ЦИФРОВАЯ ЭКОНОМИКА

УДК: 338.24; 338.012; 332.145
JEL: D81; O33; O 31; O38

Цифровой суверенитет России: барьеры и новые траектории развития

М.Н. Дудин, д.э.н., профессор
https://*orcid.org/0000-0001-6317-2916; SPIN-код (РИНЦ): 8139-4337*
Scopus author ID: 55961173100
e-mail: *dudinmn@mail.ru*

С.В. Шкодинский, *д.э.н., профессор*
https://orcid.org/0000-0002-5853-3585; SPIN-код (РИНЦ): 5372-2519
Scopus author ID: 57192955537
e-mail: *sh-serg@bk.ru*

Д.И. Усманов, к.э.н., доцент
https://orcid.org/0000-0002-0357-1584; SPIN-код (РИНЦ): 7711-9284
Scopus author ID: 57212345986
e-mail: *us.dali@mail.ru*

Для цитирования
Дудин М.Н., Шкодинский С.В., Усманов Д.И. Цифровой суверенитет России: барьеры и новые траектории развития // Проблемы рыночной экономики. – 2021. – № 2. – С. 30-49.
DOI: https://doi.org/10.33051/2500-2325-2021-2-30-49

Аннотация
Предмет/тема. Статья посвящена изучению понятия, параметров, барьеров и сценариев обеспечения цифрового суверенитета Российской Федерации в эпоху Индустрии 4.0. ***Методология.*** Для изучения понятия цифрового суверенитета как научной дефицинии авторами применялись общенаучные методы (наблюдение, сравнение, измерение, анализ и синтез, метод логического рассуждения), при проведении аналитического исследования показателей цифровой зрелости национальной экономики РФ, динамики высокотехнологичных вызовов и угроз использовались конкретно-научные методы (статический анализ, экспертные оценки, графический метод), для формирования сценариев будущей траектории развития цифрового суверенитета – методы стратегического управления – SWOT-анализ, PEST-анализ, инструменты Форсайта. Обоснованность и достоверность результатов научного исследования обеспечивается корректностью и строгостью построения логики и схемы исследования. В качестве методологической и фундаментальной основы исследования были использованы научные и прикладные исследования российских и зарубежных ученых в сфере инновационного развития, цифровой экономики и государственного управления. Исходные статистические данные для анализа взяты из открытых источников тематических обзоров и аналитических отчетов консалтинговых агентств VC.RU, Министерства экономического развития РФ, Центра исследований Сколково, Digital IQ, PWC, статистических сборников НИУ ВШЭ и Росстата. ***Результаты.*** В настоящее время цифровой суверенитет рассматривается с политической, экономической и технологической позиций, что обуславливает наличие плюрализма точек зрения на его содержательное определение в научной литературе. Авторы предлагают под *цифровым суверенитетом понимать критерий устойчивости архитектуры социально-экономической бизнес-модели перед внешними и внутренними*

цифровыми вызовами и угрозами различной природы происхождения, а также ее способности к адаптации и проактивной защите собственных интересов в цифровой сфере. Развитие цифрового суверенитета РФ представлено по четырем сценариям: 1-ый – РФ не смогла выстроить действенную национальную инфраструктуру и находится в зависимом положении от указанных групп, цифровой суверенитет стал объектом и средством влияния мировых лидеров на поведение целых государств и союзных образований, акцент на военно-политической роли цифрового суверенитета; 2-ой – РФ присоединяет цифровую инфраструктуру к Азиатской группе, а китайский конгломерат проводит политику мягкого поглощения с постепенной ассимиляцией культурно-ценностных парадигм населения на неокитайские парадигмы; 3-ий – крах олигополистической власти группы FAMGA (США) и группы BAT (Китай), вся мировая экономика перекраивается в автономные цифровые экосистемы, которые выстраивают между собой отношения на принципах win-win партнерства; 4-ый – США, ЕС, РФ активно развивают цифровую инфраструктуру в странах Азии, Африки, Южной Америки для формирования новой колониальной системы, построенной на базе цифровых технологий. ***Выводы/значимость.*** В рамках научного исследования было установлено, что цифровой суверенитет государства напрямую зависит от уровня цифровой зрелости национальной экономики и цифровой ответственности поведения социума. С учетом прохождения мировой экономической системой точки невозврата – наступлением эпохи Индустрии 4.0 – вопрос обеспечения цифрового суверенитета государства становится новым приоритетом повестки будущего развития. ***Применение.*** Полученные в процессе научного исследования результаты могут быть использованы органами власти и управления в качестве теоретической и практической основы принятия соответствующих решений в области совершенствования процессов цифровой трансформации различных уровней социума, а представителями бизнеса – для корректировки бизнес-стратегий развития на основе учета актуальных цифровых вызовов и угроз.

Ключевые слова: *цифровой суверенитет, Индустрия 4.0, технологическая инфраструктура, цифровая зрелость, киберугрозы*

Digital sovereignty of Russia: barriers and new development tracks

Mikhail N. Dudin, Dr. of Sci. (Econ.), Professor
https://*orcid.org/0000-0001-6317-2916; SPIN-код (РИНЦ): 8139-4337*
Scopus author ID: 55961173100
e-mail: *dudinmn@mail.ru*

Sergey V. Shkodinsky, Dr. of Sci. (Econ.), Professor
https://orcid.org/0000-0002-5853-3585; SPIN-код (РИНЦ): 5372-2519
Scopus author ID: 57192955537
e-mail: sh-serg@bk.ru

Daler I. Usmanov, Cand. of Sci. (Econ.), Associate Professor
https://orcid.org/0000-0002-0357-1584; SPIN-код (РИНЦ): 7711-9284
Scopus author ID: 57212345986
e-mail: *us.dali@mail.ru*

For citation
Dudin M.N., Shkodinsky S.V., Usmanov D.I. Digital sovereignty of Russia: barriers and new development tracks // Market economy problems. – 2021. – No. 2. – Pp. 30-49 (In Russian).
DOI: https://doi.org/10.33051/2500-2325-2021-2-30-49

Abstract
Subject/Topic. The article is devoted to the study of the concept, parameters, barriers and scenarios for ensuring the digital sovereignty of the Russian Federation in the era of Industry 4.0. ***Methodology.*** To study the concept of digital sovereignty as a scientific shortage, the authors used general scientific methods (observation, comparison, measurement, analysis and synthesis, the method of logical reasoning), when conducting an analytical study of indicators of the digital maturity of the national economy of the Russian Federation, the dynamics of high-tech challenges and threats specific scientific methods were used (static analysis, expert assessments, graphical method), to form scenarios of the future trajectory of the development of digital sovereignty, methods of strategic management – SWOT analysis, PEST analysis, Foresight tools. The validity and reliability of the results of scientific research is ensured by the correctness and rigor of the construction of the logic and research scheme. Scientific and applied research of Russian and foreign scientists in the field of innovative development, digital economy and public administration was used as a methodological and fundamental basis for the study. The initial statistical data for the analysis were taken from open sources of thematic reviews and analytical reports of the consulting agencies VC.RU, the Ministry of Economic Development of the Russian Federation, the Skolkovo Research Center, Digital IQ, PWC, statistical collections of the Higher School of Economics and Rosstat. ***Results.*** Currently, digital sovereignty is considered from a political, economic and technological point of view, which determines the presence of a pluralism of points of view on its meaningful definition in the scientific literature. The authors propose to understand by digital sovereignty the criterion of sustainability of the architecture of a socio-economic business model in front of external and internal digital challenges and threats of various origins, as well as its ability to adapt and proactively protect its own interests in the digital sphere. The development of the digital sovereignty of the Russian Federation is presented according to four scenarios: 1st – the Russian Federation is unable to build an effective national infrastructure and is dependent on these groups, digital sovereignty has become an object and means of influence of world leaders on the behavior of entire states and allied formations, an emphasis on military the political role of digital sovereignty; 2nd – the Russian Federation joins the digital infrastructure to the Asian group, and the Chinese conglomerate pursues a policy of soft absorption with the gradual assimilation of the cultural and value paradigms of the population into non-Chinese paradigms; 3rd – the collapse of the oligo-polistic power, the FAMGA group (USA) and the BAT group (China), the entire world economy is being reshaped into autonomous digital ecosystems that build relationships among themselves on the principles of win-win partnership; 4th – the USA, EU, Russia is actively developing digital infrastructure in Asia, Africa, South America to form a new colonial system built on the basis of digital technologies. ***Conclusions/Relevance***. As part of the scientific study, it was found that the digital sovereignty of the state directly depends on the level of digital maturity of the national economy and the digital responsibility of society's behavior. Taking into account the passage of the global economic system to the point of no return – the onset of the era of Industry 4.0 - the issue of ensuring the digital sovereignty of the state is becoming a new priority in the agenda for future development. ***Application***. The results obtained in the process of scientific research can be used by the authorities and management as a theoretical and practical basis for making appropriate decisions in the field of improving the processes of digital transformation of various levels of society, and by business representatives – for adjusting business development strategies based on taking into account relevant digital challenges and threats.

