DOI 10.22394/1726-1139-2020-12-24-39

Институты публичного управления интернетом: сравнительный анализ России, Беларуси и Казахстана*

Сморгунов Л. В.

Санкт-Петербургский государственный университет, Санкт-Петербург, Российская Федерация; lvsmorgunov@gmail.com

РЕФЕРАТ

Беларусь, Россия и Казахстан входят в число высокоразвитых стран по индексу развития электронного правительства ООН. Обладая высокими темпами цифровизации государственного управления, решением проблем доступа граждан к интернету и развитием сферы электронных услуг, эти страны отличаются друг от друга конструкцией политики цифровизации. Структура проектов цифровизации в этих странах включает все необходимые компоненты — стратегию, координацию, оценку, вмешательство, однако она отличается направленностью на цифровые изменения и политической инфраструктурой, которая обеспечивает вмешательство технологий в общественную сферу. Среди значимых факторов политики цифровизации в описанных случаях выделяется идея суверенитета, связанная с интернетом и цифровыми технологиями. Общая политика стран, входящих в евразийское пространство сотрудничества, выражается принципом «цифрового суверенитета». В статье анализируется общее понимание принципа «цифрового суверенитета» и различных стратегий его реализации — «многостороннее взаимодействие», «сотрудничество заинтересованных сторон» и «централизованное управление», а также институты управления, обеспечивающие их.

Ключевые слова: цифровой суверенитет, управление интернетом, институты, многостороннее взаимодействие, сотрудничество заинтересованных сторон, централизованное управление

Для цитирования: *Сморгунов Л. В.* Институты публичного управления интернетом: сравнительный анализ России, Беларуси и Казахстана // Управленческое консультирование. 2020. № 12. С. 24–39.

Public Internet Governance Institutes: Comparative Analysis of Russia, Belarus and Kazakhstan

Leonid V. Smorgunov

St. Petersburg State University, St. Petersburg, Russian Federation; lvsmorgunov@gmail.com

ABSTRACT

Belarus, Russia and Kazakhstan are among the highly developed countries in the UN e-Government Development Index. With a high rate of digitalization of public administration, solving the problems of citizens' access to the Internet and developing the electronic services sector, these countries differ from each other in the design of a digitalization policy. The structure of digitalization projects in these countries includes all the necessary components — strategy, coordination, evaluation, intervention, but it is distinguished by a focus on digital change and a political infrastructure that ensures technology interference in the public sphere. Among the significant factors of digitalization policy in the described cases, the idea of sovereignty related to the Internet and digital technologies stands out. The general policy of the countries included in the Eurasian space of cooperation is expressed by the principle of "digital sover-

* Работа выполнена по гранту РНФ 19-18-00210 «Политическая онтология цифровизации: исследование институциональных оснований цифровых форматов государственной управляемости».

eignty". The article analyses the general understanding of the principle of "digital sovereignty" and the various strategies for its implementation — "multilateral interaction", "stakeholder cooperation" and "centralized management", as well as the institutions of management that provide them.

Keywords: digital sovereignty, Internet governance, institutions, multilateral interaction, stakeholder cooperation, centralized management

For citing: Smorgunov L. V. Public Internet Governance Institutes: Comparative Analysis of Russia, Belarus and Kazakhstan // Administrative consulting. 2020. N 12. P. 24–39.

Введение

Внедрение цифровых технологий в управление и политику сопровождается дискуссиями о преимуществах, вызовах и рисках цифрового мира. Современное цифровое управление требует адаптивности, мобильности, гибкости, чувствительности и скорости реакции на возникающие проблемы. Все это призывает к преобразованиям в сфере институтов управления и культуры. Изменения включают в себя новые требования к взаимодействиям в публичной сфере, в том числе внимание к принципам сотрудничества, прозрачности и открытости, инноваций и совместного производства решений.

В последнее десятилетие государственный контроль над интернетом стал очевидным фактом глобальной организации коммуникационных потоков. Этот процесс особенно усилился после того, как в последние годы стало известно о незаконном использовании интернет-информации как спецслужбами, так и коммерческими структурами. Необходимость регулирования интернет-пространства извне стала рассматриваться как важный способ сохранения национального суверенитета над информацией и коммуникациями. Несмотря на то, что это пространство характеризовалось тенденцией глобализации, однако его организационная и технологическая поддержка была сосредоточена либо в руках отдельных государств, либо монополизирована частными компаниями. С одной стороны, например, в Соединенных Штатах имеется огромное количество гипермасштабируемых центров обработки данных, через которые проходил интернет-трафик, а информация хранилась как в частном, так и в общедоступном виде. По некоторым оценкам, их было до 45% от общего числа в мире. И, например, Канаду беспокоило то, что от 25 до 60% ее интернет-трафика проходит через Соединенные Штаты, и возможность использования соответствующих данных американскими спецслужбами [16]. С другой стороны, большая часть информации так или иначе проходит через сети, находящиеся под контролем мегакорпораций. В этом государства видели вызов своей безопасности и суверенитету. Кроме того, назрела необходимость в регулировании совместной экономики и интернет-торговли. Так или иначе, все государства с разной степенью интенсивности начали на это реагировать, пытаясь поднять уровень цифровой управляемости. Некоторые из них начали использовать формулы «цифрового суверенитета», «суверенного интернета» или «информационного суверенитета». Исследование проблем суверенного управления интернетом в России стало центром внимания в последние десятилетия. Большой объем исследований касается правовых аспектов суверенизации [4; 5; 9; 10]. Имеются исследования по отдельным странам и соответствующих особенностях обеспечения суверенного интернета в России, Беларуси и Казахстане [1; 2; 6; 8]. В данной статье анализируются общее движение за реализацию принципа «цифрового суверенитета» и различные стратегии управления суверенизацией — «централизованный контроль», «многостороннее взаимодействие», «сотрудничество заинтересованных сторон», а также институты, обеспечивающие это в трех странах — России, Беларуси и Казахстане.

Движение за суверенный интернет и институциональные дизайны управления

Соединенные Штаты были страной, которая в декабре 2012 г. в Дубае вместе с Великобританией, Канадой и Австралией не подписала заключительный документ Международного союза электросвязи Организации Объединенных Наций. Прежде всего, эти страны выступили против призывов ко всем государствам иметь равные права на управление интернетом. С таким предложением выступили представители России, Китая, Саудовской Аравии, Алжира и Судана. Он заключался в том, что правительства всех стран имели равные права на управление ресурсами нумерации, наименования, адресации и идентификации в интернете. Эта идея увеличения регулирующей функции государства по отношению к интернету была поддержана большинством стран (из 144 стран, имеющих право подписать такую резолюцию, 89 сделали это, а 55 — нет). История «суверенного интернета» начинается с этого исторического факта, который сегодня охватывает не только те страны, которые выступили с соответствующим предложением, но и другие развитые и развивающиеся страны. Конечно, вопрос о национальных условиях существования интернета возник еще до 2012 г. [21], однако как политическая стратегия создания условий, обеспечивающих национальный контроль над интернетом, вопрос обострился во втором десятилетии нынешнего века.

