Научно-исследовательский журнал «Modern Economy Success»
https://mes-journal.ru
2025, № 5 / 2025, Iss. 5 https://mes-journal.ru/archives/category/publications
Научная статья / Original article
Шифр научной специальности: 5.2.1. Экономическая теория (экономические науки)
УДК 004, 339.9, 338.2

[1] Козлова М.А.,
[1] Московский государственный институт международных отношений

Экономические аспекты цифрового суверенитета

Аннотация: *целью* исследования является анализ экономических аспектов цифрового суверенитета.

Методы включают в себя сравнительный анализ подходов, применяемых в разных странах, а также проведение SWOT-анализа экономических аспектов цифрового суверенитета.

Результаты: Экономические аспекты цифрового суверенитета включают в себя две основные области: затраты государства и компаний на цифровизацию и безопасность для защиты от киберпреступности и потери от кибератак. Отмечается важность развития импортозамещения в области цифровых технологий и развитие отечественного IT-сектора, поскольку это снижает зависимость страны от поставок компонентов и программного обеспечения зарубежными партнёрами и делает страну независимой. В качестве экономической выгоды от хранения данных внутри страны можно назвать снижение рисков санкционных блокировок, а также отмену оплаты зарубежным сервисам. Отмечены сложности на пути создания цифрового суверенитета. Одна из сложностей заключается в нехватке чипов и оборудования, которые раньше поставлялись иностранными компаниями. Из-за необходимости переписывать код под новые платформы на первоначальном этапе растут IT-разработки. При создании систем защиты от кибератак необходимо концентрироваться на ключевых направлениях, поскольку это требует значительных финансовых вложений.

Выводы: проведённый анализ позволяет выделить особенности обеспечения цифрового суверенитета в других странах, которые могут быть положены в основу разработки политики России в данной сфере. Выделенные опасности и возможности позволяют сделать акцент на развитии сильных сторон цифрового суверенитета.

Ключевые слова: цифровой суверенитет, кибербезопасность, информационный суверенитет, экономические аспекты суверенитета, цифровой суверенитет России

Для цитирования: Козлова М.А. Экономические аспекты цифрового суверенитета // Modern Economy Success. 2025. № 5. С. 125 – 131.

Поступила в редакцию: 4 июня 2025 г.; Одобрена после рецензирования: 3 августа 2025 г.; Принята к публикации: 23 сентября 2025 г.

[1] Kozlova M.A.,
[1] Moscow State Institute of International Relations

Economic aspects of digital sovereignty

Abstract: the *purpose* of the study is to analyze the economic aspects of digital sovereignty.

Methods include comparative analysis of approaches used in different countries, as well as SWOT analysis of the economic aspects of digital sovereignty.

Findings: The economic aspects of digital sovereignty include two main areas: state and company costs for digitalization and security to protect against cybercrime and losses from cyberattacks. The importance of the development of import substitution in the field of digital technologies and the development of the domestic IT sector is noted, since this reduces the country's dependence on the supply of components and software by foreign partners and makes the country independent. As an economic benefit from storing data within the country, we can name the

reduction of the risks of sanctions blocking, as well as the cancellation of payments to foreign services. At the same time, there are certain difficulties in creating digital sovereignty. One of the difficulties lies in the lack of chips and equipment that were previously supplied by foreign companies. Due to the need to rewrite the code for new platforms, IT developments are currently at the initial stage. When creating systems of protection against cyber attacks, it is necessary to focus on key areas, since this requires significant financial investments.

Conclusions: the analysis allows us to highlight the features of ensuring digital sovereignty in other countries, which can be the basis for the development of Russia's policy in this area. Highlighted dangers and opportunities allow us to focus on the development of the strengths of digital sovereignty.

Key words: digital sovereignty, cybersecurity, information sovereignty, economic aspects of sovereignty, digital sovereignty of Russia

For citation: Kozlova M.A. Economic aspects of digital sovereignty. Modern Economy Success. 2025. 5. P. 125 – 131.

The article was submitted: June 4, 2025; Approved after reviewing: August 3, 2025; Accepted for publication: September 23, 2025.

Введение

В настоящее время государственный суверенитет оказывается связанным и с обеспечением безопасности в условиях развития новых цифровых технологий. В условиях санкций и ухудшения отношения между странами из-за противоречий на мировой арене страна должна уметь противостоять внешнему влиянию с использованием цифровых технологий.