Keywords: *digital sovereignty, Industry 4.0, technology infrastructure, digital maturity, cyber threats*

Введение

Четвертая промышленная революция (именуемая также Индустрией 4.0) является одной из самых неоднозначных точек невозврата для всей мировой социально-экономической системы. Основой непредсказуемости ее траектории развития является вовлечение в орбиту своих интересов всех государств мира, независимо от их уровня экономического и технологического развития. Ключевой постулат Индустрии 4.0 – информационная открытость и транспарентность социально-экономических систем – стал яблоком раздора для национальных государственных институтов управления, т.к., *во-первых*, при росте информационной прозрачности сложнее защищать национальные интересы и безопасность государства; *во-вторых*, мировой угрозой XXI века стал взрывной рост хакерских структур, приобретающих все более системный и организованный характер, способных к совершению все более масштабных атак (последний пример: остановка в США крупнейшего трубопровода Colonial Pipeline после кибератак группировки DarkSide в начале мая 2021 г.); *в-третьих*, цифровые реформы, принесенные Индустрией 4.0, привели к смене ресурсной конкурентной парадигмы на интеллектуальную.

В целом же можно заключить, что бизнес-модель цифровой экономики, как основной продукт четвертой промышленной революции, практически вся построена на экстремальных цифровых вызовах:

с одной стороны, наблюдается ярко выраженная мотивация к расширению доступности персональных данных и активное развитие институтов цифрового содружества стран, поощрение их к трансграничному цифровому содружеству и формированию digital-ассоциаций;

с другой стороны, сегодня в мире отмечается рост сепаратистских настроений и деинтернационализации стран ввиду учащения возникновения в мировой экономической системе «эффекта домино», при котором наиболее вовлеченные в цифровой диалог страны становятся жертвами собственной открытости и слепого следования идеалам научно-технического прогресса.

В этой связи актуализируется проблема сохранения и обеспечения цифрового суверенитета и цифровой безопасности, как отдельных стран мира, так различных рыночных субъектов.

Обзор литературы и исследований

Генезис понятия «суверенитет» восходит к периоду формирования института римского права и означает в общем виде «власть отдельных лиц или определенным образом упорядоченной группы лиц в форме института над некоторой территорией» (Hinsley, 1986, pp. 68-69), т.е. понятие носило исключительно функциональное определение для обозначения верховенства одних лиц над другими (ролевая теория власти) (Равочкин, 2018).

Более современная трактовка суверенитета связана с научными работами Н. Макиавелли, Т. Гоббса и Ж. Бодена, которые рассматривали данную дефиницию через призму возможностей и угроз реализации собственных интересов для некоторого политического института или социально-экономического образования (бихевиористическая теория власти) (Кильметова, 2018; Митюрёва, 2015).

Именно с подачи разработанных ими политических концепций и теорий была сформирована основа для рассмотрения суверенитета не только как категории, характеризующей расстановку сил внутри некоторого политико-экономического образования, но и как агрегированный показатель самостоятельности государственных институтов на международной арене, однако акцент все же делался на политических механизмах реализации публичных интересов отдельных государств.

Непосредственно термин «цифровой суверенитет» связывают с именами Дж. Вестермана и В. Дхара[1], которые в рамках национального исследовательского проекта развития системы Big Data предложили ввести в узкий, профессиональный оборот дефиницию, характеризующую

[1] "Ведущие ученые в области цифровой экономики выступят с открытыми лекциями на FINOPOLIS 2018", доступно по адресу: https://fomag.ru/news/vedushchie-uchenye-v-oblasti-tsifrovoy-ekonomiki-vystupyat-s-otkrytymi-lektsiyami-na-finopolis-2018/ (Дата обращения 05.05.2021).

степень автономности и защищенности цифровой инфраструктуры страны от внешних вызовов и угроз (рассматривались, прежде всего, технологические риски, связанные с хакерскими атаками).

Данная идея получила широкий отклик в кругу специалистов, занимающихся вопросами кибербезопасности, но по-настоящему глубоко и со строгой научностью данный термин начал рассматриваться только в конце 90-х гг. XX в. – нач. XXI в. в работах Г. Перрита (Perritt, 1998), Дж. Раухоуфера, Ц. Бовдена (Rauhofer and Bowden, 2013).

Благодаря вкладу указанных немецких ученых, были выделены самостоятельные субструктуры цифрового суверенитета: технологический суверенитет и суверенитет данных. Причем аргументирование такого выделения было тесно связано с анализом механизма реализации национальной программы Hi-Tech Стратегии Германии до 2020 г. (ключевой агент – Siemens.gmbh) (рисунок 1).

Рис. 1. / Fig. 1. Термин «цифровой суверенитет»: структурный состав и эволюция / The term «digital sovereignty»: structural composition and evolution

Источник / Source: составлено авторами по данным / compiled by the authors according to the data (Nugraha and Sastrosubroto, 2015, p. 469-470).

Как видно из представленного рисунка 1, первым этапом эволюции термина «цифровой суверенитет» считается 2000-2008 гг., когда активно развивалась практика простого сбора данных, а уже ближе к 2008 г. – их BDA-анализ (Big Data Analyses).

По мнению Т. Мауэра и Р. Моргуса (T. Mauer, R. Morgus), на данном этапе эволюции акцентировалось внимание на нахождении баланса информационных интересов сторон: приватности информации о пользователе (физическом или юридическом лице) и коммерческой полезности собираемых сведений, т.е. сферой применения данного компонента суверенитета являлся преимущественно рынок, а, значит, в его отношении действовали рыночные теории и

законы (закон спроса и предложения, теория асимметричности информации) (Maurer, Skierka and Morgus, 2015, pp. 57-58).

По мере развития информационной инфраструктуры в масштабах национальной экономики и формирования спроса на кросс-секторальное взаимодействие физических и «виртуальных» (высокотехнологичных) бизнесов актуальным стал вопрос методологического обеспечения технологического суверенитета, который уже должен был обеспечивать защиту информации не только в рамках индивидуальных актов обмена данными, но в рамках множественных коммуникаций между отраслями и сферами рынка (Kukutai and Taylor (eds), 2016, p. 147).

На наш взгляд, цифровой суверенитет – завершающая стадия цикла цифровых реформ социально-экономической системы государства, который является, *с одной стороны*, агрегированным выражением самостоятельности изъявления и практического воплощения частных и публичных интересов рыночных и государственных стейкхолдеров как в границах системы, так и при осуществлении коммуникаций с внешним окружением, *с другой* – оценочным критерием устойчивости архитектуры социально-экономической бизнес-модели перед внешними информационными вызовами и угрозами различного происхождения и ее способности к адаптации и проактивной защите собственных интересов в цифровой сфере.

Проведенный контент-анализ научной литературы показал, что в мировой практике процесс формирования профессиональной, затем экономико-правовой, и в завершении научной дефиниции «цифровой суверенитет» включает в себя четыре временных шага (таблица 1).

Таблица 1 / Table 1

Основные этапы формирования термина «цифровой суверенитет» в мировой профессиональной, экономико-правовой и научной мысли / The main stages of the formation of the term «digital sovereignty» in the world of professional, economic, legal and scientific thought

Наименование этапа / хронологические границы	Характеристика этапа
1. Информационно-правовой этап (1940-1980 гг.)	*Основа для формирования* – международные юридические акты в области прав и свобод человека: Всеобщая декларация прав человека (1948 г.) и Международный пакт о гражданских и политических правах (1966 г.). *Вклад этапа* – юридическое закрепление прав и свобод человека на получение и пользование информацией, обеспечение беспрепятственности доступа к информационным ресурсам с учетом «разумной ответственности» за ее содержание и применение. *Особенности понимания дефиниции «цифровой суверенитет»* – термин рассматривался как мера предоставляемых государством свобод граждан к информации, свобода выражения мнений с применением средств СМИ и информационно-телекоммуникационной инфраструктуры (мировой рейтинг Civil liberties index, формируется Агентством национальной безопасности США с 1952 г.[2]). *Ключевой постулат этапа* – мировой прогресс невозможен без информационной прозрачности и свободы: чем свободнее движется информация между странами, тем быстрее человечество развивается.
2. Кибернетический этап (1990-2000 гг.)	*Основа для формирования* – в *Великобритании* для обеспечения превентивного регулирования Интернета планируется принятие Закона о защите граждан и бизнеса от цифрового социального вреда[3]; – в *ЕС* основополагающими документами, регулирующими работу сети

[2] "Civil Liberties and Privacy" (май 2021), доступно по адресу: https://www.nsa.gov/about/civil-liberties/ (Дата обращения 08.05.2021 г.).