Термин «суверенный интернет» может означать в общих чертах достаточно высокий уровень самодостаточности и технологической независимости страны в этой сфере. Сложность определения пространства такого суверенитета связывают с тем, что «интернет, если оперировать на уровне образной модели взаимодействия некоторых традиционных сфер суверенного господства, — это постоянно дрейфующий в трансграничном пространстве «открытое море — территориальные воды» информационно-телекоммуникационный архипелаг (острова — национальные сегменты Сети)» [3, с. 167]. В узком понимании суверенный интернет сводится к информационному суверенитету как праву государства контролировать на своей территории информационные потоки [5, с. 206]. Более широкое понимание такого суверенитета не ограничивается информационными потоками, а включает в себя весь набор возможных суверенитетов в сфере функционирования интернет-пространства и соответствующих направлений политики (информационный, технологический суверенитет, суверенитет данных и др.). Этот термин чаще всего используется по отношению к трем областям интернет-политики: экономический протекционизм (использование национального оборудования и программного обеспечения и поддержка национальных ИТ-компаний в их экспансии на зарубежные рынки); безопасность национальной интернет-инфраструктуры, обеспечение национализации интернет-трафика; национальная организация по использованию больших данных и их локализации в стране [12]. К важным областям также относится формирование национальных институтов управления интернетом, которые учитывают как положение страны в глобальной сети, так и национальные особенности взаимодействия государства, гражданского общества и производящие интернет инфраструктуру и услуги частные фирмы.

Если говорить в целом о возможных институциональных моделях управления интернетом, то выделяют пять основных идей/моделей: *модель киберпространства* и спонтанного упорядочения, основанная на том, что интернет — это самоуправляемая сфера личной свободы, неподконтрольной правительству; *модель транснациональных институтов* и международных организаций, основанная на представлении о том, что управление интернетом по своей сути выходит за пределы национальных границ и, следовательно, наиболее подходящими институтами являются транснациональные квазичастные кооперативы или международные организации, основанные на договоренностях между национальными правительствами; *модель алгоритмиче-*

ского кода и архитектуры интернета, основанная на представлении о том, что многие решения регулирующих органов принимаются протоколами связи и другим программным обеспечением, которое определяет работу интернета; *модель национальных правительств* и законодательства, основанная на идее о том, что по мере роста значения интернета фундаментальные регулирующие решения будут приниматься национальными правительствами посредством правового регулирования; *модель рыночного регулирования* и экономики, которая предполагает, что рыночные силы определяют фундаментальные решения о природе интернета [22]. Вместе с тем эти идейные представления в конкретной реализации предстают в некоторых смешанных формах и подходах.

Существуют три основных реализуемых подхода к формированию институциональных характеристик управления интернетом, которые имеют международное и национально-государственное выражение: (1) многостороннее взаимодействие (multilaterism); (2) сотрудничество заинтересованных сторон (multistakholderism); (3) централизованное суверенное управление (sovereign Internet governance).

Термин *мультилатеризм*, или многостороннее взаимодействие обычно относится к системе взаимодействия суверенных государств на международной арене. Международный союз электросвязи ООН представляет собой международную организацию государств по развитию интернета. Однако в связи с развитием идеи горизонтальных связей в системе публичного управления на международной и внутринациональной арене этот термин стал использоваться для характеристики управленческой системы, включающей в себя как государственные, так и негосударственные образования, взаимодействующие друг с другом в соответствующей сфере на основе консультаций и принятия многосторонних решений в виде договора/соглашения. При этом применительно к национальной системе управления данный тип институциональной конфигурации взаимодействия предполагает верховенство государства. Система частно-государственного партнерства выступает здесь модельным образцом организации. Многостороннее взаимодействие на ранних этапах становления систем управления всемирной сетью противопоставлялось государственно-центрическому подходу [15]. Однако с развитием сотрудничества заинтересованных сторон уже оно было подвергнуто критике за недостаточное внимание к механизмам более глубокого взаимодействия государственных и негосударственных участников.

Мультистейкхолдизм, или сотрудничество заинтересованных сторон также включает в себя многостороннее взаимодействие, однако в отличие от мультилатеризма здесь изменяются некоторые существенные характеристики позиций и отношений. Эта модель была признана на Всемирном саммите по информационному обществу (WSIS) в качестве глобальной модели для управления интернетом в 2005 г. Прежде всего считается, что все заинтересованные стороны находятся в относительно равных полиархических позициях при решении совместных вопросов управления. Как пишет Л. Денардис, «мультистейкхолдизм определяется ... как два или более класса участников, участвующих в общем предприятии по управлению вопросами, которые они считают общественными по своей природе, и характеризуются полиархическими властными отношениями, установленными процедурными правилами» [17, p. 195]. В число заинтересованных сторон включаются государство, бизнес и общественные ассоциации. Взаимодействие здесь строится не на партнерстве, а на сотрудничестве, т. е. взаимной ответственности за решение общих дел. Общие решения принимаются на основе консенсуса, а не компромисса, что предполагает интенсивную коммуникационную активность заинтересованных сторон в достижении общего согласия. В качестве реализуемых систем мультистейкхолдизма называют обычно Форум по управлению интернетом (IGF), уполномоченный Всемирным саммитом по информационному обществу (WSIS) в 2006 г. и интернет-корпорация по присвоению имен и номеров (ICANN), которая отвечает за техни-

ческий менеджмент и координацию системы доменных имен в интернете (DNS) и его уникальные идентификаторы [18].

Централизованное управление ориентируется на позиционирование государства как единственного гаранта суверенного управления интернетом, которое самостоятельно принимает решения относительно многообразных вопросов организации национального виртуального пространства и его обеспечения. Как правило, управление интернетом здесь становится функцией политических органов государства. Хотя централизованное суверенное управление может допускать другие заинтересованные стороны к процессу обсуждения соответствующей повестки дня и решений, однако их роль сводится к консультации и общественной экспертизе. Централизованное управление интернетом предполагает участие в международных собраниях, однако в форме скорее многостороннего партнерства, а не сотрудничества.

