализации и диверсифицировать выпускаемый продукт, исходя из норм конкретного рынка.

Последние пятнадцать лет показали практическое развитие Интернета именно во втором направлении. Twitter в Пакистане модерирует контент в соответствии с местными обычаями, а Microsoft, имеющий офис в Марокко, в своих местных материалах и продуктах отмечает территорию Западной Сахары в соответствии с нормами Рабата, в то время как Google, не имеющий такого офиса, — как спорную²⁴. Западные интернет-компании, голливудские продюсеры и даже Национальная баскетбольная лига оказались перед выбором: потерять доступ к прибыльному китайскому рынку или выполнять устанавливаемые государством требования²⁵.

Хотя каждый из этих случаев вызывает критику на Западе, а любые новые попытки обязать интернет-платформы действовать по национальным законам получают клеймо «авторитарных», практическая логика превращения Интернета в инструмент повседневной жизни предопределяет и трансформацию IT-гигантов из определителей правил Интернета в обычные ТНК, тщательно соблюдающие национальные нормы и традиции. Таким образом, Интернет и цифровые технологии действительно создают новое пространство, обладающее специфическими характеристиками. Вместе с тем оно естественным образом адаптируется под бытовые нужды человека, имеющие локаль-

ную привязку. В таких условиях речь идёт не столько об «умирании» государственного суверенитета, сколько о необходимости поиска инструментов обеспечения суверенитета в новых — цифровых — условиях.

Два уровня цифрового суверенитета

При всём многообразии подходов к концептуализации понятия «суверенитет», в его основе лежит необходимость определения правил поведения на международной арене, для чего происходит отделение «внешнего» от «внутреннего». Подобно правилам общественного поведения, согласно которым свобода человека заканчивается там, где начинается свобода другого, суверенитет государства можно разделить на «негативный» (свобода *от* внешнего вмешательства) и «позитивный» (свобода *на* самостоятельное определение внутреннего устройства) [Jackson 1990].

По мере того как повседневное использование Интернета увеличивает географическую обусловленность процессов в цифровом пространстве, фундаментальные особенности этой среды формируют комплекс новых проблем для обеспечения государственного суверенитета в обоих аспектах. Сложность обеспечения «негативного» суверенитета в цифровой среде связана с появлением новых киберинструментов внешнего вмешательства, расширением каналов проникновения и сложностью атрибуции вредоносных действий.

Наиболее уязвима для внешнего вмешательства критическая информационная инфраструктура, что отражено в Доктрине информационной безопасности Российской Федерации, ставящей обеспечение бесперебойного функционирования информационной инфраструктуры на второе

²⁴ York J.C. The Myth of a Borderless Internet // The Atlantic. June 3, 2015. URL: <https://www.theatlantic.com/technology/archive/2015/06/the-myth-of-a-borderless-internet/394670/> (accessed: 20.09.2021).

²⁵ См.: McMahon R. Bennett I. U.S. Internet Providers and the 'Great Firewall of China'. URL: <https://www.cfr.org/background/us-internet-providers-and-great-firewall-china> (accessed: 20.09.2021); Davis D.W. Modern Chinese Literature and Culture. Vol. 26. No. 1 (Spring, 2014). P. 191–241 (51 pages); Perper R. China and the NBA are coming to blows over a pro-Hong Kong tweet. Here's why. URL: <https://www.businessinsider.com/nba-china-feud-timeline-daryl-morey-tweet-hong-kong-protests-2019-10> (accessed: 20.09.2021).

место в перечне интересов²⁶. Повсеместное проникновение в повседневную жизнь цифровых технологий, с одной стороны, повышает важность информационной системы для всех аспектов государственного развития, с другой — делает объектами информационной инфраструктуры практически всё. В результате увеличивается число точек входа в системы, обеспечивающие безопасность, экономическую деятельность и обмен информацией в цифровом пространстве, а следовательно, её уязвимость.

Сегодня в мире насчитывается более 21 млрд подключённых к Интернету устройств. Ожидается увеличение данного показателя к 2025 г. в два раза. В то время как только в 2019 г. количество киберпреступлений с помощью таких устройств выросло на 300%, их раскрываемость в США остаётся на уровне 0,05%, а, по прогнозам компании Cybersecurity Ventures, потери от киберпреступлений в 2021 г. должны были достичь 6 трлн долларов, что сопоставимо с размерами третьей экономики мира²⁷.

Рост числа субъектов цифрового пространства увеличивает многообразие мотивов их поведения. Если киберпреступники не только не скрывают, но иногда, как, например, в случае с кибератакой на американский трубопровод *Colonial Pipeline*, специально подчёркивают цель незаконного обогащения²⁸, то цифровизация социально-экономических отношений и подмена физических субъектов их цифровыми аналогами создаёт серую зону для манипуляции как в политических целях, так и для получения выгоды. Ярким примером является вопрос так называемого российского

вмешательства в американские выборы. В то время как с 2016 г. различные политические силы в США эксплуатировали тему предполагаемого подрыва Россией американской демократии, отдельные исследования указывали, что использование горячих информационных поводов выступает типичным способом заработка на количестве «переходов по ссылке» (clickbait capitalism) [Howard 2018].

Данный пример иллюстрирует важность вопроса атрибуции для межгосударственных отношений. Современные технологии пока не позволяют точно определить источник киберинцидента: даже в случае уверенности в местоположении конкретного исполнителя невозможно сказать, действовал ли он самостоятельно или по заданию государственных служб, преследовал ли цель незаконного обогащения или проводил научный эксперимент, или вовсе инцидент был устроен специально таким образом, чтобы подставить какую-либо страну и спровоцировать эскалацию конфликта в отношениях.