[3] "В Британии планируют создать регулятор для интернета", (май 2021), доступно по адресу: https://jrnlst.ru/regulation#:~:text=Между%20тем%20в%20Великобритании%20считают%2C,и%20Instagram%20верифицировать%20возраст%20пользователей (Дата обращения 09.05.2021).

Наименование этапа / хронологические границы	Характеристика этапа
	Internet, является Директива Еврокомиссии 95/46/ЕС «О защите данных» (1995 г.) и «Общие правила защиты данных» (General Data Protection Regulation, GDPR) (2016 г.). *Особенности понимания дефиниции «цифровой суверенитет»* – термин рассматривался как определенный набор критериальных характеристик вовлеченности государства при реализации частных и публичных интересов в мировое информационное пространство. *Ключевой постулат этапа* – чем больше государство поощряет свободу информационных потоков, тем быстрее идет развитие института гражданского общества.
3. Этап суверенитета персональных данных (2001-2016 гг.)	*Основа для формирования* – судебные прецеденты, возникающие в результате правовых коллизий и пробелов в защите персональных данных и их коммерческого использования крупнейшими интернет-агрегаторами (группа FAMGA (Facebook, Amazon, Microsoft, Google, Apple), YouTube, Yandex, Baidu). *Вклад этапа* – активное развитие национальных механизмов административного, технического и юридического регулирования, контроля и защиты информации и персональных данных граждан, и юридических лиц: – *в США* были уточнены положения Закона о частной информации (Privacy Act of 1974) и Закона о защите частной жизни (Privacy Protection Act of 198)[4]; – в *ЕС* в 2016 г. был принят Общеевропейский регламент о персональных данных (General Data Protection Regulation, GDPR)[5], который построен на анализе мировых судебных споров в области защиты персональной информации и лучших практик обеспечения кибербезопасности, и собственно, завершает очередной этап развития цифрового суверенитета в ЕС и мире. *Особенности понимания дефиниции «цифровой суверенитет»* – это инструмент влияния на национальную экономику, поведение граждан, деловую репутацию бизнеса, а также лоббирование частных корпоративных интересов государств с сильнейшей цифровой инфраструктурой (США, Китай, Индия, в перспективе – Россия). *Ключевой постулат этапа* – цифровой суверенитет можно и нужно использовать в экономической и политической борьбе наравне с традиционными инструментами военной силы.
4. Этап суверенитета цифровых экосистем (2016 г. – наст. вр.)	*Основа для формирования* – нарастание конфликта интересов между высокотехнологичными экосистемами, построенными на базе мегабизнесов FAMGA (США) и BAT (Baidu, Alibaba, Tencent, Китай) и формирующейся экосистемой в РФ на базе ПАО «Сбербанк», ООО «Яндекс» и ГК «Ростех». *Вклад этапа* – активное вовлечение научных кругов в исследование проблем цифрового суверенитета страны, методологии его оценки и управления, а также разработки действенных механизмов противодействия деструктивным процессам влияния сети Internet на общественно-политические и экономические убеждения граждан. *Особенности понимания дефиниции «цифровой суверенитет»* – это новый политический и экономический фактор ведения гибридной войны в виртуальном пространстве мировой сети Internet, обладающий реальной силой влияния и уникальными сетевыми эффектами распространения и мультипликации.

[4] "Защита персональных данных за рубежом: США", доступно по адресу: http://www.weta.ru/privacy-comments-us-law-analysis.php (Дата обращения 09.05.2021).

[5] General Data Protection Regulation (2020), "Регламент Евросоюза о персональных данных", доступно по адресу: https://www.tadviser.ru/index.php/Статья:GDPR_(Регламент_Евросоюза_о_персональных_данных)#:~:text=В%20мае%202016%20года%20в,о%20свободном%20движении%20таких%20данных)) (Дата обращения 09.05.2021).

Наименование этапа / хронологические границы	Характеристика этапа
	Ключевой постулат этапа – цифровой суверенитет – стратегический, политико-экономический ресурс государства, своеобразная «валюта» и мера самостоятельности политического и экономического поведения страны в мировой системе рыночных отношений.

Источник / Source: составлено авторами по данным (Ефремов, 2017, с. 213-214; Стукалов, 2017, с. 131) / compiled by the authors according to the data (Efremov, 2017, p. 213-214; Stukalov, 2017, p. 131).

Как следует из описания этапов эволюции дефиниции «цифровой суверенитет» в мировой профессиональной, экономико-правовой и научной мысли, между простым «любопытством» и узким профессиональным термином и важным политическим и экономическим аспектом, характеризующим уровень свободы поведения государства прошло немногим больше двадцати лет, причем именно в эти два десятилетия произошло переосмысление постулатов дефиниции от драйвера прогресса и мирового благополучия к военному инструменту «завтрашнего дня».

Результаты

В российской практике введение в терминологический оборот «цифрового суверенитета» произошло только в 2016 г. и связано с именами Н.Н. Федотова (ведущий аналитик компании в области кибербезопасности InfoWatch) и И.С. Ашманова (генеральный директор компании, занимающейся маркетинговой разведкой «Ашманов и партнёры»), которые определяют термин как «самостоятельность и защищенность частных и публичных акторов в национальном и мировом цифровом пространстве» (Бухарин, 2016, с. 87).

В настоящее время как в отечественном, так и зарубежном научном обороте не содержится унифицированного определения термина «цифровой суверенитет», что объясняется высокой индивидуальностью целей и задач основных участников его формирования: крупнейших корпораций в сфере информационно-компьютерных технологий, государственных институтов национальной безопасности, публичных и частных акторов информационного пространства.

Для выявления существенных различий авторами был проведен компаративный анализ мотивирующих предпосылок и целевых установок при формировании цифрового суверенитета государства на примере США, ЕС и Российской Федерации (таблица 2).

Таблица 2 / Table 2

Мотивирующие предпосылки и целевые установки формирования цифрового суверенитета государства на примере РФ, США и ЕС / Motivating preconditions and targets for the formation of digital sovereignty of the state on the example of the Russian Federation, the United States and the EU

Наименование показателя	РФ	США	ЕС
1. Источник мотивации формирования цифрового суверенитета	– количественная и качественная эскалация вызовов и угроз в национальном и международном киберпространстве; – целевые установки профильных государственных программ (Национальная	– неуправляемое разрастание зоны влияния через цифровую инфраструктуру группы FAMGA; – военный интерес к использованию цифровых сервисов; – политические цели поддержания мирового	– стратегические интересы политических лидеров снижения технологической зависимости от США; – формирование нового полюса силы – центра цифровых компетенций; – уязвимость критических объектов инфраструктуры от хакерских атак;

Наименование показателя	РФ	США	ЕС
	программа «Цифровая экономика»[6], федеральный проект «Цифровое государственное управление»[7]); – повышение технологической автономии от потенциальных военных противников (США).	лидерства в высокотехнологичной индустрии.	– необходимость консолидации усилий разобщенных национальных программ строительства цифровой экономики в магистральные программы (Стратегия единого цифрового рынка ЕС, 2015 г.), Декларация ОЭСР «Инновации, рост и социальное благополучие».
2. Механизм формирования цифрового суверенитета	Государственный регуляторный институт (Министерство связи и массовых коммуникаций) вместе с профильными инфраструктурными акторами (ПАО «Ростелеком», федеральные провайдеры) и прикладными разработчиками (ГК «Ростех») формируют систему адаптивного контроля за информационными потоками и потенциальными киберугрозами национальной безопасности, исходя из критериев, закрепленных в Указе Президента РФ «О Стратегии национальной безопасности Российской Федерации» № 683 от 31.12.2015 г.[8].	Согласование корпоративных стратегий группы FAMGA и национальных целей, и задач с группой государственных стейкхолдеров (АНБ, ЦРУ, Пентагон, ФБР, Министерство внутренней безопасности), т.е., по существу, формируется государственно-частное партнерство с условием предоставления требуемых данных контролирующим органам[9].	Включает в себя национальные (страновые) и наднациональные (союзные) органы регуляции рынка ИКТ, которые разрабатывают единую стратегию информационной защиты ЕС и развития союзного рынка ИКТ – Генеральный Директорат по информационному обществу, Форум информационного общества ЕС с опорой на ключевых игроков рынка – Revolut, MONZO, N26, Starling Bank, DeutchBank (ЕС)[10].