Однако другие страны перед лицом нарастающих вызовов (экономических, финансовых, безопасности, политических) все больше склоняются к «суверенному интернету». В апреле 2019 г. правительство Великобритании опубликовало Белую книгу о вреде в онлайн-пространстве[1], которая предусматривает создание независимого регулирующего органа для оценки содержания онлайн-сайтов. Хотя США заявляют себя сторонниками мультистейкхолдеровского подхода к управлению интернетом, однако налицо усиление координирующей функции государственных органов в этом процессе после принятия в 2018 г. «Национальной киберстратегии»[2]. В условиях усиления национального контроля над интернет-пространством глобальные сети вынуждены учитывать важность государственного регулирования ряда вопросов и заявлять о своей поддержке. Итак, Facebook прямо заявил о необходимости государственного регулирования, а Google проводит дифференцированную политику с учетом этой тенденции. По словам обозревателя BBS Селли Эди: «Отдельный интернет для одних, опосредованный Facebook суверенитет для других: независимо от того, установлены ли информационные границы отдельными странами, коалициями или глобальными интернет-платформами, ясно одно — открытый интернет, Создатели, о которых мечтали, уже ушли» [11]. В своем исследовании свободы интернета, проведенном в 2018 г., Дом свободы (Fredom House) отмечает явную тенденцию к усилению функций государственного надзора, цитируя отчет «Свобода в сети 2018: рост цифрового авторитаризма». Эти оценочные суждения, независимо от того, как они к ним относятся, отражают обеспокоенность по поводу растущего контроля государства над электронными сетями. Отчасти законная, отчасти неразумная, эта политика является отражением потребностей и порядка организации в пространстве глобальных сетей. Такая политика в некоторой степени является отражением общей тенденции государств перед лицом современных вызовов безопасности и устойчивого развития. В движении за суверенный интернет можно выделить множество стратегий, связанных с технологическими, инфраструктурными, политическими, социально-экономическими и культурными аспектами. Три страны евразийского экономического сотрудничества — Россия, Беларусь и Казахстан, которые за последние годы стали одними из высокоразвитых государств по уровню развития электронного правительства, вписываются в это движение со своеобразными политическими замыслами.

[1] Online Harms White Paper. (2019, 8 April) [Электронный ресурс]. URL https://www.gov.uk/government/consultations/online-harms-white-paper (дата обращения: 15.09.2020).

[2] National Cyber Strategy of the United States of America [Электронный ресурс]. URL https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf (дата обращения: 15.09.2020).

Стратегии цифрового суверенитета в России, Беларуси и Казахстане

Развитие национальных цифровых сетей. Россия, Беларусь и Казахстан относятся к числу высокоразвитых стран по индексу развития электронного правительства Организации Объединенных Наций. Для сравнения уровня развития электронного правительства в странах мы использовали показатели индекса развития электронного правительства (EGDI), которые используются ООН для ежегодного обзора состояния мира (табл. 1). Сравнение России, Белоруссии и Казахстана проводится с использованием самого индекса и трех основных показателей. Индекс развития электронного правительства (EGDI) представляет собой средневзвешенное значение нормализованных оценок по трем наиболее важным параметрам электронного правительства, а именно: объем и качество онлайн-услуг (индекс онлайн-услуг, OSI), состояние развития телекоммуникаций. инфраструктура (индекс телекоммуникационной инфраструктуры, TII) и собственный человеческий капитал (индекс человеческого капитала, HCI). Каждый из этих наборов индексов сам по себе является составной мерой, которую можно извлекать и анализировать независимо [23].

Россия в этих рейтингах 2020 г. занимает 36-е место, Беларусь — 40-е, Казахстан — 29-е. Хотя Россия и Беларусь демонстрируют снижение рейтингов, однако все три государства входят в число стран с очень высоким уровнем развития электронного правительства (29% всех обследуемых стран). Эти страны различаются по составным частям индекса развития электронного правительства (см. табл. 1). Таким образом, Казахстан опережает страны по большинству показателей, но отстает по развитию телекоммуникационной инфраструктуры. Обладая высокими темпами цифровизации государственного управления, решением проблем доступа граждан к интернету и развитием сферы электронных услуг, эти страны отличаются друг от друга конструкцией политики цифровизации государственного управления.

Все три страны имеют высокие показатели включенности населения в интернет-пространство — 79% Беларусь, 78% Казахстан и 81% Россия в 2018 г. Беларусь имеет показатели по абонентскому доступу к фиксированной широкополосной связи, сопоставимые с Европейским союзом (соответственно 33,9 и 34,3%), Россия демонстрирует 22,0%, а Казахстан — 13,4%. Все страны характеризуются устойчивой динамикой по развитию интернета (рисунок).

Концепция цифрового суверенитета использовалась в последние годы в связи с политикой формирования цифровой экономики и общества. Это понятие было включено в документы Евразийского союза как особый принцип. Цифровой суверенитет — принцип формирования цифрового государства и общества в Евразийском экономическом союзе. Главы правительств обсудили вопросы цифровизации в ЕАЭС на форуме «Цифровое будущее глобальной экономики» в Алматы (Казахстан) в 2020 г. Председатель Коллегии Евразийской экономической комиссии (ЕЭК)

Таблица 1

Индекс развития электронного правительства
Table 1. Electronic government development index

Страна	OSI	HCI	TII	EGDI	Ранг 2018	Ранг 2020
Россия	0,8176	0,8833	0,7723	0,8244	32	36
Беларусь	0,7059	0,8912	0,8281	0,8084	38	40
Казахстан	0,9235	0,8866	0,7024	0,8375	39	29

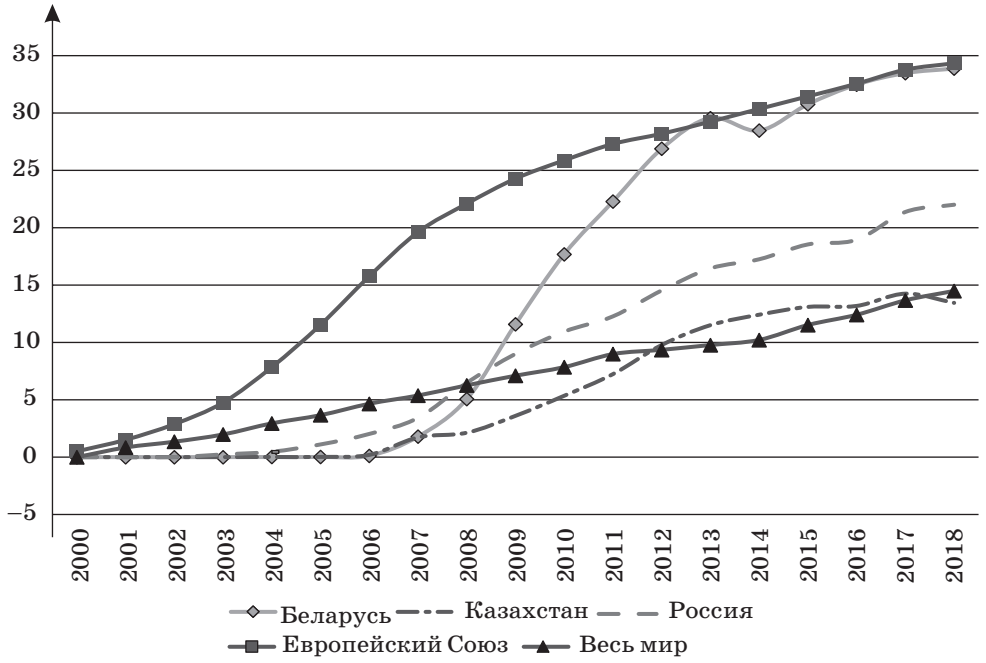

Рис. Абоненты фиксированного широкополосного доступа (на 100 человек)
Fig. Fixed broadband subscriptions (per 100 people)