Разные авторы дают разное определение цифрового суверенитета. В.И. Авдийский, А.В. Иванов и А.В. Царегородцев дают следующее определение: «Цифровой суверенитет нами рассматривается как возможность государства контролировать свои цифровые данные, информацию, а также обеспечивать безопасность и защиту цифровых технологий и инфраструктуры» [1, с. 4]. Это понятие тесно связано с такими понятиями, как информационный суверенитет и кибербезопасность. Под информационным суверенитетом понимается право государства самостоятельно формировать информационную политику, распоряжаться информационными потоками и обеспечивать информационную безопасность, не завися от внешних влияний [2]. Кибербезопасность – это «комплекс правовых, организационных, технических и образовательных средств, направленных на обеспечение конфиденциальности, целостности и доступности информации» [3]. Также её понимают как «практику защиты сетей, устройств, приложений, систем и данных от киберугроз» [4].

Е.Г. Зорина выделяет два основных критерия технологического суверенитета – технический и идеологический [5]. Под техническим суверенитетом понимается существование национального программного обеспечения, собственных социальных сетей, поисковых механизмов и национальной электронной платёжной системы. В. Бухарин добавил к этому списку ещё наличие микроэлектроники, сетевого оборудования, национального сегмента в сети Интернет, криптографических алгоритмов и протоколов, навигационной системы и средств защиты [6]. К идеологической составляющей относятся национальная идея или идеология, пропаганда и проработанное в информационной среде законодательство.

Е.И. Соболев [7] в обзоре развития информационного суверенитета ссылается на статью А.А. Ефремова, отмечающего четыре этапа развития информационного суверенитета [8]. Первый пришёлся на 1980-е гг., когда обмен информацией происходил благодаря использованию спутников, телевидения и радио, а правовая основа ограничений потока информации на межгосударственном уровне только складывалась. Второй этап связан с распространением Интернета в 1990-е гг. Третий этап связан с необходимостью защиты данных на серверах страны. На четвёртом этапе основной задачей становится контроль над информационно-коммуникационной инфраструктурой.

В данной статье делается акцент на изучение экономических аспектов цифрового суверенитета. Среди основных аспектов экономического суверенитета можно выделить: 1) затраты государства и компаний на цифровизацию и безопасность для защиты от киберпреступлений; 2) потери от кибератак. Потери от кибератак представлены в табл. 1.

Таблица 1

Потери от кибератак.

Table 1

Losses from cyber attacks.

Финансовые потери	• потери от прекращения экономической деятельности; • потери от нарушения работы инфраструктуры; • потери от перебоев в работе оборудования
Нефинансовые потери	• репутационные потери; • снижение заинтересованности в партнёрстве со стороны иностранных партнёров; • панические настроения среди населения

Источник: Составлено автором, в том числе с использованием [3].
Source: Compiled by the author, including using [3].

Для снижения потерь от кибератак государство проводит меры по снижению потерь. Чтобы определить оптимальный уровень затрат, на рис. 1 представлен график, на котором показаны расходы на кибербезопасность.

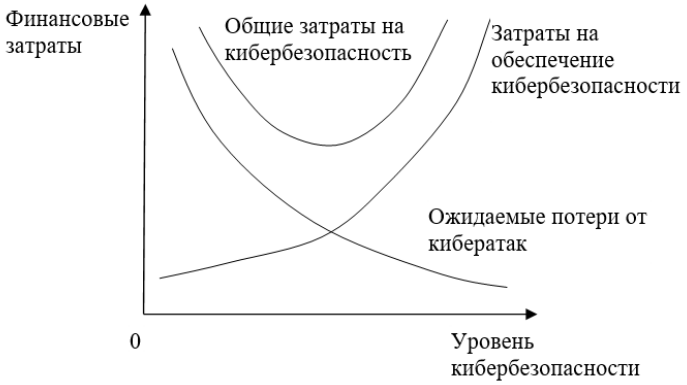

Рис. 1. Расходы на кибербезопасность. Источник [3].
Fig. 1. Cybersecurity expenditures. Source [3].

Для определения оптимального уровня нужно найти минимальное значение общих затрат, складывающихся из затрат на обеспечение кибербезопасности и ожидаемых потерь от кибератак.

Материалы и методы исследований

Был проведён анализ российских и иностранных источников, в которых рассматриваются экономические аспекты цифрового суверенитета. Был проведён сравнительный анализ подходов, применяемых в разных странах. Рассмотрены кейсы, отражающие экономические потери в случае кибератак, а также успешные случаи импортозамещения в данной сфере.