[6] Распоряжение Правительства РФ от 28.07.2017 г. № 1632-р, “Цифровая экономика Российской Федерации”, доступно по адресу: http://static.government.ru/media/files/9gFM4FHj4PsB79I5v7yLVuPgu4bvR7M0.pdf (Дата доступа 05.05.2021).

[7] “Паспорт федерального проекта «Цифровое государственное управление»”, доступно по адресу: https://digital.ac.gov.ru/poleznaya-informaciya/material/Паспорт-федерального-проекта-Цифровое-государственное-управление.pdf (Дата обращения 02.05.2021).

[8] “Указ Президента РФ «О Стратегии национальной безопасности Российской Федерации» № 683”, доступно по адресу: http://www.consultant.ru/document/cons_doc_LAW_191669/ (Дата обращения 09.05.2021).

9 “Цензура (контроль и анонимность) в интернете. Мировой опыт” (2021), доступно по адресу: https://www.tadviser.ru/index.php/Статья:Цензура_(контроль_и_анонимность)_в_интернете._Мировой_опыт#. (Дата обращения 09.05.2021)

10 “Centre for Research in Financial Technologies and Digital Economy SKOLKOVO-NES”, доступно по адресу: https://finance.skolkovo.ru/downloads/documents/FinChair/Research_Reports/SKOLKOVO_Digital_transformation_of_financial_services_Report_Full_2019-11_ru.pdf

Наименование показателя	РФ	США	ЕС
3. Финансирование механизма управления цифровым суверенитетом	– бюджетные и внебюджетные расходы, закрепленные в программе «Цифровая экономика»; – специальные целевые фонды Роскомнадзора, Минкомсвязи, ФСБ; – частные фонды по развитию киберзащиты крупнейших ИКТ-бизнесов РФ (Kasperskiy.Lab).	– частные фонды и R&D-программы развития киберзащиты группы FAMGA; – государственные военные программы интернет-разведки, курируемые Министерством обороны США; – внебюджетные целевые фонды ФБР, АНБ, Министерства кибербезопасности.	– специальные программные и проектные фонды ЕС: Horizon 2020, IMPETUS, ENSURESEC[11]; – национальные программы развития киберзащиты и цифровой безопасности.
4. Целевые установки формирования цифрового суверенитета	– обеспечение технологической независимости государства от мировых центров ИКТ, прежде всего, FAMGA (США) и BAT (Китай); – формирование действенного механизма защиты цифровой инфраструктуры от хакерских атак; – военно-политическое и технологическое лидерство в Евразийском экономическом союзе.	– дальнейшая инкорпорация продуктов FAMGA в мировое информационное пространство; – развитие государственно-частного военизированного института для проведения кибератак; – противодействие растущим центробежным силам формирования многополярного мира (ЕС, Китай, РФ).	– формирование единого союзного механизма защиты от кибератак[12]; – развитие государственного института кибервойск для ведения гибридной войны; – формирование собственной цифровой инфраструктуры для снижения технологической зависимости от США, Китая, Японии, РФ[13].

Источник / Source: составлено авторами по данным (Ефремов, 2017, с. 213-214; Липунцов, 2011, с. 90-91) / compiled by the authors according to the data (Efremov, 2017, pp. 213-214; Lipuntsov, 2011, pp. 90-91).

Из приведенных в таблице 2 данных видно, что цели и задачи формирования и обеспечения (защиты) цифрового суверенитета в РФ, США и ЕС достаточно сильно отличаются. Причем в отношении РФ и США четко прослеживается политический и военный акцент интересов к данному термину, что обусловлено ростом напряженности отношений между данными странами.

В настоящее время в России, равно как и во всем мире, не сложилось единой методики оценки цифрового суверенитета. Это связано со значительной дифференциацией целей, параметров и собственно уровня цифрового развития различных государств. Исходя из этого, авторами были проанализированы наиболее существенные оценочные критерии цифровой самостоятельности государства, сформированные на основе изучения методики расчетов Индекса развития электронного правительства ООН и Индекса развития информационно-коммуникационных технологий Международного союза электросвязи[14] (таблица 3).

11 "ЕС выделяет 38 млн. евро на защиту инфраструктуры от киберугроз" (2020), доступно по адресу: https://www.dw.com/ru/ec-выделяет-38-млн-евро-на-защиту-инфраструктуры-от-киберугроз/a-53818150 (Дата обращения 10.05.2021)

12 "Еврокомиссия намерена создать сеть центров по кибербезопасности" (2020), доступно по адресу: https://news.myseldon.com/ru/news/index/242547890 (Дата обращения 10.05.2021).

13 "Правила кибербезопасности ЕС: государства-члены определили поставщиков «основных услуг»" (2019), доступно по адресу: https://globalcentre.hse.ru/news/314936968.html (Дата обращения 11.05.2021).

14 "ИНТЕГРАЦИОННЫЙ «ПЛАН ГОЭЛРО» ДЛЯ XXI ВЕКА" (2021), доступно по адресу: https://globalaffairs.ru/articles/czifrovoj-suverenitet-eaes/ (Дата обращения 11.05.2021).

Таблица 3 / Table 3

Ключевые показатели формирования и развития цифрового суверенитета РФ в 2015-2020 гг. / Key indicators of the formation and development of the digital sovereignty of the Russian Federation in 2015-2020

Показатели	2015 г.	2016 г.	2017 г.	2018 г.	2019 г.	2020 г. *(оценка)*
1. Удельный вес расходов на цифровые реформы национальной экономики, % от ВВП	…	1,7	3,6	3,6	3,7	*4,5*
2. Средневзвешенный уровень инкорпорации ИКТ в национальную экономику, %	24	25	27	29	…	*31,3*
3. Индекс развития национального рынка ИКТ	6,79	6,91	7,07	7,32	…	*8,03*
4. Индекс цифровизации государственного управления	0,73	…	0,72	…	0,77	*0,81*
5. Удельный вес цифровизации приоритетных государственных услуг, соответствующих стандартам мастер-данных, %	-	-	-	3,0	6,0	*15,0*
6. Удельный вес цифровизации документооборота между РФ и странами-членами ЕАЭС и ЕЭК, %	-	-	-	-	10,0	*20,0*

Источник / Source: составлено авторами по данным ("О Стратегии развития информационного общества в Российской Федерации на 2017-2030 годы"; Абдрахманова и др., 2017; Абдрахманова и др., 2018; Абдрахманова и др. 2019, Абдрахманова и др. 2020; "Цифровое правительство – следующий этап развития", 2020) / compiled by the authors according to the data ("On the Strategy for the Development of the Information Society in the Russian Federation for 2017-2030"; Abdrakhmanova. et al, 2017, Abdrakhmanova. et al, 2018, Abdrakhmanova. et al, 2019, Abdrakhmanova. et al, 2020, Indicators of the Digital Economy: statistical compendium: 2017, 2018, 2019, 2020; "Digital government – the next stage of development", 2020).

Таким образом, из приведенных выше данных следует, что РФ достаточно активно и устойчиво развивает основные блоки цифрового суверенитета, и, прежде всего, в части цифровизации государственного управления: в 2009 г. был запущен Единый и региональный порталы государственных и муниципальных услуг (в 2015-2017 гг. прошел глубокий реинжиниринг программной платформы, позволяющий блокировать атаки бот-роботов и определять геолокацию аккаунтов посетителей сайта); в 2010 г. была запущена Единая система идентификации и аутентификации (ЕСИА), позволяющая гражданам РФ получать доступ к суперсервисам на госуслугах (в 2017-2018 гг. была проведена модернизация системы криптозащиты данных пользователей и обмена информацией с государственными службами); в 2010-2012 гг. была запущена система межведомственного электронного взаимодействия (СМЭВ), позволяющая в виртуальном формате обмениваться данными между различными уровнями государственной власти, а также обсуждать нестандартные прецеденты в режиме реального времени.

Используя данные отчета InfraOne Research «Инвестиции в инфраструктуру. Информационные технологии», представим анализ структуры расходов на формирование и защиту цифрового суверенитета РФ (рисунок 2).