Источник: World Development Indicators, World Bank [Электронный ресурс]. URL: https://datacatalog.worldbank.org/dataset/world-development-indicators (дата обращения: 28.04.2020).

Тигран Саркисян обратился к странам Евразийского экономического союза (ЕАЭС) совместно решать вопросы обеспечения цифрового суверенитета и защиты данных. Об этом он заявил на форуме 31 января 2020 г.: «Мы не должны стремиться копировать то, что сделали транснациональные компании. Мы должны выработать свою собственную систему, а ключ к этому — современные системы управления этим процессом. Это мы можем сделать только совместно, ни одна из наших стран отдельно не сможет реализовать свой цифровой суверенитет. Единственный шанс — сделать это евразийским проектом» [7]. В исследуемых странах этот термин хоть и используется в документах, но как синоним более конкретных концепций, отражающих современный уровень понимания цифрового суверенитета. «На практике, — пишут С. Будницкий и Л. Цзя, — ни одно правительство не придерживается ни одной из этих абсолютистских позиций, а, скорее, преследует прагматическое сочетание открытости и протекционизма. И к свободе интернета, и к суверенитету интернета следует подходить критически как к часто противоречащим друг другу дискурсивным идеологическим принципам конструкции, а не как объективным абсолютам» [13, p. 597]. Информационной и организационной базой, на которой формируется политика информационного суверенитета (хотя и не ограничивается этим), выступают национальные сети и система серверов доменных имен.

Ряд общих данных по национальным сетям представлен в табл. 2. Национальные сайты Рунета, Белнета и Казнета сформированы на территории России, Беларуси и Казахстана. Количество пользователей национальной сети растет: в исследуемых странах проживает около 80% населения, использующее интернет. Развивается система национальных доменных имен. В настоящее время их в Рунете около

Таблица 2

Национальные сети России, Беларуси и Казахстана в 2020 г.
Table 2. National nets of Russia, Belarus and Kazakhstan in 2020

Национальные сети	Интернет-пользователи, % населения	Число доменов		Число корневых DNS-серверов	Число публичных DNS-серверов
Runet	80,9	.ru	4 950 749	14	117
		.рф	728 653		
		.su	109 394		
Bynet	79,7	.by	135 883	1	3
		.бел	14 504		
Kaznet	78,1	.kz	150 316	3	8
		.қаз	611		
Источник данных	internetworldstats.com	domainnamestats.com		root-servers.org	public-dns.info

5,8 млн, в Белнете и Казнете — по 150 тыс. в каждой сети. На территории соответствующих стран есть вторичные корневые серверы и система публичных серверов. Больше всего эта серверная система разработана в России, на территории которой имеется 14 реплик корневых и 117 публичных DNS-серверов. Наличие реплик (или зеркал) корневых серверов вместе с распределенными по территории страны публичных серверов позволяет обеспечить как отказоустойчивость работы интернета, так и скорость работы системы доменных имен (DNS).

Определение информационного суверенитета. В России информационный суверенитет становится частью ориентации на обеспечение государственной безопасности и находит отражение в Концепции внешней политики Российской Федерации и Доктрине информационной безопасности Российской Федерации[1]. Как справедливо отмечает М.М. Кучерявый, существует проблема определения «информационного суверенитета» как особой сферы государственного суверенитета [6, с. 9]. Ясно, что информационный суверенитет связан с верховенством Российской Федерации в области регулирования и использования национального информационного пространства. Он обеспечивает ряд условий деятельности государства и граждан в информационной сфере. В этом отношении акцент на безопасности выступает центральным в определении сферы и направленности информационного суверенитета. Доктрина информационной безопасности определяет основные принципы, механизмы и направления обеспечения информационной безопасности в стране. Он содержит термин «*суверенитет Российской Федерации в информационном пространстве*», определяя его содержание в широком смысле как определенное верховенство Российской Федерации в организации и использовании информационного пространства страны. Центральным моментом такого верховенства является обеспечение национальных интересов в области информации, их предоставление и защита как на территории страны, так и в международном сотрудничестве.

[1] Указ Президента Российской Федерации от 30.11.2016 № 640 «Об утверждении Концепции внешней политики Российской Федерации» [Электронный ресурс]. URL: http://kremlin.ru/acts/bank/41451 (дата обращения: 12.09.2020); Указ Президента Российской Федерации от 05.12.2016 № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации» [Электронный ресурс]. URL http://kremlin.ru/acts/bank/41460 (дата обращения: 12.09.2020).

Понятие «*информационный суверенитет*» присутствует и в законодательстве Беларуси. В «Стратегии развития информатизации в Республике Беларусь на 2016–2022 годы»[1] говорится, что необходимо «способствовать укреплению национального суверенитета в информационной сфере и национальной безопасности». В документе также присутствует термин «цифровой суверенитет», определение которого отсутствует. Однако очевидно, что эти понятия не идентичны. В Стратегии подчеркивается, что «развитие национальной индустрии информационных технологий является необходимым условием успешного развития информатизации, обеспечения „цифрового суверенитета" государства, а также важным фактором глобальной конкурентоспособности экономики страны». В качестве важной задачи было отмечено, что организация научных исследований, разработка и производство собственного оборудования и программного обеспечения для защиты информации, ключевых элементов информационной и коммуникационной инфраструктуры, совершенствование их стандартизации, системы сертификации в целях обеспечения информационной безопасности и цифрового суверенитета республики. Однако, как отмечают исследователи, «действующее законодательство Республики Беларусь пока не содержит стандартов, полностью гарантирующих цифровую безопасность и цифровой суверенитет. государства» [8, с. 156–157]. Важным шагом в понимании информационного суверенитета является принятие Концепции информационной безопасности Республики Беларусь, утвержденной постановлением Совета Безопасности 18 марта 2019 г., в которой информационный суверенитет рассматривается в контексте информационной безопасности как отдельное явление и регулирующий институт, а также находят правовое закрепление основы государственной политики по защите национальных интересов в информационной сфере. В этом документе информационный суверенитет определяется как неотъемлемое и исключительное верховенство права государства самостоятельно определять правила владения, использования и распоряжения национальными информационными ресурсами, осуществлять независимую внешнюю и внутреннюю государственную информационную политику, формировать национальную информационную инфраструктуру, обеспечивать информационную безопасность[2]. Фактически, здесь информационный суверенитет рассматривается как цифровой суверенитет. Информационный суверенитет рассматривается вместе с *информационным нейтралитетом Беларуси*, а обеспечение безопасности национального сегмента интернета включает в себя в основном отражение основного объема кибератак на информационные системы и сети передачи данных. Информационный нейтралитет трактуется в аспекте политики международного доверия и сотрудничества в области использования новых средств коммуникации.