В мировой практике имеется опыт предотвращения подобных ситуаций посредством создания компетентных экспертных институтов, способных проводить беспристрастное расследование и устанавливать факты произошедшего. Однако технологии цифровой судебной экспертизы не дают гарантии беспристрастности оценки полученных улик, а сами международные организации, занимающиеся расследованиями и установлением фактов, как показывает пример Организации по запрещению химического оружия²⁹, могут подвергаться политическому давлению.

²⁶ Доктрина информационной безопасности Российской Федерации от 5 декабря 2016 г. [Электронный ресурс]. URL: <http://static.kremlin.ru/media/acts/files/0001201612060002.pdf> (дата обращения: 20.09.2021).

²⁷ The Global Risks Report 2020. World Economic Forum. P. 63. [Электронный ресурс]. URL: http://www3.weforum.org/docs/WEF_Global_Risk_Report_2020.pdf (accessed: 20.09.2021).

²⁸ Menn J., Satter R. Pipeline hackers say their aim is cash, not chaos // Reuters. May 10, 2021. URL: <https://www.reuters.com/business/energy/statement-suspected-us-pipeline-hackers-say-they-dont-want-cause-problems-2021-05-10/> (accessed: 20.09.2021).

²⁹ См.: Постпред РФ: ОЗХО превращается в инструмент политического давления на неугодные страны // ТАСС. URL: <https://tass.ru/politika/11223473> (дата обращения 20.09.2021); Chemical weapons watchdog defends Syria report after leaks // The Guardian. URL: <https://www.theguardian.com/world/2019/nov/25/chemical-weapons-watchdog-opcw-defends-syria-report-after-leaks> (accessed: 20.09.2021).

Не меньше проблем возникает в установлении «позитивного» цифрового суверенитета при определении правил регулирования киберпространства внутри страны. Возрастающая цифровизация ведёт к росту накапливаемых данных, которые можно разделить на две категории: персональные данные и большие данные [Nadkarni, Prügl 2021]. В то время как не существует единых международных стандартов в области обращения с такими сведениями, страны идут опытным путём, опираясь на устоявшиеся культурные и экономические практики. Например, в США и личные данные, и большие данные активно используются в коммерческих и политических целях, а компании фактически вынуждают пользователей под угрозой непредоставления услуг давать на это разрешение. Не в коммерческих, но в политических целях массовый сбор персональных данных происходит в Китае, где существуют строгие нормы деанонимизации пользователей в Интернете. В ЕС, напротив, был создан крайне рестриктивный режим. Действующий с 2018 года «Общий регламент защиты персональных данных»³⁰ ограничивает возможности компаний по сбору информации, запрещает длительное хранение данных, а также предполагает «право на забвение».

Увеличение объёмов данных, предоставляемых сознательно или в виде так называемого цифрового следа³¹, и сокращение свободы в Интернете в результате регулирования цифровой среды неизбежны. В условиях повсеместной цифровизации избежать предоставления данных можно только при отказе от использования новых технологий и цифровых продуктов, а значит, и от получаемого благодаря им повышения производительности

труда и удобств быта. При этом поддерживать безопасность населения (одна из ключевых функций государства) невозможно без ограничения «цифровой вседозволенности»³². Как металлоискатели в аэропортах и при входе на массовые мероприятия стали привычной практикой во многих странах, так же общество будет вынуждено принять новую реальность. Вместе с тем государства стоят перед необходимостью поиска правильного баланса между обеспечением безопасности, защитой прав граждан и эффективным использованием цифровых технологий для экономического развития. Ключом к такому балансу может стать создание атмосферы доверия в цифровой среде.

Показательным в этом плане может быть пример Эстонии, где в систему электронного правительства встроен принцип деанонимизации факта использования данных. Доступ к персональным данным открыт для компетентных государственных служб и компаний, но каждый факт обращения к реестрам фиксируется, и гражданин может проверить, кто и для каких целей использовал его персональную информацию. Эта система гарантирует прозрачность и саморегулирование цифровой среды без ущерба для экономики: граждане, имея возможность контролировать использование своих данных, более склонны их предоставлять, а государственные учреждения и компании более осмотрительны в их использовании [Priisalu, Ottis 2017].

Таким образом, обеспечение цифрового суверенитета должно быть направлено на решение одновременно двух задач: обеспечение безопасности от внешнего вмешательства при создании сбалансированной системы регулирования социально-экономических отношений в киберпространстве.

³⁰ Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance). URL: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32016R0679> (accessed: 20.09.2021).

³¹ Цифровой след — это уникальный набор действий в Интернете или на цифровых устройствах.

³² Под «цифровой вседозволенностью» подразумевается отсутствие государственного контроля в цифровом пространстве.

Последнее невозможно обеспечить без участия неправительственных субъектов, то есть коллегиального управления Интернетом. При этом привлечение иностранных игроков фактически означает передачу части суверенитета. В то время как в мире имеются примеры успешного функционирования государств в условиях частичного отказа от самостоятельности (Япония, Германия), в России под влиянием богатого опыта международных конфликтов сложилось устойчивое и, на наш взгляд, небезосновательное убеждение³³, что передача даже части элементов суверенитета может подорвать выживаемость страны. В этом плане можно ожидать, что дорожащие суверенитетом державы предпочтут разделять коллегиальное управление с национальными негосударственными субъектами, а значит, может сложиться двухуровневая структура: коллегиальное управление внутри страны и взаимодействие суверенных цифровых пространств на международной арене.