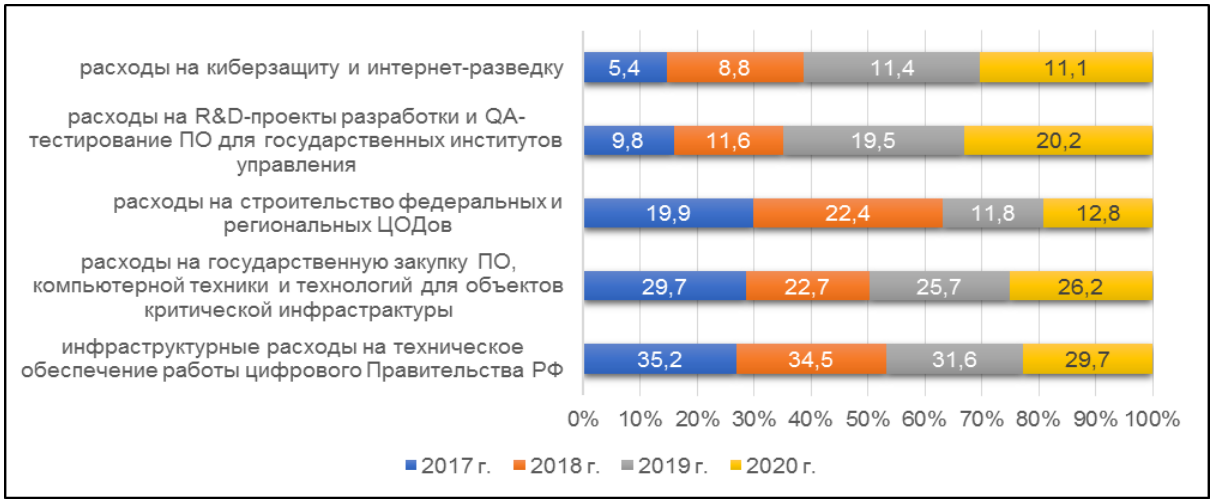

Рис. 2. / Fig. 2. Структура расходов на формирование и защиту цифрового суверенитета РФ в 2017-2020 гг., в % / The structure of expenditures on the formation and protection of the digital sovereignty of the Russian Federation in 2017-2020, in %

Источник / Source: составлено авторами по данным (Абдрахманова и др., 2017; Абдрахманова и др., 2018; Абдрахманова и др. 2019, Абдрахманова и др. 2020) / compiled by the authors according to the data (Abdrakhmanova. et al, 2017, Abdrakhmanova. et al, 2018, Abdrakhmanova. et al, 2019, Abdrakhmanova. et al, 2020).

Как видно из динамики расходов в 2017-2020 гг. ключевое место занимают инфраструктурные расходы на техническое обеспечение работы цифрового Правительства РФ – в среднем они составили 32,8%, на втором месте – расходы на госзакупку ПО, компьютерной техники и технологий для объектов критической инфраструктуры – в среднем они составили 26,0%, на третьем месте – расходы на строительство федеральных и региональных ЦОДов – 16,7%. Таким образом, стратегия обеспечения цифрового суверенитета РФ носит преимущественно защитный характер, что обусловлено невозможностью единовременного отказа от импорта продуктов ИКТ.

В заключение рассмотрим основные результаты реализации программы технологического импортозамещения в 2016-2019 гг. (таблица 4).

Таблица 4 / Table 4

Основные результаты реализации программы технологического импортозамещения в 2016-2019 гг., % / Key results of the implementation of the technological import substitution program in 2016-2019, %

Показатели	2016 г.	2017 г.	2018 г.	2019 г.
1. Удельный вес инновационных товаров-субститутов, реализованных на внутреннем рынке, %	7,7	8,4	6,6	5,8
2. Увеличение доли внутреннего рынка присутствия ИКТ-бизнесов за счет производства импортозамещающих товаров, %	2,2	2,5	2,7	1,9
3. Удельный вес продукции сферы высоких технологий, реализованных на внутреннем рынке в рамках программы импортозамещения, %	6,4	6,6	8,0	8,0

Источник / Source: составлено авторами по данным (Гохберг и др., 2020; Гохберг и др., 2019; Городникова и др., 2018; Технопарки России: ежегодный обзор, 2020) / compiled by the authors according to the data (Gokhberg et al, 2020; Gokhberg et al, 2019; Gorodnikova et al, 2018; Technoparks of Russia: annual review, 2020).

Как следует из данных таблицы 4, программа импортозамещения РФ последовательно укрепляет позиции отечественных ИКТ в деловой сфере и органах государственного

управления. Отдельно следует отметить сильное влияние административных рычагов в форме прямых запретов на импорт отдельных видов продукции ИКТ: Постановление Правительства РФ «Об установлении запрета на допуск отдельных видов товаров машиностроения, происходящих из иностранных государств, для целей осуществления закупок для обеспечения государственных и муниципальных нужд» № 656[15]; Постановление Правительства РФ «Об установлении запрета на допуск программного обеспечения, происходящего из иностранных государств, для целей осуществления закупок для обеспечения государственных и муниципальных нужд» №1236[16].

Для оценки эффективности принимаемых политическими лидерами и профильными государственными институтами управления мер по формированию и защите цифрового суверенитета РФ авторами был проведен анализ динамики наиболее важных индексов, отражающих как цифровую зрелость национальной экономики, так и ее защищенность перед внешними цифровыми вызовами и угрозами (рисунок 3).

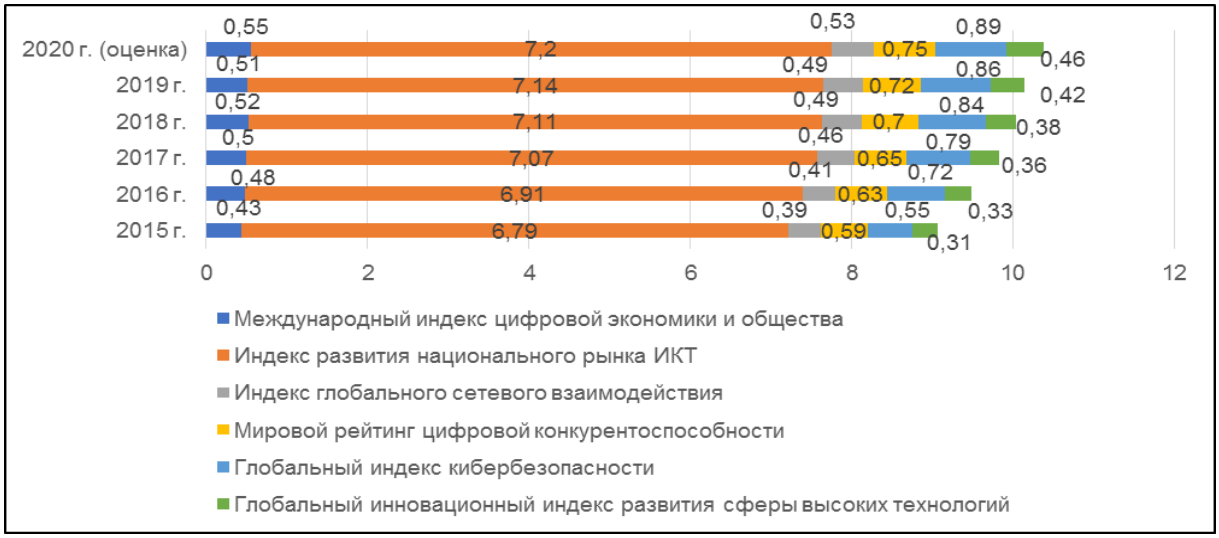

Рис. 3. / Fig. 3. Отдельные показатели цифрового суверенитета РФ в международных рейтингах развития цифровой экономики и общества в 2015-2020 гг., пункты / Selected indicators of the digital sovereignty of the Russian Federation in the international ratings of the development of the digital economy and society in 2015-2020, items

Источник / Source: составлено авторами по данным (Абдрахманова и др., 2017; Абдрахманова и др., 2018; Абдрахманова и др. 2019, Абдрахманова и др. 2020) / compiled by the authors according to the data (Abdrakhmanova. at al, 2017, Abdrakhmanova. at al, 2018, Abdrakhmanova. at al, 2019, Abdrakhmanova. at al, 2020).

Согласно представленному рисунку 3, в нашей стране основным фактором обеспечения цифрового суверенитета является развитие национального рынка ИКТ (РФ оценочно занимает 38 место среди 167 стран по данным за 2020 г.). Вторым по значимости параметром является повышение места России в рейтинге кибербезопасности: по данным за 2020 г. страна заняла 19 место по этому показателю, причем локомотивом роста выступили технические решения в области обеспечения кибербезопасности банковской системы и объектов критической инфраструктуры.

[15] Постановление Правительства РФ от 14.07.2014 N 656 (ред. от 30.04.2020),"Об установлении запрета на допуск отдельных видов товаров машиностроения, происходящих из иностранных государств, для целей осуществления закупок для обеспечения государственных и муниципальных нужд", доступно по адресу: http://www.consultant.ru/document/cons_doc_LAW_165608/

[16] Постановление Правительства РФ от 16 ноября 2015 г. N 1236 (2020), "Об установлении запрета на допуск программного обеспечения, происходящего из иностранных государств, для целей осуществления закупок для обеспечения государственных и муниципальных нужд", доступно по адресу: https://base.garant.ru/71252170/

В завершение научного исследования авторы обобщили барьеры и представили возможные пути развития цифрового суверенитета РФ (таблица 5).

