УДК 004.3, 339.97;339.98

Цифровое развитие государства как основа достижения цифрового суверенитета

В статье представлены результаты анализа понятия «цифровой суверенитет» в контексте зарубежных исследований и политических практик. Выделены основные составляющие цифрового суверенитета, включая технологический потенциал, цифровую трансформацию промышленности, создание и использование национального программного обеспечения и программных продуктов с открытым исходным кодом, стимулирование научно-исследовательского сектора и кадрового потенциала, развития ИТ-индустрии, экономики данных и т. д. По каждому из составляющих приведены примеры мировых инициатив на разных уровнях. Указаны ключевые доктринальные и нормативные правовые документы, призванные обеспечить цифровой суверенитет. Также в статье выделено понятие цифровой стабильности, которая представляет собой один из наиболее эффективных векторов достижения цифрового суверенитета. Указано, что приведенные в статье примеры зарубежного опыта могут быть адаптированы на национальном уровне в целях достижения цифровой стабильности.

А. Е. АЛЕКСЕЕВ,
директор ОАО «Гипросвязь»

Д. А. КАЧАН,
начальник Центра перспективных исследований в сфере цифрового развития

Н. Г. ЮНЕВИЧ,
аспирант БГТУ, научный сотрудник Центра перспективных исследований в сфере цифрового развития

ОАО «Гипросвязь»

Ключевые слова:
цифровой суверенитет, технологический суверенитет, стратегическая автономия, цифровая автономия, киберсуверенитет, цифровое развитие, экономика данных, ПО, свободно распространяемое ПО, цифровая стабильность.

Введение. Информационные технологии приобрели глобальный трансграничный характер и стали основой развития современного государства вне зависимости от территориальности, ресурсной базы, экономического, научно-технического и иных потенциалов. Развитие мировых держав диктуется такими реалиями, как: повсеместное внедрение информационных технологий, интернет-глобализация, рост ценности данных, возникновение новых рыночных моделей, новых типов продуктов и услуг, развитие цифровой экономики и т. д. Данные аспекты определили в последнее десятилетие появление в повестке многих стран вопросов обеспечения цифрового суверенитета. Учитывая, что непосредственное понятие «цифровой суверенитет» развивается в рамках европейских научных школ и политических подходов, в контексте определения данного понятия и его составляющих будет рассмотрен опыт Европейского союза (далее – ЕС), а также Китайской Народной Республики (далее – КНР) как обладателя диаметрально противоположной модели.

Понятие цифрового суверенитета. Понятие цифрового суверенитета возникло как факт расширения понятий «государственный суверенитет» и «национальный суверенитет» в ходе цифрового развития экономики.

В ЕС изначально образовалось понятие технологического суверенитета. Под ним понимали способность разрабатывать, предоставлять, защищать и сохранять важнейшие технологии,

необходимые для государственного управления, благосостояния граждан и процветания бизнеса. Также его воспринимали как способность действовать и принимать независимые решения в глобализированной среде [1]. Позже начало применяться понятие «цифровая стратегическая автономия». Первоначально оно использовалось в ЕС как стратегическая автономия в контексте безопасности и обороны, однако ввиду цифровых преобразований общества переросло в цифровую автономию. Цифровая стратегическая автономия представляла собой способность государства полагаться на свои ресурсы в ключевых стратегических областях, а также выбирать, когда, в какой области возможна кооперация с партнерами-единомышленниками [2]. После использования понятий технологического суверенитета (2019 г.), стратегической автономии (2018 г.) и цифровой автономии (2020 г.), в 2020 г. лейтмотивом европейской цифровой политики стало понятие цифрового суверенитета [3].

Национальная академия наук и инженерии Германии разделяет термин «цифровой суверенитет» на три области действия:

- освоение технологий и данных;
- обретение кадрами необходимых навыков и компетенций для использования и дальнейшего развития цифровых технологий и данных;
- разработка нормативно-правовой базы для направления технологического развития в эффективном направлении [4].

По данным других зарубежных авторов (G. Falkner, S. Heidebrecht и др.), цифровой суверенитет может рассматриваться как контроль на *физическом уровне* (инфраструктура, устройства), *уровне кода* (стандарты, правила, дизайн) и *уровне данных* (владение, потоки, использование). Контроль в данном случае предполагает возможность влиять на разработку и использование цифровых технологий и данных. Это в большей степени связано с политикой государства. Также специалисты в области информационной безопасности (Z. Zakhour, V. Gomes) указывают, что цифровой суверенитет стоит на двух столпах: суверенитете данных и технологическом суверенитете. Сам цифровой суверенитет представляет собой способ контроля над всей своей цифровой средой, включая данные, приложения, программное обеспечение, системы и оборудование [5].