Подчёркнуто самостоятельная внешняя политика России вызывает неприятие у большинства западных стран, но в целом укрепила позиции страны в качестве ответственного и надёжного участника мировой политики. Эта репутация может служить заделом для лидерства Москвы в вопросах формирования международной архитектуры управления цифровым пространством. Россия в последние годы активно участвует в работе ряда международных структур, где происходит выработка новых моделей регулирования цифровой среды. Российский вклад в этой области связан с тремя ключевыми направлениями: инициированием Конвенции об обеспечении между-

народной информационной безопасности³⁴, обновлённый вариант которой был представлен в июне 2021 года; участием в Форуме по управлению Интернетом (IGF) на уровне национальных инициатив при поддержке ICANN³⁵; деятельностью в рамках Первого и Третьего комитетов Генеральной Ассамблеи ООН, в том числе в Рабочей группе открытого состава (Open-ended Working Group) и Группе правительственных экспертов (Group of Governmental Experts), учреждённой в соответствии с резолюцией ГА ООН 73/266 с целью поощрения ответственного поведения государств в киберпространстве в контексте международной безопасности.

Помимо страновой специфики, категории «цифрового суверенитета» на позицию России при выстраивании международного диалога влияет и свойственное российской стратегической культуре понимание безопасности. Цифровая (информационная) безопасность в видении России предполагает автономность от внешних субъектов не только в части технической составляющей, но и в части содержания потребляемого контента. Угрозы цифровой безопасности отождествляются с угрозами суверенитету страны. С одной стороны, такое широкое понимание проблемы, укorenившееся в национальном дискурсе и лоббируемое на международной арене, отражает стратегическое видение Москвы, заключающееся в поступательном продвижении на мировой арене идей суверенности в том числе в цифровом пространстве. С другой стороны, оно служит препятствием в деле наращивания международной кооперации.

³³ Путин заявил, что глобальные цифровые платформы – эфемерность // Газета.Ру. URL: https://www.gazeta.ru/politics/news/2021/10/21/n_16728661.shtml (дата обращения: 20.09.2021); Подписаны соглашения о намерениях между Правительством и крупнейшими компаниями о развитии отдельных высокотехнологичных направлений // Официальный сайт Президента Российской Федерации. URL: <http://kremlin.ru/events/president/news/60971> (дата обращения: 20.09.2021).

³⁴ Developments in the field of information and telecommunications in the context of international security // UN Office for Disarmament Affairs. [Электронный ресурс] URL: <https://www.un.org/disarmament/ict-security/> (accessed: 20.09.2021).

³⁵ Одиннадцатый российский форум по управлению Интернетом (RIGF 2021) пройдёт 7–9 апреля 2021 г. // Russian Internet Governance Forum. [Электронный ресурс] URL: <https://rigf.ru/about/> (дата обращения: 20.09.2021).

Ввиду отсутствия у российских высокотехнологичных компаний опыта создания комплексных платформенных решений [Bezrukov et al. 2021], России по-прежнему необходимо более широко интегрироваться в процесс глобального диалога по проблематике регулирования Интернета и цифровых технологий как по линии ООН, так и другим релевантным каналам. Инициативы за рамками ООН могут обсуждаться при участии либо широкого круга государств (в форме дискуссионной площадки, с целью повышения транспарентности российской цифровой политики), либо в более узком кругу участников, которые разделяют ценность цифрового суверенитета. В случае реализации второго варианта — вовлечения узкого круга государств в переговорный процесс — его полезность могла бы быть вызвана соображениями обмена технологиями и опытом существования в условиях нарастающей цифровой американо-китайской дуополии в цифровой среде.

В России с конца 2000-х годов активно создаются правовые и технологические основы суверенного цифрового пространства. Была создана национальная система доменных имён и национальная система маршрутизации интернет-трафика, операторам связи было предписано устанавливать государственное оборудование на точках обмена трафиком для его анализа и фильтрации при законодательном регулировании подобных мер³⁶, предприятия государственного сектора переводятся на российское программное обеспечение. Эти меры были предприняты не столько в целях создания конкурентоспособной с западными аналогами цифровой среды, сколько для гарантий национальной безопасности. В то же время одно только законодотворчество не способствует созданию атмосферы доверия. Оптимальным механизмом для реализации данной задачи могло бы стать привлечение к процессу внутреннего регу-

лирования цифровой среды национальных лидеров отрасли (создание института коллегиального управления на национальном уровне), с одной стороны, и выработка проекта международной архитектуры управления Интернетом, который мог бы гарантировать равноправие всех сторон на международном уровне, с другой стороны.

* * *

Пробуждение национального цифрового самосознания, происходящее в начале 2020-х годов, отражает естественный процесс определения государствами своей роли в условиях, заданных технологической революцией. Этот поиск далёк от завершения, но уже на современном этапе отчётливо наблюдается различие национальных подходов к определению принципов функционирования цифрового пространства (что показывают множественные интерпретации самого понятия «цифровой суверенитет»), а также готовность, казалось бы, растворившихся в глобальном мире государств отстаивать право на самостоятельное определение данных принципов.

Интернет, которому было суждено появиться на свет в условиях расцвета либеральной модели, долгое время сохранял иллюзию внегеографического пространства. В реальности он подпитывался интересами США, у которых была — и отчасти остаётся — монополия на определение правил киберсреды. Тем не менее по мере сокращения американского влияния, укрепления незападных центров силы, а также всё более чёткого проявления негативных сторон глобализации начался процесс государственного огораживания отдельных сегментов цифрового пространства при одновременной выработке общих принципов его функционирования.