Таблица 5 / Table 5

Характеристика барьеров и возможных путей развития цифрового суверенитета РФ / Characteristics of barriers and possible ways to develop the digital sovereignty of the Russian Federation

Барьеры формирования цифрового суверенитета	Возможные пути развития цифрового суверенитета
1. *Высокая централизация контроля над сетью Internet в полномочиях государственных институтов* – Роскомнадзоре, Минцифры, что приводит к дисбалансу интересов ключевых акторов цифровой экономики – деловых кругов и граждан в их доступе к информационным ресурсам и сервисам	1. Для более эффективного регулирования национального сегмента сети и ее взаимодействия с мировым пространством рекомендуется инициировать создание института информационного саморегулирования цифровой экономики по отраслям, что позволит более гибко реагировать на сигналы рыночных стейкхолдеров и граждан-пользователей
2. *Программно-целевой формат управления цифровизацией государства* – в РФ доминирующую роль в реализации цифровых реформ и проектов киберзащиты играют государственные программы, финансируемые за счет средств бюджета или специальных государственных фондов, что ограничивает круг потенциальных участников таких программ государственными корпорациями (ГК «Ростех», ГК «Роснано») и отдельными предприятиями сферы военно-промышленного комплекса	2. Активизация вовлечения крупнейших бизнесов РФ в процессы финансирования проектов обеспечения кибербезопасности объектов критической инфраструктуры, а также организацию внутреннего трансферта технологий криптозащиты и информационного аудита для создания действенной системы частного финансирования инициатив в области кибербезопасности
3. *Ярко выраженный военно-политический акцент формирования цифрового суверенитета* – политические лидеры РФ открыто декларируют политическую и военную роль цифрового суверенитета в обеспечении преимуществ и влияния РФ на международной политической арене и лидерства в регионе (например, в составе ЕврАзЭС)	3. Смещение фокуса с политической роли цифрового суверенитета возможно путем проведения национальных и международных хакатонов и соревнований в сфере кибербезопасности, выявления уязвимостей и QA-анализа среди школьников и студентов, а также представителей IT-бизнеса для поиска кадров, для обмена лучшим опытом обеспечения безопасности в цифровой сфере
4. *Эскалация политики санкций в отношении трансферта технологий и решений для обеспечения киберзащиты* – ограничение доступа для РФ к лучшим практикам обеспечения кибербезопасности, а также эмбарго на импорт технологий увеличивает издержки на их получение и обостряет слабые точки национальной цифровой инфраструктуры	4. Развитие технологической кооперации и трансферта технологий с восточными партнерами (Китай, Индия) на принципах win-win партнерства, а также формированием системы юридических и политических противовесов, исключающих враждебное использование инновационных разработок в отношении друг друга
5. *Распыленность внутреннего потенциала лидеров рынка ИКТ* – в РФ имеются ярко выраженные лидеры отрасли (т.н. хедлайнеры), которые задают тренд развития цифровых технологий в конкретной отрасли, но при этом они не склонны к кооперации с более мелкими бизнесами, а межфирменную кооперацию рассматривают как инструмент расширения рыночного влияния	5. Формирование федеральной сети бизнес-инкубаторов в области кибербезопасности с привлечением институтов финансового развития (ВЭБ.РФ, АО «Корпорация МСП», АО «РВК»), а также действующей региональной инновационной инфраструктуры (технопарки, кластеры, особые экономические зоны), в т.ч. с привлечением иностранных партнеров из дружественных РФ государств

Источник / Source: составлено авторами по данным (Васильковский и Игнатов, 2020, с. 14-17; Ефременко, 2020, с. 37-40) / compiled by the authors according to the data (Vasilkovsky and Ignatov, 2020, p. 14-17; Efremenko, 2020, p. 37-40).

Как видно из данных таблицы 5, в РФ в настоящее время сложились достаточно сильные властные императивы регуляции информационного пространства как внутри страны, так и при коммуникациях с внешним миром, но именно централизация управления несет в себе существенные ограничения для развития цифровой экономики в целом, поэтому лучшим решением в сложившихся условиях будет формирование диалогической государственно-частной модели регуляции информационных потоков в сети Internet. Это позволит разрешить следующие противоречия:

во-первых, снизится градус напряжения со стороны инициаторов технологических санкций, т.к. они увидят готовность политической элиты к диалогу сторон, внимание к проблеме агентских отношений в цифровой реальности;

во-вторых, появится возможность инфраструктурной диверсификации в отношении ключевых регуляторных институтов – если в отношение одного из них будет объявлен политический и (или) технологический бойкот, то его дублеры смогут практически полностью возместить утраченные функции;

в-третьих, активное вовлечение частных структур в организацию цифрового суверенитета означает снижение долговой нагрузки на бюджетные источники, а также предоставляет более гибкое и качественное технологическое обеспечение реализации функций безопасности;

в-четвертых, при росте вовлеченности рыночных акторов в вопросы кибербезопасности, происходит повышение уровня информационной культуры как бизнеса, так и населения, так первые активно реализуют образовательные и разъяснительные мероприятия с целью вовлечения клиентов в диалог о безопасном поведение в цифровой реальности.

В заключение представим четыре основных сценария будущего цифрового суверенитета РФ, используя метод Форсайта «4 мира» (таблица 6).

Таблица 6 / Table 6

Сценарии будущего цифрового суверенитета Российской Федерации (построено по методу «4 мира») / Scenarios of the future digital sovereignty of the Russian Federation (built using the «4 worlds» method)

Сценарий	Характеристика сценария
1. Красный мир (мир биполярного лидера)	*Исходные предпосылки*: – группа FAMGA (США) и группа BAT (Китай) стали мировыми центрами управления цифровой экономикой; – РФ не смогла выстроить действенную национальную инфраструктуру и находится в зависимом положении от указанных групп; – информационная инфраструктура ЕС находится под управлением группы FAMGA (США). *Характеристика мира*: цифровой суверенитет стал объектом и средством влияния мировых лидеров на поведение целых государств и союзных образований, акцент на военно-политической роли цифрового суверенитета. Хакерские атаки перешли под контроль государственного института и осуществляются в качестве инструмента устрашения или усмирения противника. Политическая система строится на принципах цифирного диктата с предоставлением властных полномочий крупнейшим ТНК мира, управляющими персональными данными всех граждан.

Сценарий	Характеристика сценария
2. Желтый мир (цифровой монополизм Азии)	*Исходные предпосылки*: – группа компаний BAT (Китай) и новые цифровые гиганты Азии (Индия, Япония) установили мировое лидерство в Евразийском цифровом пространстве и активно оккупируют Северную и Южную Америку; – группа FAMGA (США) частично поглощается инвесторами из Азии и теряет мировую монополию; – РФ присоединяет цифровую инфраструктуру к Азиатской группе. *Характеристика мира*: китайский конгломерат проводит политику мягкого поглощения национальных интернет-провайдеров и лидеров интернета (форумы, социальные сети, ньюсмейкеров и публичных персон-инфлуенсеров на общественное мнение) с постепенной ассимиляцией культурно-ценностных парадигм населения на неокитайские. Политическое управление строится на принципе «разделяй и властвуй» – цифровой суверенитет становится объектом торгов: чем выше «политическая лояльность» Китаю, тем больше преимуществ у его обладателя.
3. Зеленый мир (мультицентризм цифровых экосистем)	*Исходные предпосылки*: – страны мира активно развивают национальные цифровые экосистемы на базе крупнейших и инновационно активных бизнесов (банки, ИТ-компании, управляющие компании национальной информационной инфраструктуры); – крах олигополистической власти группы FAMGA (США) и группы BAT (Китай). *Характеристика мира*: вся мировая экономика перекраивается в автономные цифровые экосистемы, которые выстраивают между собой отношения на принципах win-win партнерства, а для защиты собственных интересов используется цифровой суверенитет – как средство экономического и технологического давления на противников или конкурентов.
4. Голубой мир (мир цифровой колонизации)	*Исходные предпосылки*: – растущее напряжение и количество хакерских атак показало неспособность обеспечения цифровой безопасности силами отдельных государств; – гражданские протесты против сбора и коммерческого использования персональных данных. *Характеристика мира*: мировое сообщество перекраивает стандарты сотрудничества и партнёрства с ресурсной парадигмы на цифровую. ЕС активно реализует программы поддержки и развития цифровой инфраструктуры в странах Восточной Европы и Африки, США активно инкорпорирует свои технологии в обеспечение национальной безопасности в Южной Америке. РФ активно развивает цифровую инфраструктуру в странах Азии (Монголия, Казахстан, Туркменистан, Таджикистан), что означает формирование новой колониальной системы, построенной на базе цифровых технологий.