В Казахстане в документах используется понятие «электронные границы», имеющие отношение к суверенному праву государства на регулирование информационного пространства. Еще в 2011 г. Президент Нурсултан Назарбаев на саммите Шанхайской организации сотрудничества впервые публично заявил о электронном суверенитете и необходимости усилий по поддержанию электронных границ. В программе «Цифровой Казахстан»[3] используется концепция информационной безопас-

[1] Стратегия развития информатизации в Республике Беларусь на 2016–2022 годы: постановление коллегии Минсвязи Респ. Беларусь от 30.09.2015 № 35 [Электронный ресурс]. URL: http://e-gov.by/zakony-i-dokumenty/strategiya-razvitiya-informatizacii-v-respublike-belarus-na-2016-2022-gody (дата обращения: 07.10.2020).

[2] О Концепции информационной безопасности Республики Беларусь: постановление Совета Безопасности Респ. Беларусь от 18 марта 2019 г. № 1[Электронный ресурс]. URL president.gov.by/uploads/documents/2019/1post.pdf (дата обращения: 07.10.2020).

[3] Государственная программа «Цифровой Казахстан»: постановление Правительства Респ. Казахстан от 12 декабря 2017 г. № 827 [Электронный ресурс]. URL: https://digitalkz.kz/wp-content/uploads/2020/03/CK-rus.pdf (дата обращения: 12.07.2020).

ности, содержание которой направлено на обеспечение защищенности электронных границ. Она включает в себя необходимость обеспечения борьбы с киберпреступностью, религиозным экстремизмом и терроризмом. В 2017 г. была разработана концепция безопасности страны «Киберщит Казахстана», целью которой является обеспечение информационной безопасности общества и государства в сфере информации и коммуникации, а также защита конфиденциальности граждан, когда они используют информационную и коммуникационную инфраструктуру.

Все эти национальные подходы к суверенному интернету включают в себя его ориентацию на обеспечение безопасности государства, общества и личности. В литературе такой суверенитет часто называют сильным суверенитетом в противоположность слабому. Слабый суверенитет относится к инициативам частного сектора по защите данных с акцентом на сочетание суверенитета данных с цифровыми правами, а сильный суверенитет относится к деятельности государства по управлению интернетом с акцентом на обеспечение национальной безопасности.

Дизайны управляющих институтов цифровизации и суверенизации интернета

Структура институтов управления, которые разрабатывают и реализуют политику цифровизации и обеспечивают цифровой суверенитет в различных странах, строится с учетом многих факторов внутреннего и внешнего порядка. Они часто определяются доминирующей формой менталитета менеджмента, конкретной историей, культурой и стилем управления. Под структурой управленческих институтов мы подразумеваем сознательную и преднамеренную попытку определить цели политики и связать их с инструментами или средствами, которые, как ожидается, помогут реализовать эти цели [19, p. 292]. Существует несколько подходов к классификации институтов проектного менеджмента цифровизации. Один из подходов предполагает нацеливание на государственные уровни, которые обеспечивают общую координацию усилий по цифровизации. Здесь могут выделяться замыслы централизованного правительства, уполномоченного государственного органа или специально созданного органа централизованного управления. Второй подход берет за основу взаимодействие государства, бизнеса и гражданского общества в процессе разработки и реализации политик цифровизации. Отсутствие такого взаимодействия часто порождает технократический подход, выражающийся в невольном авторитаризме. Есть сторонники идеи широкого плюрализма участников взаимодействия в управлении цифровизацией. Однако, как подчеркивает Мэдлин Карр, «одна из фундаментальных проблем нынешних договоренностей состоит в том, что вместо того, чтобы распределять власть среди широкого круга участников, принцип многостороннего участия усиливает существующую динамику власти, которая с самого начала была „встроена“ в модель» [14, с. 658]. Все исследованные страны характеризуются централистическим дизайном институтов управления с акцентом на государстве. Однако есть элементы мультилатерализма и мультистейкхолдизма.

Система централизованного управления цифровизацией в России. Российская политика формирования системы управления цифровизацией, включая обеспечение цифрового суверенитета, основана на убеждении, что текущее распределение между странами ресурсов, необходимых для обеспечения безопасного и стабильного функционирования интернета, не позволяет реализовать совместное справедливое управление, основанное на принципах доверия[1]. Следовательно, Россия ориентиро-

[1] О Доктрине информационной безопасности Российской Федерации: Указ Президента Российской Федерации от 5 декабря 2016 г. № 646[Электронный ресурс]. URL: https://rg.ru/2016/12/06/doktrina-infobezobasnost-site-dok.html (дата обращения: 07.06.2020).

вана прежде всего на формирование национальной системы управления процессом цифровизации всех сторон общественной жизни и защиты информационного пространства для обеспечения национального суверенитета. Эта национальная система, по сути, состоит из трех подсистем: (1) управление национальной программой «Цифровая экономика Российской Федерации»; (2) система защиты информации; (3) национальная система управления российским сегментом сети интернет.

Структура первой подсистемы определена Постановлением Правительства Российской Федерации от 2 марта 2019 г.[1] Ее содержательные компоненты и принципы организаций указывают на то, что система организована по смешанному принципу, который включает государственную централизацию, элементы многосторонности и государственно-частного партнерства. Этой подсистемой руководит Президиум Совета при Президенте по стратегическому развитию и национальным проектам. Подсистема состоит из трех блоков: Правительственная комиссия по цифровому развитию с соответствующими структурами управления, отраслевые органы цифровизации, а также автономные некоммерческие организации цифровой экономики, в формировании которых наряду с государством участвует бизнес. В данной подсистеме ослаблена роль гражданского общества.

В систему защиты информации входят все основные органы государственной власти, а также частные и негосударственные структуры и организации, обеспечивающие информационные процессы в стране. По сути, эта система представляет собой всю политическую и административную структуру государства, а также бизнеса и СМИ в аспекте реализации задач суверенитета Российской Федерации в информационной сфере.