Такие особенности нового пространства, как тотальность цифровизации, накопление объёмов данных и оптимизация мето-

³⁶ Федеральный закон от 1 мая 2019 г. № 90-ФЗ «О внесении изменений в Федеральный закон “О связи” и Федеральный закон “Об информации, информационных технологиях и о защите информации”». [Электронный ресурс]. URL: <https://rg.ru/2019/05/07/fz90-dok.html> (дата обращения: 20.09.2021).

дов их обработки, растущая привязка цифрового аналога объекта к его физическому оригиналу являются общими для всех государств и скорее подталкивают их к диалогу о поиске механизмов институционализации цифровых отношений. Эти процессы сочетаются с необходимостью сокращать влияние иностранных негосударственных игроков на внутригосударственные процессы, что и предусмотрено в современной модели коллегиального управления Интернетом. Впрочем, её инклюзивный характер проявил себя в качестве весьма действенного механизма по эффективному

использованию экономического потенциала и выстраиванию доверительной атмосферы между всеми участниками цифрового пространства.

В таких условиях оптимальной архитектурой для обеспечения цифрового суверенитета может стать двухуровневая система, в рамках которой в международной среде будет вестись диалог суверенных пространств, а внутри стран будет выстроена система коллегиального управления, в рамках которого роль государства будет зависеть от сложившихся социально-культурных традиций.

Список литературы

- Батуева Е.В. Информационные войны США: к определению национальной киберстратегии // Международные процессы. 2014. Т. 12. № 1–2. С. 117–127.
- Виноградова Е.В., Полякова Т.А. О месте информационного суверенитета в конституционно-правовом пространстве современной России // Правовое государство: теория и практика. 2021. Т. 17. №1. С. 32–49.
- Володенков С.В., Воронов А.С., Леонтьева Л.С., Сухарева М. Цифровой суверенитет современного государства в условиях технологических трансформаций: содержание и особенности // Полилог/ Polylogos. 2021. № 5(1). URL: <https://polylogos-journal.ru/s258770110014073-2-1/> (дата обращения: 20.09.2021).
- Золотарёва О.А. Гуманитарно-технологическая революция: оценка состояния готовности перехода в новый технологический уклад / О.А. Золотарёва, Е.С. Дарда, А.В. Тихомирова // Вестник НГУЭУ. 2021. № 4. С. 55–66.
- Касенова М.Б., Демидов О.В. Кибербезопасность и управление интернетом: Документы и материалы для российских регуляторов и экспертов. М.: Статут, 2013. 465 с.
- Ковальчук М.В., Нарайкин О.С., Яцишина Е.Б. Природоподобные технологии: новые возможности и новые вызовы // Вестник Российской академии наук. 2019. Т. 89. №5. С. 455–465.
- Косаян Н.Л. Аддитивная технологическая совокупность 6-го технологического уклада // Экономика и управление: проблемы, решения. 2021. Т. 1. №2. С. 4–8.
- Кутюр С., Тоупин С. Что означает понятие «суверенитет» в цифровом мире? // Вестник международных организаций. 2020. № 15(4). С. 48–69.
- Макарычева А.В. Цифровой и безопасный? // Международные процессы. Апрель–июнь 2015. Т. 13. № 2 (41). С. 141–145.
- Никонов В.А., Воронов А.С., Сажина В.А., Володенков С.В., Рыбакова М.В. Цифровой суверенитет современного государства: содержание и структурные компоненты (по материалам экспертного исследования) // Вестник Томского государственного университета. Философия. Социология. Политология. 2021. № 60. С. 206–216.
- Потеев А.Т. Технологический уклад: методология оценки уровня технологического уклада отрасли / А.Т. Потеев, Т.С. Мешкова // Предприятия, отрасли и регионы: генезис, формирование, развитие и прогнозирование: Сб. научных трудов по материалам III Международной научно-практической конференции, Пермь, 31 марта 2017 года. Пермь: Научная общественная организация «Профессиональная наука», 2017. С. 161–169.
- Ромашкина Н.П. Информационный суверенитет в современную эпоху стратегического противоборства // Информационные войны. 2019. № 4(52). С. 14–19.
- Усков В.С. Научно-технологическое развитие российской экономики в условиях перехода к новому технологическому укладу // Экономические и социальные перемены: факты, тенденции, прогноз. 2020. Т. 13. №1. С. 70–86.
- Шариков П. Информационный суверенитет и вмешательство во внутренние дела в российско-американских отношениях // Международные процессы. 2018. Т. 16. № 3 (54). С. 170–188.
- Bezrukov A.O., Mamonov M.V., Suchkov M.A., & Sushentsov A.A. Russia in the Digital world: international Competition and leadership // Russia in Global Affairs. 2021. Vol. 19. No. 2. P. 64–85.