Источник / Source: составлено авторами по данным (Сюэфен, Ашмарина и Павлов, 2020, с. 495; Бейсенбаев, 2020, с. 212-214; Дмитриева, 2019, с. 144-145) / compiled by the authors according to the data (Xuefeng, Ashmarina and Pavlov, 2020, p. 495; Beisenbayev, 2020, p. 212-214; Dmitrieva, 2019, p. 144-145).

Каждый из представленных выше сценариев является вероятным отражением будущих событий, но единственно точным остается тот факт, что цифровой суверенитет государства станет объектом политической и экономической борьбы не только руководящей элиты стран, но и крупнейших бизнесов в сфере цифровых технологий.

Заключение

Результаты проведенного исследования, посвящённого выявлению и уточнению категориального аппарата, определению параметров и будущих сценариев развития цифрового суверенитета Российской Федерации в эпоху Индустрии 4.0, позволили авторам сделать следующие выводы:

1) цифровой суверенитет государства является следствием четвертой промышленной революции, обозначившей в качестве магистрального вектора развития цифровую транспарентность и открытость национальных социально-экономических систем;

2) в настоящее время цифровой суверенитет рассматривается с политической, экономической и технологической точек зрения, что обуславливает наличие плюрализма подходов на его содержательное наполнение в научной литературе;

3) считаем возможным предложить следующее определение: под *цифровым суверенитетом следует понимать критерий устойчивости архитектуры социально-экономической бизнес-модели перед внешними и внутренними цифровыми вызовами и угрозами различной природы происхождения, а также ее способности к адаптации и проактивной защите собственных интересов в цифровой сфере*;

4) развитие цифрового суверенитета России может осуществляться по следующим сценариям:

1-*ый* – РФ не смогла выстроить действенную национальную инфраструктуру и находится в зависимом положении от указанных групп, цифровой суверенитет стал объектом и средством влияния мировых лидеров на поведение целых государств и союзных образований, акцент на военно-политической роли цифрового суверенитета;

2-ой – РФ присоединяет цифровую инфраструктуру к Азиатской группе, а китайский конгломерат проводит политику мягкого поглощения с постепенной ассимиляцией культурно-ценностных парадигм населения на неокитайские парадигмы;

3-ий – крах олигополистической власти группы FAMGA (США) и группы BAT (Китай), вся мировая экономика перекраивается в автономные цифровые экосистемы, которые выстраивают между собой отношения на принципах win-win партнерства;

4-ый – США, ЕС, РФ активно развивают цифровую инфраструктуру в странах Азии, Африки, Южной Америки для формирования новой колониальной системы, построенной на базе цифровых технологий.

Литература / References

1. Абдрахманова, Г.И., Гохберг, Л.М., Кевеш, М.А. и др. (2017), *Индикаторы цифровой экономики: 2017: статистический сборник*, Нац. исслед. ун-т «Высшая школа экономики», НИУ ВШЭ, М., 320 с. [Abdrakhmanova, G.I., Gokhberg, L.M., Kevesh, M.A. at al (2017), *Indicators of digital economy: 2017: statistical collection*, Natz. researched. un-t «Higher School of Economics», HSE, M., 320 p.].

2. Абдрахманова, Г.И., Вишневский, К.О., Волкова, Г.Л., Гохберг, Л.М. и др. (2018), *Индикаторы цифровой экономики: 2018: статистический сборник*, Нац. исслед. ун-т «Высшая школа экономики», НИУ ВШЭ, М., 268 с. [Abdrakhmanova, G.I., Vishnevsky, K.O., Volkova, G.L., Gokhberg, L.M. at al (2018), *Indicators of digital economy: 2018: statistical collection*, Natz. researched. un-t «Higher School of Economics», HSE, M., 268 p.].

3. Абдрахманова, Г.И., Вишневский, К.О., Гохберг, Л.М. и др. (2019), *Индикаторы цифровой экономики: 2019: статистический сборник*, Нац. исслед. ун-т «Высшая школа экономики», НИУ ВШЭ, М., 248 с. [Abdrakhmanova, G.I., Vishnevsky, K.O., Gokhberg, L.M. at al (2019), *Indicators of digital economy: 2019: statistical collection*, Natz. researched. un-t «Higher School of Economics», HSE, M., 248 p.].

4. Абдрахманова, Г.И., Вишневский, К.О., Гохберг, Л.М. и др. (2020), *Индикаторы цифровой экономики: 2020: статистический сборник*, Нац. исслед. ун-т «Высшая школа экономики», НИУ ВШЭ, М., 360 с. [Abdrakhmanova, G.I., Vishnevsky, K.O., Gokhberg L.M. at al (2020), *Indicators of digital economy: 2020: statistical collection*, Natz. researched. un-t «Higher School of Economics», HSE, M., 360 p.].

5. Бейсенбаев, О.Т. (2020), "Сотрудничество Казахстана, России и Китая в развитии цифрового Шелкового пути: новые вызовы и перспективы*", Восточная Азия: прошлое, настоящее, будущее: Материалы 7-й международной конференции молодых востоковедов,* с. 209-219. [Beisenbaev, O.T. (2020), "Cooperation of Kazakhstan, Russia and China in the development of the digital Silk Road: new challenges and prospects", *East Asia: past, present, future: Materials of the 7th international conference of young orientalists*, pp. 209-219].

6. Бухарин, В.В. (2016), "Компоненты цифрового суверенитета Российской Федерации как техническая основа информационной безопасности", *Вестник МГИМО Университета*, №

6, с. 76-91. [Bukharin V.V. (2016), "Components of digital sovereignty of the Russian Federation as a technical basis for information security" *Bulletin of MGIMO University*, no.6, pp. 76-91].

7. Бухарова, М.М., Данилов, Л.В., Кашинова, Е.А., Кравченко, Е.И. и др. (2020), *Технопарки России: ежегодный обзор*, Ассоциация развития кластеров и технопарков России, Том 6., АКИТ РФ, М., 110 с. [Bukharov, M.M., Danilov, L.V., Kashinova, E.A., Kravchenko, E.I. at al (2020), *Technoparks of Russia: annual review*, Association for the Development of Clusters and Technology Parks of Russia, Vol. 6, AKIT of the Russian Federation, M., 110 p.].

8. Васильковский, С.А. и Игнатов, А.А. (2020), "Управление интернетом: системные диспропорции и пути их разрешения", *Вестник международных организаций: образование, наука, новая экономика,* т. 15, № 4, с. 7-29 (на русском и английском языках), doi: 10.17323/1996-7845-2020-04-01. [Vasilkovsky, S.A. and Ignatov, A.A. (2020), "Internet governance: system imbalances and ways to resolve them", *Bulletin of international organizations: education, science, new economy*, vol. 15, no. 4, pp. 7-29 (in Russian and English), doi: 10.17323/1996-7845-2020-04-01].

9. Городникова, Н.В., Гохберг, Л.М., Дитковский, К.А. и др. (2018), *Индикаторы инновационной деятельности: 2018: статистический сборник*, Нац. исслед. ун-т «Высшая школа экономики», НИУ ВШЭ, М., 344 с. [Gorodnikova, N.V., Gokhberg, L.M., Ditkovsky K.A. at al (2018), *Indicators of innovation:2018: statistical collection*, Natz. is-trail. un-t «Higher School of Economics», HSE, M., 344 p.].

10. Гохберг, Л.М., Дитковский, К.А., Евневич Е.И. и др. (2020), *Индикаторы инновационной деятельности: 2020: статистический сборник,* Нац. исслед. ун-т «Высшая школа экономики», НИУ ВШЭ, М., 336 с. [Gokhberg, L.M., Ditkovsky, K.A., Evnevich E.I. at al (2020), *Indicators of innovation: 2020: statistical collection*, Natz. researched. un-t «Higher School of Economics», HSE, M., 336 p.].

11. Гохберг, Л.М., Дитковский, К.А., Кузнецова И.А. и др. (2019), *Индикаторы инновационной деятельности: 2019: статистический сборник*, Нац. исслед. ун-т «Высшая школа экономики», НИУ ВШЭ, М., 376 с. [Gokhberg, L.M., Ditkovsky, K.A., Kuznetsova I.A. at al (2019), *Indicators of innovation: 2019: statistical collection*, Natz. is-trail. un-t «Higher School of Economics», HSE, M., 376 p.].