Наконец, создание национальной системы управления российским сегментом сети интернет активизировалось с принятием так называемого Закона о «Суверенном интернете» — неофициальное название Федерального закона от 1 мая 2019 г.[2], который предусматривает создание национальной системы маршрутизации интернет-трафика, инструментов централизованного управления и др. В соответствии с ним в системе управления связью происходит ряд перестановок, повышающих роль Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор), строится национальная система доменных имен, операторы связи обязуются установить государственное оборудование в точках обмена трафиком для анализа и фильтрации трафика (Deep Packet Inspection; DPI) внутри страны и линий связи, пересекающих Россию на границе и т. д. Роскомнадзор заменил в 2020 г. Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации в качестве одного из учредителей основного координирующего органа в сфере национальных доменных имен — Координационный центр доменов .RU/.РФ (https://cctld.ru/about/). Задачи этого центра включают в себя как обеспечение качества и доступности услуг регистрации доменных имен в российских национальных доменах, так и совершенствование правил регистрации, организация деятельности регистраторов и их аккредитация. К ним также относится техническое и технологическое обеспечение работы DNS для национальных доменов; обеспечение целостности, непрерывности, стабильности, устойчивости и защищенности функционирования российского национального сегмента сети интернет; содействие повышению безопасности использования интернета и расширению ис-

[1] О системе управления реализацией национальной программы «Цифровая экономика Российской Федерации»: постановление Правительства РФ от 2 марта 2019 г. № 234 [Электронный ресурс]. URL: https://base.garant.ru/72190034/ (дата обращения: 15.06.2020).

[2] О внесении изменений в Федеральный закон «О связи» и Федеральный закон «Об информации, информационных технологиях и защите информации»: федер. закон Рос. Федерации от 1 мая 2019 г. № 90-ФЗ[Электронный ресурс]. URL https://rg.ru/2019/05/07/fz90-dok.html (дата обращения: 12.10.2020).

пользования интернета в России в интересах различных интернет-пользователей. Россия участвует в международных структурах, обеспечивающих регулирование глобальных процессов в развитии интернета. В частности, проводятся национальные Российские форумы по управлению интернетом (https://rigf.ru/), в основе которых лежит идея мультистейкхолдизма. Было проведено десять таких форумов с участием государства, бизнеса и гражданского общества. В 2025 г. в России планируется очередной 20-й Форум ООН по управлению интернетом (IGF 2025).

Причастность России к использованию электронных технологий иногда описывается как способность системы повышать уровень управления посредством контроля, что приводит к непреднамеренному цифровому авторитаризму [20]. Однако, на наш взгляд, это скорее смешанная конструкция политических институтов и взаимодействий со значительными элементами централизации и технократизма.

Казахстанская система управления сервисной моделью для цифровизации. В отличие от России в Казахстане принята пусть и централизованная, но с большим участием бизнеса и гражданского общества система управления ИТ, основанная на цифровизации. Это можно назвать умеренным мультистейкхолдизмом. Республика активно участвует в международных организациях и форумах по управлению интернет-пространством, в частности являясь важным организатором и участником Центрально-Азиатского форума по управлению интернетом.

24 октября 2015 г. в Казахстане был принят закон «Об информатизации»[1]. Основная идея нового Закона — переход государственных органов на сервисную модель информатизации. *Сервисная модель основана на концепции многостороннего сотрудничества заинтересованных сторон для управления информатизацией*. В этой связи она рассматривается как централизованный подход в информатизации государственных органов, основанный на предоставлении государственным органам информационно-коммуникационных услуг оператором информационно-коммуникационной инфраструктуры «электронного правительства» с привлечением владельцев информационно-коммуникационной инфраструктуры и сервисных программных продуктов. Государство переходит от капитальных затрат на создание собственной инфраструктуры и создание собственных информационных продуктов к расходам на использование информационной инфраструктуры и продуктов с участием бизнеса. В связи с этим в новом Законе об информатизации прямо предусмотрено, что создание и развитие информационно-коммуникационных услуг в рамках сервисной модели может осуществляться как за счет бюджетных средств, так и из других источников, в том числе на основе государственно-частного партнерства.

Что касается механизма с участием многих заинтересованных сторон для управления процессом информатизации, он включает в себя ряд авторитетных институтов власти и развития и функций, связанных как с внедрением цифровых технологий, так и с обеспечением информационной безопасности с учетом цифрового суверенитета. В этом централизованном механизме можно выделить актуальную государственную систему управления информацией и безопасностью, формирование в ней институтов и функций для развития и внедрения ИКТ с участием бизнеса, а также на современном этапе подключения гражданского общества для участия в цифровизации в виде специального института цифровых комиссаров. Фактическая государственная система управления информацией и безопасностью включает правительство республики, которое отвечает за политику информатизации и формирование ее институтов. Здесь необходимо выделить уполномоченный орган в сфере информатизации, в который входит Министерство цифрового развития,

[1] Об информатизации (с изменениями и дополнениями по состоянию на 25.06.2020 г.): закон Республики Казахстан от 24 ноября 2015 года № 418-V [Электронный ресурс]. URL https://online.zakon.kz/document/?doc_id=33885902 (дата обращения: 22.07.2020).

инноваций и аэрокосмической промышленности, созданное в 2016 г. Именно на него ложится задача координации работ по формированию политики импортозамещения в области производства новой цифровой техники и программ, а также по вопросам обеспечения безопасности в информационном пространстве. В этой связи отмечаются ряд сложностей с реализацией этой политики, касающихся кадровой, финансовой и производственной ее составляющих [1, с. 96]. Второе важное государственное учреждение — агентство информационной безопасности. В его состав входит Комитет государственной безопасности республики, под общим руководством которого находится республиканское государственное предприятие «Государственная техническая служба». Именно последний выполняет функции Национального координационного центра информационной безопасности. Наконец, государство формирует ряд институтов для развития цифровизации с участием бизнеса. К ним относятся, в частности, Национальный институт ИКТ, сервисный интегратор электронного правительства, оператор информационно-коммуникационной инфраструктуры электронного правительства, Международный технопарк «Астана Хаб». Важным центром координации национального сегмента интернета выступает «Казахский центр сетевой информации» (KazNIC), который был создан в 1999 г. как некоммерческая организация. Центр выступает важным звеном координации движения сетевой информации, управления и контроля использования национальных доменных имен, устанавливает, публикует и администрирует правила их использования, поддерживает их регистрацию, обеспечивает процедуры авторизации изменений зарегистрированных доменных имен и выполняет еще ряд дополнительных задач подобного профиля.