- Bierwisch A., Kayser V., & Shala E.* Emerging technologies in civil security – A scenario-based analysis // *Technological Forecasting and Social Change*. 2015. Vol. 101. P. 226–237.
- Bremmer I.* The Technopolar Moment // *Foreign Affairs*. 2021. No. 6. URL: <https://www.foreignaffairs.com/articles/world/2021-10-19/ian-bremmer-big-tech-global-order> (accessed: 16.11.2021).
- Carr M.* Power Plays in Global Internet Governance // *Millennium*. 2015. Vol. 43. No. 2. P. 640–659.
- Choucri N.* Cyberpolitics in International Relations. Cambridge: The MIT Press, 2012. 320 p.
- Crystal D.* The Language Revolution. Cambridge: Polity, 2004. 152 p.
- Doria A.* Use [and Abuse] of Multistakeholderism in the Internet // *The Evolution of Global Internet Governance: Principles and Policies in the Making* / ed. by R. Radu, J.-M. Chenou, R.H. Weber. New York: Springer, 2013. P. 115–138.
- Drezner D.W.* The Global Governance of the Internet: Bringing the State Back // *Political Science Quarterly*. 2004. Vol. 119. No. 3. P. 477–498.
- Floridi L.* The Fight for Digital Sovereignty: What It Is, and Why It Matters, Especially for the EU // *Philosophy and Technology*. 2020. Vol. 33. P. 369–378.
- Globerman S.* Canadian science policy and technological sovereignty // *Canadian Public Policy/Analyse De Politiques*. 1978. Vol. 4. No. 1. P. 34–45.
- Goldsmith J.* The Internet and the Abiding Significance of Territorial Sovereignty // *Indiana Journal of Global Legal Studies*. 1998. Vol. 5. No. 2. URL: <https://www.repository.law.indiana.edu/ijgls/vol5/iss2/6> (accessed: 20.09.2021).
- Goldsmith J., Wu T.* Who controls the internet? Illusions of a borderless world. Oxford: Oxford University Press, 2006. 238 p.
- Goodchild M.F.* Towards a location theory of distributed computing and e-commerce // *Worlds of E-Commerce: Economic, Geographical and Social Dimensions* / ed. by T.R. Leinbach, S.D. Brunn. New York: Wiley, 2001. P. 67–86.
- Grant P.* Technological sovereignty: Forgotten factor in the 'hi-tech' razzamatazz" // *Prometheus*. 1983. Vol. 1. No. 2. P. 239–270.
- Hanelt A., Bohnsack R., Marz D., & Antunes Marante C.* A systematic review of the literature on digital transformation: Insights and implications for strategy and organizational change // *Journal of Management Studies*. Vol. 58. No. 5. P. 1159–1197.
- Hardy I.T.* The Proper Legal Regime for 'Cyberspace' // *University of Pittsburgh Law Review*. 1994. Vol. 55. P. 993–1055.
- Harmaakorpi V., Haikonen A., Kauranen I.* The Shift of Techno-Economic Paradigm and Its Effects on Regional Disparities // *The 43rd Conference of European Regional Sciences Association (ERSA)*, 27–31 Aug. Lahti Center, Jyväskylä, Finland: Helsinki University of Technology. 2003. 226 p.
- Hill R.* Internet Governance: The Last Gasp of Colonialism, or Imperialism by Other Means? // *The Evolution of Global Internet Governance: Principles and Policies in the Making* / ed. by R. Radu, J.-M. Chenou, R.H. Weber. New York: Springer, 2013. P. 79–94.
- Howard P.N., Ganesh B., Liotsiou D.* The IRA, Social Media and Political Polarization in the United States, 2012–2018. Computational Propaganda Research Project. University of Oxford, 2012. 47 p.
- Jackson R.* Quasi-States: Sovereignty, International Relations and the Third World. Cambridge: Cambridge University Press, 1990. 181 p.
- Jiang M.* Authoritarian Informalism: China's Approach to Internet Sovereignty // *SAIS Review of International Affairs*. 2010. Vol. 30. No. 2. P. 71–89.
- Johnson D.R., Post D.* Law and Borders – The rise of law in Cyberspace // *First Monday*. 1996. Vol. 1. No. 1. P. 1–25.
- Kello L.* The Virtual Weapon and International Order. New Haven: Yale University Press, 2017. 320 p.
- Kissinger H.* World Order. Penguin, 2014. 432 p.
- Korzak E.* Russia's Cyber Policy Efforts in the United Nations // *Tallinn Papers*. 2021. No. 11. P. 4–20.
- Laurence S.* The Four-Dimensional Human: Ways of Being in the Digital World. London: Penguin Random House, 2015. 272 p.
- Mainwaring S.* Always in control? Sovereign states in cyberspace // *European Journal of International Security*. 2020. Vol. 5. No. 2. P. 215–232.
- Mueller M.L.* Against Sovereignty in Cyberspace // *International Studies Review*. 2020. Vol. 22. No. 4. P. 779–801.
- Mueller M.L.* Ruling the Root: Internet Governance and the Taming of Cyberspace. Cambridge.: The MIT Press, 2002. 328 p.
- Nadkarni S., & Prügl R.* Digital transformation: a review, synthesis and opportunities for future research // *Management Review Quarterly*. 2021. Vol. 71(2). P. 233–341.
- Naughton J.* The evolution of the Internet: from military experiment to General Purpose Technology // *Journal of Cyber Policy*. 2016. Vol. 1. No. 1. P. 5–28.