В КНР ключевой составляющей цифрового суверенитета является киберсуверенитет. По определению председателя КНР Си Цзиньпина, киберсуверенитет – это уважение права каждой страны выбирать свой собственный путь развития сети интернет, свою собственную модель управления интернетом и свою собственную государственную политику в интернете. Также он обозначает равноправное участие в управлении международным киберпространством [6]. Китайское понимание киберсуверенитета крайне многогранное. На данный момент китайское руководство находится в процессе создания самого обширного режима управления киберпространством и ИКТ среди всех стран мира [7].

Вышеприведенные подходы в своей совокупности могут позволить определить цифровой суверенитет как способность государства или региона управлять своими цифровыми ресурсами и технологиями, сохраняя возможность адекватно реагировать на изменения технического, экономического, социального, политического и иного характера на национальном и международном уровнях.

Основные механизмы обеспечения цифрового суверенитета. Каждое современное государство

в той или иной степени движется в сторону обеспечения цифрового суверенитета. Данное движение находит выражение в инициативах различного характера и масштаба.

Развитие и наращивание технического потенциала. Одним из ключевых компонентов формирования цифровой инфраструктуры любой страны выступает компонентная база (микро-, радиоэлектроника и т. п.). На текущий момент более 90 % объема выпуска полупроводниковых элементов приходится на о. Тайвань [8]. Данный факт стал прецедентом технологической зависимости стран от полупроводниковых компонентов, необходимых для производства ключевых технических средств обеспечения цифрового развития. К тому же это создало тренд наращивания и расширения национального производственного потенциала, включая локализацию проектирования и производства изделий микро- и радиоэлектроники внутри страны.

Помимо наращивания производства микро- и радиоэлектроники, государства активизируют деятельность и в более широком спектре и номенклатуре ИКТ-продукции. Например, это нашло отражение в программном документе «Сделано в Китае 2025», инициативе «Один пояс, один путь», программе «Цифровой Шелковый путь» в КНР, программе «Сделай во Вьетнаме» и т. п.

Цифровое развитие промышленности. Наращивание производственного потенциала невозможно без пересмотра и актуализации основных деловых и производственных процессов, применения современных технологий (искусственный интеллект, аналитика больших данных, «интернет вещей», блокчейн, виртуальная и дополненная реальность, аддитивные технологии и т. д.). Мировые державы стали продвигать инициативы по цифровому развитию производств (программа Help to Grow: Digital и Made Smarter Innovation в Великобритании, программа «Путь к цифровому десятилетию» до 2030 г. в ЕС, план «Сделано в Китае 2025» и др.).

Переход от использования проприетарных программных продуктов к программному обеспечению (ПО) с открытым исходным кодом, включая свободно распространяемое и бесплатное ПО. Помимо зависимости в технических решениях, на текущий момент практически все страны мира столкнулись с зависимостью от иностранного системного и прикладного ПО. Ряд стран, в целях экономии государственных средств путем отказа от проприетарных решений, перешли на свободно распространяемое ПО еще в начале XXI века (Индия, Бразилия, Венесуэла, Эквадор, Уругвай, Боливия и т. д.) [9]. Более развитые страны начали данный переход позже, отчего попали в зависимость от иностранных программных продуктов.

Стимулирование научно-исследовательского сектора экономики для обеспечения цифрового развития и создания инновационных решений. Основой цифрового развития выступает возможность страны создавать инновационные решения. Учитывая важность современных цифровых технологий, ряд стран реализует масштабные государственные программы финансирования научных исследований и разработок в сфере цифрового развития (например, программа Horizon Europe 2027 с бюджетом в 95,5 млрд евро).

Развитие кадрового потенциала, навыков и компетенций для соответствия потребностям цифровой экономики. Высокие темпы цифрового развития не только меняют стандартные процессы труда, но и изменяют потребности ключевых отраслей экономики в кадрах и компетенциях. По последним прогнозам, к 2025 г. 85 млн рабочих мест могут исчезнуть, а их места займут 97 млн новых [10]. Учитывая эти изменения, развитие у людей как базовых, так и специальных цифровых навыков – один из главных аспектов успешного развития государства. Помимо этого, высокую актуальность приобретает стимулирование подготовки кадров по актуальным специальностям цифрового развития (например, искусственному

интеллекту, аналитике больших данных и др.). В кадровой политике наблюдается активизация привлечения иностранных специалистов для постоянного трудоустройства. Например, это реализуется посредством выдачи технических виз для привлечения иностранных талантов для сотрудников стартапов, учредителей и инвесторов в сфере цифрового развития (Германия, Великобритания, Франция, Южная Корея, КНР, Российская Федерация и др.).