12. Дмитриева, М.О. (2019), "Россия и Китай в Центральной Азии: сотрудничество или соперничество", *Вестник Московского государственного областного университета. Серия: История и политические науки*, № 1, с. 139-147, doi: 10.18384/2310-676X-2019-1-139-146. [Dmitrieva, M.O. (2019), "Russia and China in Central Asia: cooperation or rivalry", *Bulletin of Moscow State Regional University. Series: History and Political Sciences*, no 1, pp. 139-147, doi: 10.18384/2310-676X-2019-1-139-146].

13. Ефременко, Д.В. (2020), "Формирование цифрового общества и геополитическая конкуренция", *Контуры глобальных трансформаций: политика, экономика, право*, т. 13, № 2, с. 25-43, doi: 10.23932/2542-0240-2020-13-2-2 25. [Efremenko, D.V. (2020), "Formation of a digital society and geopolitical competition", *Contours of global transformations: politics, economics, law*, vol. 13, no 2, pp. 25-43, doi: 10.23932/2542-0240-2020-13-2-2].

14. Ефремов, А.А. (2017), "Формирование концепции информационного суверенитета государства", *Право. Журнал Высшей школы экономики*, № 1, с. 201-215, doi: 10.17323/2072-8166.2017.1.201.215 [Efremov, A.A. (2017), "Formation of the concept of information sovereignty of the state", *Law. Journal of the Higher School of Economics*, no. 1, pp. 201-215, doi: 10.17323/2072-8166.2017.1.201.215].

15. Кильметова, Р.Р. (2018), "Политико-правовые учения Никколо Макиавелли", *Правовое государство: теория и практика,* № 4, с. 69-73. [Kilmetova, R.R. (2018), "The political and legal teachings of Niccolo Machiavelli", *The legal state: theory and practice*, no 4, pp. 69-73].

16. Липунцов, Ю.П. (2011), "Управление информационно-коммуникационными технологиями в госсекторе. Обзор зарубежного опыта", *Экономика и управление*, № 5, с. 87-92. [Lipuntsov, Yu.P. (2011), "Management of information and communication technologies in the public sector. Overview of foreign experience", *Economics and management*, no 5, pp. 87-92].

17. Митюрёва, Д.С. (2015), "Жан Боден и Томас Гоббс: в поисках идеального государя" *Вестник Кемеровского государственного университета*, т. 2, № 3, с. 44-48. [Mityureva, D.S.

(2015), “Jean Boden and Thomas Hobbes: in search of the ideal sovereign”, *Bulletin of Kemerovo State University*, vol. 2, no 3, pp. 44-48].

18. Равочкин, Н.Н. (2018), “Анализ значения философских идей в становлении политических и правовых институтов в индустриальном обществе”, *Теология. Философия. Право*, № 3, с. 53-67. [Ravochkin, N.N. (2018), “Analysis of the significance of philosophical ideas in the formation of political and legal institutions in an industrial society”, *Theology. Philosophy. Right*, no 3, pp 53-67].

19. Стукалов, А.С. (2017),“Европейская модель регулирования информационных отношений в сети Интернет”, *Проблемы экономики и юридической практики*, № 1, с. 129-133. [Stukalov, A.S. (2017), “European Model for the Regulation of Information Relations on the Internet”, *Problems of Economics and Legal Practice*, no 1, pp. 129-133].

20. Сюэфен, Ли, Ашмарина, Т.И. и Павлова И.М. (2020), “Вектор развития «Цифрового шелкового пути» – Китай-Россия*”, Образование и право,* № 4, с. 493-498. [Xuefen, Li, Ashmarina, T.I. and Pavlova I.M. (2020), “Vector of development of the Digital Silk Road – China-Russia”, *Education and Law*, no 4, pp 493-498].

21. Усманов, Д.И. и Канищев, Р.Ю. (2013), “Теория ролей и институциональных факторов, воздействующих на инновационное развитие локальных региональных рынков на уровне муниципальных образований”, *Вестник БГТУ им. В. Г. Шухова*, № 2, с. 115-121. [Usmanov, D.I. and Kanishchev, R.Yu. (2013), “Theory of roles and Institutional factors influencing the innovative development of local regional markets at the Municipal level”, *Bulletin of the V.G. Shukhov BSTU*, no. 2, pp. 115-121].

22. Усманов, Д.И. и Прядко, С.Н. (2013), “Создание и развитие стартапов при участии университетов – Российский и американский опыт”, *Вестник БГТУ им. В. Г. Шухова*, № 3, с. 94-99. [Usmanov, D.I. and Pryadko, S.N. (2013), “Creation and development of startups with the participation of universities – Russian and American experience”, *Bulletin of the V.G. Shukhov BSTU*, no. 3, pp. 94-99].

23. Усманов, Д.И., Растворцева, С.Н. и Ченцова, А.С (2014), “Обзор исследований влияния международных интеграционных процессов на социально-экономическое неравенство регионов”, *Вестник БГТУ им. В. Г. Шухова*, № 5, с. 99-105. [Usmanov, D.I., Rastvortseva, S.N. and Chentsova, A.S. (2014), “Review of studies of the Impact of International integration processes on the socio-economic inequality of regions”, *Bulletin of the V.G. Shukhov BSTU*, no. 5, pp. 99-105].

24. Усманов, Д.И. (2013), “Сущность и факторы институционального развития региональных рынков продовольствия”, *Вестник БГТУ им. В. Г. Шухова*, № 3, с. 112-118. [Usmanov, D.I. (2013), “The essence and factors of the Institutional development of regional food markets”, *Bulletin of the V. G. Shukhov BSTU*, no. 3, pp. 112-118].

25. Указ Президента Российской Федерации от 09.05.2017 г. № 203, “О Стратегии развития информационного общества в Российской Федерации на 2017-2030 годы”, доступно по адресу: http://www.kremlin.ru/acts/bank/41919 (Дата обращения 11.05.2021). [Decree of the President of the Russian Federation of 09.05.2017 No. 203, “On the Strategy for the Development of the Information Society in the Russian Federation for 2017-2030”, available at: http://www.kremlin.ru/acts/bank/41919 (Accessed 11.05.2021)].

26. “Цифровое правительство – следующий этап развития” (2020), Аналитические материалы TAdviser, доступно по адресу: https://www.tadviser.ru/index.php/Статья:Электронное_правительство_России#.(Дата обращения 06.01.2021. [“Digital government – the next stage of development” (2020), Analytical materials TAdviser, available at: https://www.tadviser.ru/index.php/Статья: Electronic _ government _ of Russia # (Accessed 06.01.2021)].

27. Hinsley, F.H. (1986), *Sovereignty*, 2nd ed., Cambridge University Press, Cambridge, MA, 258 p.

28. Kukutai T. and Taylor J. (eds) (2016), *Indigenous Data Sovereignty: Toward an Agenda (CAEPR)*, Research monograph, no. 38, pp. 139-156, Centre for Aboriginal Economic Policy Research, College of Arts and Social Sciences, The Australian National University, Canberra.

29. Maurer, T., Skierka, I. and Morgus, R. (2015), "Technological sovereignty: missing the point?", *7th international conference on Cyber conflict: Architectures in cyberspace (CyCon)*, pp. 53-68. IEEE, available at: http://ieeexplore.ieee.org/abstract/document/7158468/ (Accessed: 08.05.2021).

30. Nugraha, Y.K. and Sastrosubroto, A.S. (2015), "Towards data sovereignty in cyberspace", *3rd international conference on information and communication technology (ICoICT)*, pp. 465-471, available at: https://ieeexplore.ieee.org/document/7231469 (Accessed: 07.05.2021).

31. Perritt, Henry H. Jr. (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, issue 2, pp. 423-442.

32. Rauhofer, J. and Bowden, C. (2013), *Protecting Their Own: Fundamental Rights Implications for EU Data Sovereignty in the Cloud*, Edinburgh School of Law Research Paper. http://dx.doi.org/10.2139/ssrn.2283175.

Об авторах

Дудин Михаил Николаевич, доктор экономических наук, профессор, заместитель директора по науке, Институт проблем рынка РАН, Москва.

Шкодинский Сергей Всеволодович, доктор экономических наук, профессор, заведующий лабораторией промышленной политики и экономической безопасности, Институт проблем рынка РАН, Москва.

Усманов Далер Ирматович, кандидат экономических наук, доцент, старший научный сотрудник, Институт проблем рынка РАН, Москва.

About authors

Mikhail N. Dudin, Doctor of Sci. (Econ.), Professor, Deputy Director, Market Economy Institute of RAS, Moscow.

Sergey V. Shkodinsky, Doctor of Sci. (Econ.), Professor, Head of the Lab. of Industrial Policy and Economic Security, Market Economy Institute of RAS, Moscow.

Daler I. Usmanov, Candidate of Sci. (Econ.), Associate Professor, Senior Researcher, Market Economy Institute of the RAS, Moscow.