- Perritt H.* The Internet as a Threat to Sovereignty? Thoughts on the Internet's Role in Strengthening National and Global Governance // *Indiana Journal of Global Legal Studies*. 1998. Vol. 5. No. 2. P. 423–442.
- Priisalu J., Ottis R.* Personal control of privacy and data: Estonian Experience // *Health and Technology*. 2017. Vol. 7. P. 441–451.
- Pohle J., Thiel T.* Digital sovereignty // *Internet Policy Review*. 2020. Vol. 9. No. 4. P. 1–19.
- Perez C.* Technological revolutions and techno-economic paradigms // *Cambridge journal of economics*. 2010. Vol. 34 (1). P. 185–202.
- Rainie L., Anderson J.* Whether or not people disconnect, the dangers are real. Security and civil liberties issues are being magnified by the rapid rise of the Internet of Things // *Pew Research Center*. 2017. URL: <https://www.pewresearch.org/internet/2017/06/06/theme-7-whether-or-not-people-disconnect-the-dangers-are-real-security-and-civil-liberties-issues-are-being-magnified-by-the-rapid-rise-of-the-internet-of-things/> (дата обращения: 20.09.2021).
- Shen Y.* Cyber Sovereignty and the Governance of Global Cyberspace // *Chinese Political Science Review*. 2016. Vol. 1. P. 81–93.
- Scholte J.A.* Globalization: A Critical Introduction. New York: St. Martin's Press, 2000. 519 p.
- Suchkov M.A.* Whose hybrid warfare? How 'the hybrid warfare' concept shapes Russian discourse, military, and political practice // *Small Wars & Insurgencies*. 2021. Vol. 32. No. 3. P. 415–440.
- Tikk E., Kerttunen M.* Routledge Jandbook of International Cybersecurity. Routledge, 2020. 416 p.
- Vesali Naesh M.* Person and Personality in Cyber Space: A Legal Analysis of Virtual Identity // *Masaryk University Journal of Law and Technology*. 2016. Vol. 10. No 1. P. 1–21.
- Verhoef P.C., Broekhuizen T., Bart Y., Bhattacharya A., Dong J.Q., Fabian N., & Haenlein M.* Digital transformation: A multidisciplinary reflection and research agenda // *Journal of Business Research*. 2021. Vol. 122. P. 889–901.
- Wu T.* Cyberspace Sovereignty? – The Internet and the International System // *Harvard Journal of Law & Technology*. 1997. Vol. 10. No. 3. P. 647–666.

THE NOTION OF “DIGITAL SOVEREIGNTY” IN MODERN WORLD POLITICS

CHALLENGES AND OPPORTUNITIES FOR RUSSIA*

OLGA REBRO
ANASTASIA GLADYSHEVA
MAXIM SUCHKOV
ANDREY SUSHENTSOV
MGIMO University, Moscow 119454, Russian Federation

Abstract

The global digital revolution transforms technological and economic structures, social relations and the very philosophy of human life. Along with that, it has a dramatic impact on states as key actors in international relations. For many centuries sovereignty has been a fundamental principle of a functioning state and has been mainly defined in physical and geographical terms. However, the transboundary nature of the digital environment has brought new issues to the agenda: how actors, including states, should function in a new digital reality; where the borders between the ‘national’ and the ‘transnational’ should

* The study was funded by RFBR and EISR, project number N°21-011-31278.

lie and by which rules the new environment should be regulated. The key question summarizing all the above-stated is: 'What does "state sovereignty" mean in the digital era?'. To answer this question, the article identifies key characteristics of digital space vis-à-vis sovereignty, studies the evolution of two approaches to the internet – as a new exceptional environment or as the next stage of telecommunications' development – and points out challenges to maintaining digital sovereignty along with ways to mitigate them. Noting that the digital space is a unique environment for intergovernmental interaction which continuously evolves due to technological progress and the socio-economic practices, the authors observe the organic emergence of cyber-borders which brings seemingly obsolete idea of state sovereignty back into play. Modern states face a difficult challenge: how to find effective mechanisms to ensure sovereignty in the digital space without losing the benefits of the digital revolution while guaranteeing the equality and security of all parties involved. The absence of unified methodology and generally accepted conceptual terms in the previous scientific studies and political practice underpins the academic novelty of the research. At the same time, the study is practically oriented, since it is the digital technological sovereignty of the state that serves as a basis of its leadership in the new era and as a necessary condition for establishing and maintaining political independence and national coherence.

Keywords:

digital environment; digital sovereignty; global governance; digital competition; strategy; cybersecurity; Russia; USA; multi-stakeholder internet governance.

References

- Batueva E. (2014) Informacionnye voyny SSHA: k opredeleniyu nacional'noy kiberstrategii [The US Information Wars: Towards Defining a National Cyber Strategy. *Mezhdunarodnye Processy*. Vol. 12. No. 1–2. P. 117–127.
- Bezrukov A.O., Mamonov M.V., Suchkov M.A., & Sushentsov A.A. (2021). Russia in the Digital world: international Competition and leadership. *Russia in Global Affairs*. Vol. 19. No. 2. P. 64–85.
- Bremmer I. (2021). The Technopolar Moment. *Foreign Affairs*. November/December 2021. URL: <https://www.foreignaffairs.com/articles/world/2021-10-19/ian-bremmer-big-tech-global-order> (accessed: 16.11.2021)
- Bierwisch A., Kayser V., & Shala E. (2015). Emerging technologies in civil security – A scenario-based analysis. *Technological Forecasting and Social Change*. Vol. 101. P. 226–237.
- Carr M. (2015). Power Plays in Global Internet Governance. *Millennium*. Vol. 43. No. 2. P. 640–659.
- Choucri N. (2012). *Cyberpolitics in International Relations*. Cambridge: The MIT Press. 320 p.
- Couture S., Toupin S. (2020). Chto oznachaet ponyatie «suverenitet» v cifrovom mire? [What does the notion of "sovereignty" mean when referring to the digital?]. *Vestnik mezhdunarodnykh organizatsij*. Vol. 15. No. 4. P. 48–69.
- Crystal D. (2004). *The Language Revolution*. Cambridge: Polity. 152 p.
- Doria A. (2013). Use [and Abuse] of Multistakeholderism in the Internet. In: Radu R., Chenou J.-M., Weber R.H. (eds.) *The Evolution of Global Internet Governance: Principles and Policies in the Making*. New York: Springer. P.115–138.
- Drezner D.W. (2004). The Global Governance of the Internet: Bringing the State Back. *Political Science Quarterly*. Vol. 119. No. 3. P. 477–498.
- Floridi L. (2020). The Fight for Digital Sovereignty: What It Is, and Why It Matters, Especially for the EU. *Philosophy and Technology*. Vol. 33. P. 369–378.
- Globerman S. (1978). Canadian science policy and technological sovereignty. *Canadian Public Policy/Analyse De Politiques*. Vol. 4. No. 1. P. 34–45.
- Goldsmith J. (1998). The Internet and the Abiding Significance of Territorial Sovereignty. *Indiana Journal of Global Legal Studies*. Vol. 5. No. 2. URL: <https://www.repository.law.indiana.edu/ijgl/vol5/iss2/6> (accessed: 20.09.2021).
- Goldsmith J., Wu T. (2006). *Who controls the internet? Illusions of a borderless world*. Oxford: Oxford University Press. 238 p.
- Goodchild M.F. (2001). Towards a location theory of distributed computing and e-commerce. In: Leibach T.R., Brunn S.D. (eds.) *Worlds of E-Commerce: Economic, Geographical and Social Dimensions*. New York: Wiley. P. 67–86.
- Grant P. (1983). Technological sovereignty: Forgotten factor in the 'hi-tech' razzamatazz". *Prometheus*. Vol. 1. No. 2. P. 239–270.