Наращивание потенциала собственных разработчиков ПО и иных информационных технологий. Мировые цифровые гиганты не только монополизируют рынок, но и имеют значительные преимущества использования и коммерциализации массивов цифровых данных. В свою очередь это позволяет получить необоснованные конкурентные преимущества на национальных рынках. Ряд событий последних лет, связанных с необходимостью развития цифровой базы государственных и частных предприятий для удаленной работы в условиях Covid-19, наглядно продемонстрировал сложность конкурирования национальных разработчиков и их продуктов с цифровыми гигантами. Ввиду этого многие страны активизировали деятельность по стимулированию, поддержке национальных разработчиков ПО и созданию для них честной конкурентной среды на национальном рынке. Например, национальные стартапы привлекли во Францию более 11 млрд евро в 2021 г. Также инициатива «French Tech», созданная в 2014 г. и посвященная растущим французским стартапам, позволила к концу 2021 г. создать во Франции 26 технологических «единорогов» – компаний с рыночной стоимостью не менее 1 млрд евро [11].

Формирование политики государства по регулированию процессов хранения и трансграничной передачи данных. В 2017 г. 35 стран внедрили 67 законов, постановлений и правительственных политик, требующих хранения цифровой информации в национальном сегменте цифровой инфраструктуры. В 2021 г. уже 62 страны ввели 144 ограничения, и еще десятки в настоящее время находятся на рассмотрении [12].

Изменение бизнес-моделей ключевых игроков цифрового рынка под воздействием национальных требований к цифровым технологиям, услугам, платформам. В ряде стран сформированы не только требования к локализации и передаче данных организациями, но и требования, которые обязывают иностранных поставщиков онлайн-услуг нести ответственность за свои практики ведения онлайн-бизнеса (Закон о цифровых услугах (DSA) и Закон о цифровых рынках (DMA) в ЕС).

Развитие экономики данных. Приобретает актуальность принятие мер по коммерциализации данных. Наибольшую активность в данной сфере проявляют страны европейского региона. По оценкам Европейской Комиссии, объем экономики данных в ЕС составит 829 млрд евро в 2025 г. (от 301 млрд евро (2,4 % ВВП) в 2018 г.), главным образом путем создания единого рынка данных, разработки саморегулируемых стандартов для содействия свободному перемещению данных, а также разрешения на обмен, повторное использование и обработку данных [13]. Великобритания предпринимает шаги по развитию такого направления экономики данных, как Smart Data – безопасный обмен данными для предоставления инновационных услуг [14].

Формирование общего видения цифрового развития страны или региона. Цифровой суверенитет носит комплексный характер. Начиная от сырьевой, производственной, кадровой, научно-технической и иных баз для цифрового развития и заканчивая аспектами регулирования потоков данных и архитектуры веб-пространств. При этом возникает необходимость формирования комплексного видения дальнейшего развития стран и регионов. Это нашло отражение в многочисленных программных и стратегических документах, принятых мировыми державами. Например, комплексная стратегии КНР «Стратегия кибервласти», «Китайские стандарты до 2035 года», Закон США о безопасных и надежных сетях связи (включая мандат на избавление телекоммуникационных сетей от китайских технологий) и др.

Заключение. Несмотря на вышеприведенные инициативы, анализ мирового опыта указывает, что достижение полной степени автономности любого государства в этой сфере невозможно по ряду объективных причин. К ним относится сформировавшаяся система международного разделения труда, обеспечивающая высокую экономическую эффективность мировой системы производства товаров и услуг, в том числе в сфере информационных технологий. Полной локализации препятствуют также ограниченные материальные и кадровые ресурсы, производственные мощности и научно-технический потенциал, недостаточно благоприятный инвестиционный климат [15]. Следует отметить, что страны, достигшие высокой степени автономности государства в сфере цифрового развития (Иран, КНР), прошли этот путь эволюционно, на протяжении длительного времени, начинавшегося в период слабой зависимости жизнедеятельности государства от информационных технологий.

Таким образом, цифровой суверенитет главным образом должен быть выражен в способности государства сохранять цифровую стабильность. В свою очередь, цифровая стабильность представляет собой функционирование цифровой экономики и электронного правительства при воздействии различных внешних и внутренних факторов, направленных на замедление цифрового развития. Объективными способами сохранения цифровой стабильность могут стать инициативы мировых держав, приведенные в данной статье.