Система управления процессом информатизации Беларуси. Система управления процессом информатизации и институциональная структура развития информатизации разработаны в Стратегии развития информатизации в Республике Беларусь на 2016–2022 гг.[1] По сравнению с Россией, система, хотя и централизованная и в которой доминирует государство, имеет явное желание включать в себя элементы механизма многостороннего партнерства для управления сетями. Основными принципами системы являются: централизация управления процессами формирования, реализации и сопровождения программ в области информатизации; согласование интересов всех заинтересованных сторон (различных ветвей и уровней власти и управления, бизнеса, исследовательского сектора, гражданского общества) в рамках программ информатизации; качественная независимая техническая экспертиза программ и проектов информатизации; постоянный мониторинг, оценка результатов и корректировка планов. В Беларуси прошли четыре национальных Форума по управлению интернетом, она сотрудничает по этому вопросу с рядом пограничных государств и международными структурами.

Институциональная структура, реализующая эти принципы, сформирована из следующих государственных органов и организаций: Совет по развитию информационного общества при Президенте Республики Беларусь; Оперативно-аналитический центр при Президенте Республики Беларусь; Министерство связи и информатизации Республики Беларусь; Национальная академия наук Беларуси; Государственный военно-промышленный комитет Республики Беларусь; сеть базовых организаций по информатизации.

Администратором национальной доменной зоны Беларуси выступает Оперативно-аналитический центр при Президенте Республики Беларусь (https://oac.gov.by/).

[1] Стратегия развития информации в Республике Беларусь на 2016–2022 гг.: постановление коллегии Минсвязи Респ. Беларусь от 30.09.2015 № 35[Электронный ресурс]. URL: http://e-gov.by/zakony-i-dokumenty/strategiya-razvitiya-informatizacii-v-respublike-belarus-na-2016-2022-gody (дата обращения: 07.10.2020).

Он был создан в 2008 г. и относится к государственным органам, осуществляющим регулирование, связанное с защитой государственной информации. В 2010 г. ему были переданы функции независимого регулятора в сфере информационно-коммуникационных технологий.

Заключение

Исследование процессов организации управления государственной политикой цифровизации в трех странах ЕАЭС демонстрирует, что с общей стратегией выбора политических целей цифровизации и акцентом на цифровой суверенитет каждая страна вносит свой вклад в интерпретацию базовых концепций и разработку дизайна политических институтов для управления этим процессом. Цифровой суверенитет, понимаемый как верховенство государства в организации национального информационного пространства, находит свое выражение прежде всего в организации информационной безопасности. Вместе с тем цифровой суверенитет предполагает создание собственной технологической и инфраструктурной базы, организацию и защиту данных, развитие национальных платформ государственного управления. Эти вопросы решаются в исследуемых странах с разной интенсивностью. Наибольший прогресс наблюдается у нас в России, но другие страны постепенно реализуют соответствующие задачи. Для их эффективной реализации были созданы собственные разработки для управления процессом цифровизации в целом и обеспечения цифрового суверенитета в частности. Россия здесь использует централизованный контроль. Беларусь склонна к ограниченному многостороннему подходу. Казахстан ориентирован на умеренное сотрудничество заинтересованных сторон. Интересно, что институты поддержания цифрового суверенитета с акцентированием роли бизнеса и гражданского общества четко прописаны в системе управления цифровизацией в Беларуси и Казахстане, но имеют некоторую общую постановку в России. Вместе с тем, если мы понимаем цифровой суверенитет шире, чем обеспечение информационной безопасности, то все представленные проекты управляющих институтов цифровизации обеспечивают эту цель.

Литература

1. *Асадова З. А.* Состояние и стратегии обеспечения информационной безопасности в странах Центральной Азии: на примере Республики Казахстан // Вестник МГИМО-Университета. 2016. № 6 (51). С. 92–96.
2. *Бухарин В. В.* Компоненты цифрового суверенитета Российской Федерации как техническая основа информационной безопасности // Вестник МГИМО-Университета. 2016. № 6 (51). С. 76–91.
3. *Даниленков А. В.* Государственный суверенитет Российской Федерации в информационно-телекоммуникационной сети интернет // Русский закон. 2017. № 7 (128). С. 154–165.
4. *Джойс Е. А., Симаков А. А.* Цифровой суверенитет и правовое регулирование пиринговых платежных систем // Научный Вестник Омской академии МВД России. 2018. № 3 (70). С. 54–60.
5. *Ефремов А. А.* Формирование концепции информационного суверенитета государства // Право. Журнал Высшей школы экономики. 2017. № 1. С. 201–215.
6. *Кучерявый М. М.* Государственная политика информационного суверенитета России в условиях современного глобального мира // Управленческое консультирование. 2014. № 9 (69). С. 12–18.
7. *Саркисян Т.* Цифровую трансформацию стран ЕАЭС должны осуществлять вместе // Сайт Евразийской экономической комиссии [Электронный ресурс]. URL: http://www.eurasiancommission.org/ru/nae/news/Pages/31-01-2020-4.aspx (дата обращения: 10.06.2020).
8. *Становление* и развитие цифровой трансформации и информационного общества (IT-страны) в Республике Беларусь / под ред. В. Г. Гусакова. Минск : Белорусская книга, 2019.

9. *Терентьева Л. В.* Принципы установления территориальной юрисдикции государства в киберпространстве // Русский закон. 2019. № 7 (152). С. 119–129.
10. *Черняк Л. Ю.* К вопросу о понятии информационного суверенитета: теоретический и сравнительно-правовой анализ // Сибирский юридический Вестник. 2012. № 3 (58). С. 117–122.
11. *Adee S.* The global internet is disintegrating. What comes next? BBC: Future Now. 2019, 15 May [Электронный ресурс]. URL http://www.bbc.com/future/story/20190514-the-global-internet-is-disintegrating-what-comes-nex (дата обращения: 12.06.2020).
12. *Brokeš F.* Russia's sovereign internet. Central European Financial Observer. 2018, 24 September [Электронный ресурс]. URL https://financialobserver.eu/cse-and-cis/russias-sovereign-internet/ (дата обращения: 15.05.2020).
13. *Budnitsky S., Jia L.* Branding Internet sovereignty: Digital media and the Chinese–Russian cyberalliance // European Journal of Cultural Studies 2018. Vol. 21. N 5. P. 594–613.
14. *Carr M.* Power Plays in Global Internet Governance // Millennium: Journal of International Studies. 2015. Vol. 43. N 2. P. 640–659.
15. *Christou G., Simpson S.* The European Union, multilateralism and the global governance of the Internet // Journal of European Public Policy. 2011. Vol. 18. N 2. P. 241–257.
16. *Clement A.* Canadian Network Sovereignty: A Strategy for Twenty-First-Century National Infrastructure Building. 2018, 26 March. URL https://www.cigionline.org/articles/canadian-network-sovereignty (дата обращения: 11.09.2020).
17. *DeNardis L.* The Global War for Internet Governance. New Haven, Connecticut : Yale University Press, 2015.
18. *Hofmann J.* Multi-stakeholderism in Internet governance: putting a fiction into practice // Journal of Cyber Policy. 2016. Vol. 1. N 1. P. 29–49.
19. *Howlett* M. Designing Public Policies. Principles and Institutions. New York : Routledge, 2015.
20. *Morgus* R. The Spread of Russia's Digital Authoritarianism // Artificial Intelligence, China, Russia, and the Global Order / ed. Wright N. D. Maxwell Air Force Base : Air University Press, 2019.
21. *Shen Y.* Cyber Sovereignty and the Governance of Global Cyberspace // Chinese Political Science Review. 2016. Vol. 1. N 1. P. 81–93.
22. *Solum L.* B. Models of Internet Governance (September 3, 2008). Illinois Public Law Research Paper N 07-25, U Illinois Law & Economics Research Paper N LE08-027 [Электронный ресурс]. URL https://ssrn.com/abstract=1136825 (дата обращения: 11.09.2020).
23. *United* Nations E-Government Survey 2020. Digital Government in the Decade of Action for Sustainable Development. New York : United Nations, 2020.