- Hanelt, A., Bohnsack, R., Marz, D., & Antunes Marante, C. (2021). A systematic review of the literature on digital transformation: Insights and implications for strategy and organizational change. *Journal of Management Studies*. Vol. 58 (5). P. 1159–1197.
- Hardy I.T. (1994). The Proper Legal Regime for 'Cyberspace'. *University of Pittsburgh Law Review*. Vol. 55. P. 993–1055.
- Harmaakorpi V., Haikonen A., Kauranen I. (2003). The Shift of Techno-Economic Paradigm and Its Effects on Regional Disparities. *The 43rd Conference of European Regional Sciences Association (ERSA)*, 27–31 Aug. Lahti Center, Jyväskylä, Finland: Helsinki University of Technology.
- Hill R. (2013). Internet Governance: The Last Gasp of Colonialism, or Imperialism by Other Means? In: Radu R., Chenou J.-M., Weber R.H. (eds.) *The Evolution of Global Internet Governance: Principles and Policies in the Making*. New York: Springer. P. 79–94.
- Howard P. N., Ganesh B., Liotsiou D. (2012). *The IRA, Social Media and Political Polarization in the United States, 2012–2018. Computational Propaganda Research Project*. University of Oxford. 47 p.
- Jackson R. (1990). *Quasi-States: Sovereignty, International Relations and the Third World*. Cambridge: Cambridge University Press. 181 p.
- Jiang M. (2010). Authoritarian Informationalism: China's Approach to Internet Sovereignty. *SAIS Review of International Affairs*. Vol. 30. No. 2. P. 71–89.
- Johnson D.R., Post D. (1996). Law and Borders – The rise of law in Cyberspace. *First Monday*. Vol. 1. No. 1. P. 1–25.
- Kasenova M.B., Demidov O.V. (2013). *Kiberbezopasnost' i upravlenie internetom: Dokumenty i materialy dlya rossijskikh reguljatorov i ekspertov* [Cybersecurity and Internet Governance: Documents and Materials for Russian Regulators and Experts]. Moscow: Statut. 465 p.
- Kello L. (2017). *The Virtual Weapon and International Order*. New Haven: Yale University Press. 320 p.
- Kissinger H. (2014). *World Order*. Penguin. 432 p.
- Korzak E. (2021). Russia's Cyber Policy Efforts in the United Nations. *Tallinn Papers*. No. 11. P. 4–20.
- Kosakian N.L. (2021). Additivnaya tehnologicheskaja sovokupnost' 6-go tehnologicheskogo uklada [Additive Technological Network of the 6th Technological Setup]. *Ekonomika I upravlenie: problem I resheniya*. Vol. 1. No. 2. P. 4–8.
- Kovalchuk M.V., Naraikin O.S., Yatsishina E.B. Prirodopodobnye tehnologii: novye vozmozhnosti I novye vyzovy [Nature-like technologies: new opportunities and new challenges] // *Vestnik Rossijskoj akademii nauk*. 2019. Vol. 89. No. 5. P. 455–465.
- Laurence S. (2015). *The Four-Dimensional Human: Ways of Being in the Digital World*. London: Penguin Random House. 272 p.
- Mainwaring S. (2020). Always in control? Sovereign states in cyberspace. *European Journal of International Security*. Vol. 5. No. 2. P. 215–232.
- Makarycheva A.V. Cifrovoy i bezopasnyj? [Digital and secure?] *Mezhdunarodnye process*. 2015. Vol. 13. No. 2 (41). P. 141–145.
- Mueller M.L. (2020). Against Sovereignty in Cyberspace. *International Studies Review*. Vol. 22. No. 4. P. 779–801.
- Mueller M.L. (2002). *Ruling the Root: Internet Governance and the Taming of Cyberspace*. Cambridge: The MIT Press. 328 p.
- Nadkarni S., & Prügl R. (2021). Digital transformation: a review, synthesis and opportunities for future research. *Management Review Quarterly*. Vol. 71(2). P. 233–341.
- Naughton J. (2016). The evolution of the Internet: from military experiment to General Purpose Technology. *Journal of Cyber Policy*. Vol. 1. No. 1. P. 5–28.
- Nikonov V.A., Voronov A.S., Sazhina V.A., Volodenkov S.V., Rybakova M.V. (2021). Tsifrovoy suverenitet sovremennogo gosudarstva: soderzhanie i strukturnye komponenty (po materialam ekspertnogo issledovaniya) [Digital Sovereignty of a Modern State: Content and Structural Components (Based on Expert Research)]. *Vestnik Tomskogo gosudarstvennogo universiteta. Filosofiya. Sociologiya. Politologiya*. No. 60. P. 206–221.
- Perez C. (2010). Technological revolutions and techno-economic paradigms. *Cambridge journal of economics*. Vol. 34 (1). P. 185–202.
- Perritt H. (1998). The Internet as a Threat to Sovereignty? Thoughts on the Internet's Role in Strengthening National and Global Governance. *Indiana Journal of Global Legal Studies*. Vol. 5. No. 2. P. 423–442.
- Poteev A.T. (2017). *Tekhnologicheskij uklad: metodologiya ocenki urovnya tekhnologicheskogo uklada otrasli* [Technological mode: methodology for assessing the level of the technological mode of the industry]. In: *Predpriyatiya, otrasli i regiony: genezis, formirovanie, razvitie i prognozirovanie: Sbornik nauchnykh trudov po materialam III Mezhdunarodnoj nauchno-prakticheskoy konferencii. Nauchnaya obshchestvennaya organizaciya "Professional'naya nauka"*. P. 161–169.