ЛИТЕРАТУРА

1. European Parliament: Key enabling technologies for Europe's technological sovereignty [Electronic resource]. – Mode of access: https://www.europarl.europa.eu/thinktank/en/document/EPRS_STU(2021)697184. – Date of access: 22.12.2022.
2. Decoding EU Digital Strategic Autonomy: Sectors, Issues, and Partners [Electronic resource]. – Mode of access: https://liberalforum.eu/wp-content/uploads/2022/06/Decoding-EU-Digital-Strategic-Autonomy_ELF-Study_Techno-Politics_vol.1-2.pdf. – Date of access: 22.12.2022.
3. Innerarity D. European Digital Sovereignty [Electronic resource]. – Mode of access: https://cadmus.eui.eu/bitstream/handle/1814/73437/Innerarity_2021.pdf?sequence=1&isAllowed=y. – Date of access: 22.12.2022.
4. Society Byte / Science Magazine of the Bern University of Applied Sciences [Electronic resource]. – Mode of access: https://www.societybyte.swiss/en/2022/05/04/data-sovereignty-more-than-just-hype/. – Date of access: 24.12.2022.
5. Digital Security Magazine [Electronic resource]. – Mode of access: https://atos.net/en/lp/digital-sovereignty-cybersecurity-magazine/what-is-sovereignty-and-why-it-does-matter. – Date of access: 21.12.2022.
6. China's Vision for Cyber Sovereignty and the Global Governance of Cyberspace [Electronic resource]. – Mode of access: https://www.nbr.org/publication/chinas-vision-for-cyber-sovereignty-and-the-global-governance-of-cyberspace/. – Date of access: 22.12.2022.
7. China's Emerging Cyber Governance System [Electronic resource]. – Mode of access: https://www.csis.org/programs/strategic-technologies-program/other-projects-cybersecurity/chinas-emerging-cyber. – Date of access: 22.12.2022.
8. Отчет Boston Consulting Group за 2021 [Electronic resource]. – Mode of access: https://www.bcg.com/publications/2021/strengthening-the-global-semiconductor-supply-chain. – Date of access: 23.12.2022.
9. Digital sovereignty or digital colonialism? [Electronic resource]. – Mode of access: https://sur.conectas.org/en/digital-sovereignty-or-digital-colonialism/. – Date of access: 15.12.2022.
10. The Future of Jobs Report 2020 [Electronic resource]. – Mode of access: https://cepa.org/comprehensive-reports/divided-digital-europe-the-continent-connects-at-different-speeds/. – Date of access: 15.12.2022.
11. Divided Digital Europe: The Continent Connects at Different Speeds [Electronic resource]. – Mode of access: https://cepa.org/comprehensive-reports/divided-digital-europe-the-continent-connects-at-different-speeds/. – Date of access: 16.12.2022.
12. France's new mantra: liberty, equality, digital sovereignty [Electronic resource]. – Mode of access: https://www.atlanticcouncil.org/blogs/new-atlanticist/frances-new-mantra-liberty-equality-digital-sovereignty/.– Date of access: 06.12.2022.
13. Building a European data strategy [Electronic resource]. – Mode of access: https://www.theparliamentmagazine.eu/news/article/building-a-european-data-strategy. – Date of access: 09.01.2023.
14. Smart data working group [Electronic resource]. – Mode of access: https://www.gov.uk/government/groups/smart-data-working-group. – Date of access: 02.01.2023.
15. Разработка научно обоснованных предложений для формирования Концепции национального суверенитета Республики Беларусь в сфере цифрового развития на пятилетний период: Отчет о НИР (промежуточный, этап 1) / ОАО «Гипросвязь»; рук. Д.А. Качан, исполн.: Н.Г. Юневич [и др.]. – Минск, 2022. – 361 с. – № ГР 20221711.

The article presents the results of the analysis of the concept of «digital sovereignty» in the context of foreign research and political practices. The main components of digital sovereignty are highlighted, including technological potential, digital transformation of industry, creation and use of national software and open-source software products, stimulation of the research sector and human resources potential, development of the IT industry, data economy and more. Examples of global initiatives at different levels are given for each component. Key doctrinal and normative legal documents aimed at ensuring digital sovereignty are indicated. The concept of «digital stability» is also highlighted in the article, which is one of the most effective vectors for achieving digital sovereignty. It is noted that the examples of foreign experience presented in the article can be adapted at the national level in order to achieve digital stability.

Key words: *digital sovereignty, technological sovereignty, strategic autonomy, digital autonomy, cyber sovereignty, digital development, data economy, software, open-source software, digital stability.*

Получено 27.01.2023.