Об авторе:

Сморгунов Леонид Владимирович, профессор кафедры политического управления Санкт-Петербургского государственного университета (Санкт-Петербург, Российская Федерация), доктор философских наук, профессор; lvsmorgunov@gmail.com

References

1. Asadova Z. A. State and strategies for ensuring information security in the countries of Central Asia: on the example of the Republic of Kazakhstan // Bulletin of MGIMO-University [Vestnik MGIMO-Universiteta]. 2016. N 6 (51). P. 92–96. (In rus)
2. Bukharin V. V. Components of digital sovereignty of the Russian Federation as a technical basis for information security // Bulletin of MGIMO-University [Vestnik MGIMO-Universiteta]. 2016. N 6 (51). P. 76–91. (In rus)
3. Danilenkov A. V. State sovereignty of the Russian Federation in the information and telecommunications network of the Internet // Russian law [Russkii zakon]. 2017. N 7 (128). P. 154–165. (In rus)
4. Joyce E. A., Simakov A. A. Digital sovereignty and legal regulation of peer-to-peer payment systems // Scientific Bulletin of the Omsk Academy of the Ministry of Internal Affairs of Russia [Nauchnyi Vestnik Omskoi akademii MVD Rossii]. 2018. N 3 (70). P. 54–60. (In rus)
5. Efremov A. A. Formation of the concept of information sovereignty of the state // Law. Journal of the Higher School of Economics [Pravo. Zhurnal Vysshei shkoly ekonomiki]. 2017. N 1. P. 201–215. (In rus)
6. Kucheryavyy M. M. State policy of information sovereignty of Russia in the modern global world // Administrative consulting [Upravlencheskoe konsul'tirovanie]. 2014. N 9 (69). P. 12–18. (In rus)

7. Sargsyan T. The digital transformation of the EAEU countries should be carried out together [Electronic resource] // Website of the Eurasian Economic Commission. URL: http://www.eurasiancommission.org/ru/nae/news/Pages/31-01-2020-4.aspx (date of address: 10.06.2020). (In rus)
8. Formation and development of digital transformation and information society (IT-countries) in the Republic of Belarus / edited by V. G. Gusakova. Minsk: Belarusian Book, 2019. (In rus)
9. Terentyeva L. V. Principles of establishing the territorial jurisdiction of the state in cyberspace // Russian law [Russkii zakon]. 2019. N 7 (152). P. 119–129. (In rus)
10. Chernyak L.Yu. On the question of the concept of information sovereignty: theoretical and comparative legal analysis // Siberian Legal Bulletin [Sibirskii yuridicheskii Vestnik]. 2012. N 3 (58). P. 117–122. (In rus)
11. Adee S. The global internet is disintegrating. What comes next? BBC: Future Now. 2019, 15 May [Electronic resource]. URL http://www.bbc.com/future/story/20190514-the-global-internet-is-disintegrating-what-comes-nex (date of address: 12.06.2020).
12. Brokeš F. Russia's sovereign internet. Central European Financial Observer. 2018, 24 September [Electronic resource]. URL https://financialobserver.eu/cse-and-cis/russias-sovereign-internet/ (date of address: 15.05.2020).
13. Budnitsky S., Jia L. Branding Internet sovereignty: Digital media and the Chinese–Russian cyberalliance // European Journal of Cultural Studies 2018. Vol. 21. N 5. P. 594–613.
14. Carr M. Power Plays in Global Internet Governance // Millennium: Journal of International Studies. 2015. Vol. 43. N 2. P. 640–659.
15. Christou G., Simpson S. The European Union, multilateralism and the global governance of the Internet // Journal of European Public Policy. 2011. Vol. 18. N 2. P. 241–257.
16. Clement A. Canadian Network Sovereignty: A Strategy for Twenty-First-Century National Infrastructure Building. 2018, 26 March. URL https://www.cigionline.org/articles/canadian-network-sovereignty (date of address: 11.09.2020).
17. DeNardis L. The Global War for Internet Governance. New Haven, Connecticut : Yale University Press, 2015.
18. Hofmann J. Multi-stakeholderism in Internet governance: putting a fiction into practice // Journal of Cyber Policy. 2016. Vol. 1. N 1. P. 29–49.
19. Howlett M. Designing Public Policies. Principles and Institutions. New York : Routledge, 2015.
20. Morgus R. The Spread of Russia's Digital Authoritarianism // Artificial Intelligence, China, Russia, and the Global Order / ed. Wright N. D. Maxwell Air Force Base : Air University Press, 2019.
21. Shen Y. Cyber Sovereignty and the Governance of Global Cyberspace // Chinese Political Science Review. 2016. Vol. 1. N 1. P. 81–93.
22. Solum L. B. Models of Internet Governance (September 3, 2008). Illinois Public Law Research Paper N 07-25, U Illinois Law & Economics Research Paper N LE08-027 [Electronic resource]. URL https://ssrn.com/abstract=1136825 (date of address: 11.09.2020).
23. United Nations E-Government Survey 2020. Digital Government in the Decade of Action for Sustainable Development. New York : United Nations, 2020.

About the author:

Leonid V. Smorgunov, Professor of the Chair of the Political Governance at the St. Petersburg State University (St. Petersburg, Russian Federation), Doctor of Science (Philosophy), Professor; lvsmorgunov@gmail.com