- Priisalu J., Ottis R. (2017). Personal control of privacy and data: Estonian Experience. *Health and Technology*. Vol. 7. P. 441–451.
- Pohle J., Thiel T. (2020). Digital sovereignty. *Internet Policy Review*. Vol. 9. No. 4. P. 1–19.
- Rainie L., Anderson J. (2017). Whether or not people disconnect, the dangers are real. Security and civil liberties issues are being magnified by the rapid rise of the Internet of Things // Pew Research Center. URL: <https://www.pewresearch.org/internet/2017/06/06/theme-7-whether-or-not-people-disconnect-the-dangers-are-real-security-and-civil-liberties-issues-are-being-magnified-by-the-rapid-rise-of-the-internet-of-things/> (accessed: 20.09.2021).
- Romashkina N.P. (2019). *Informatsionnyj suverenitet v sovremennuyu epohu strategicheskogo protivoborstva* [Information Sovereignty in the Modern Era of Strategic Warfare]. *Informatsionnye voyny*. Vol. 4. No. 52. P. 14–19.
- Sharikov P. (2018). Informatsionny suverenitet i vmeshatel'stvo vo vnutrennie dela v rossijsko-amerikanskij otnoshenijah [Information sovereignty and interference in internal affairs in Russian-American relations]. *Mezhdunarodnye Processy*. Vol. 16. No. 3(54). P. 170–188.
- Shen Y. (2016). Cyber Sovereignty and the Governance of Global Cyberspace. *Chinese Political Science Review*. Vol. 1. P. 81–93.
- Scholte J.A. (2000). *Globalization: A Critical Introduction*. New York: St. Martin's Press. 519 p.
- Suchkov M.A. (2021). Whose hybrid warfare? How 'the hybrid warfare' concept shapes Russian discourse, military, and political practice. *Small Wars & Insurgencies*. Vol. 32. No. 3. P. 415–440.
- Tikk E., Kerttunen M. (2020) *Routledge Jandbook of International Cybersecurity*. Routledge. 416 p.
- Uskov V.S. (2020) Nauchno-tehnologicheskoe razvitiye rossijskoy ekonomiki v usloviyah perehoda k novomu tehnologicheskomu ukladu [Scientific and Technological Development of the Russian Economy in the Transition to a New Technological Order]. *Ekonomicheskie i social'nye peremeny: facty, tendencii, prognoz*. Vol. 13. No.1. P. 70–86.
- Verhoef, P. C., Broekhuizen, T., Bart, Y., Bhattacharya, A., Dong, J. Q., Fabian, N., & Haenlein, M. (2021). Digital transformation: A multidisciplinary reflection and research agenda. *Journal of Business Research*. Vol. 122. P. 889–901.
- Vesali Naesh M. (2016). Person and Personality in Cyber Space: A Legal Analysis of Virtual Identity. *Masaryk University Journal of Law and Technology*. Vol. 10. No 1. P. 1–21.
- Vinogradova E.V., Polyakova T.A. (2021). O meste informacionnogo suvereniteta v konstitucionno-pravovom prostranstve sovremennoj Rossii [On the Place of Information Sovereignty in the Constitutional Legal sphere in Modern Russia]. *Pravovoe gosudarstvo: teoriya i praktika*. Vol. 17. No. 1. P. 32–49.
- Volodenkov S.V., Voronov A.S., Leont'eva L.S., Suhareva M. (2021). Tsifrovoy suverenitet sovremennogo gosudarstva v usloviyah tehnologicheskij transformatsij: soderzhanie i osobennosti [Digital sovereignty of a modern state in the context of technological transformations: content and features]. *Polylogos*. Vol. 5. No. 1. URL: <https://polylogos-journal.ru/s258770110014073-2-1/> (accessed: 20.09.2021).
- Wu T. (1997). Cyberspace Sovereignty? – The Internet and the International System. *Harvard Journal of Law & Technology*. Vol. 10. No. 3. P. 647–666.
- Zolotareva, O. A. (2021). Gumanitarno-tehnologicheskaya revolyuciya: ocenka sostoyaniya gotovnosti perekhoda v novyj tehnologicheskij uklad [Humanitarian and technological revolution: assessment of the state of readiness for the transition to a new technological order]. *Vestnik NGUEU*. Vol. 4. P. 55–66.