Также был проведён SWOT-анализ экономических аспектов цифрового суверенитета – выделены сильные и слабые стороны, потенциальные опасности и возможности для дальнейшего развития.

Результаты и обсуждения

Для обеспечения цифрового суверенитета страны большое значение имеет государственное и международное законодательство. В 2019 г. в России был принят федеральный закон от 01.05.2019 г. № 19 «О внесении изменений в Федеральный закон «О связи» и Федеральный закон «Об информации, информационных технологиях и о защите информации», который предусматривает создание централизованной системы управления Интернетом со стороны государственной власти. В данной сфере Россия следует опыту зарубежных стран, которые незадолго до этого приняли аналогичные меры. Например, в ЕС только с 2016 г. происходит объединение и унификация законодательства в сфере кибебрезопасности и защиты информационных систем и сетей.

В период пандемии коронавируса на международном уровне в рамках ООН в 2020 г. была принята Дорожная карта по цифровому сотрудничеству, в соответствии с которой страны координировали свои усилия по внедрению цифровых технологий. 12 апреля 2021 г. в РФ принят Указ Президента РФ № 213 «Основы государственной политики в области международной информационной безопасности». 25 ноября 2022 г. Минцифры объявило о достижении Россией цифрового суверенитета, однако это было связано в значительной

степени с уходом с российского рынка почти всех иностранных компаний [9].

Разные страны применяют разные подходы к осуществлению государственной политики в области цифрового суверенитета. Основы этих подходов изложены в таких документах как Национальная стратегия безопасности КНР в киберпространстве, Национальная киберстратегия США, Киберстратегия Министерства обороны США, Директива NIS2 и Закон о киберустойчивости в ЕС. В табл. 2 составлен сравнительный анализ подходов разных стран к организации цифровой безопасности.

Таблица 2

Сравнительный анализ разных стран к обеспечению цифровой безопасности.

Table 2

Comparative analysis of different countries in ensuring digital security.

Страны	Особенности подхода
ЕС	- улучшение координации между государствами-членами и усиление сотрудничества в вопросах трансграничного реагирования на инциденты; - затрагивает организации, которые находятся за пределами ЕС, но предоставляют услуги или сотрудничают с компаниями в Европейском Союзе; - строгие правила в отношении управления рисками кибербезопасности, включая меры по обеспечению безопасности цепочек поставок, контроль доступа и отчетность об инцидентах; - цензура информации и социальных сетей
Китай	- использование «Золотого щита» («Великого китайского файрволла») для фильтрации контента в Интернете и блокировки опасных сайтов; - западные СМИ недоступны для китайских пользователей; - использование системы социальных кредитов, поощряющих или наказывающих граждан в зависимости от их активности в социальных сетях
США	- свободный доступ к сети Интернет; - поддержка развития передовых технологий в области кибербезопасности, повышение квалификации специалистов и укрепление международного сотрудничества в этой сфере; - укрепление партнерских отношений с союзниками для совместного противостояния киберугрозам
Россия	- импортозамещение в области цифровых технологий; - развитие российского сегмента в сети Интернет (Rutube), замена иностранного программного обеспечения, создание собственной инфраструктуры; - развитие научных исследований в области цифровых технологий; - цензура информации и социальных сетей, распространение государственной позиции

Если говорить об экономических аспектах цифрового суверенитета, то важно отметить две основные области: затраты государства и компаний на цифровизацию и информационную безопасность и затраты на защиту от киберпреступности и потери от кибератак.

Рассмотрим вначале затраты России на цифровизацию и информационную безопасность. На государственном уровне создаются подразделения, направленные на выявление киератак и их устранение [10]. В 2024 г. затраты РФ на осуществление национальной программы «Цифровая экономика» составили 146 132,5 млн рублей (99,7 % от запланированного объема) [11]. Данные НИУ ВШЭ говорят о том, что общий объём валовых внутренних затрат на цифровую экономику в 2023 г. составил 5,5 трлн рублей, повысившись на 6 % относительно предыдущего года в текущих ценах [12]. По данным исследования Б1 за 2024 г., Россия оказалась на девятом месте по инвестициям бизнеса в информационную безопасность. На первом месте по этому показателю оказались США (44 %), на втором Китай (8 %), далее Великобритания (6 %), Япония (5 %), Германия (4 %), Франция (3 %), Австралия и Канада (по 2 %) [13]. В соответствии с этим исследованием, объём российского рынка инвестиционной безопасности составляет 299 млрд долларов, а рост по сравнению с 2023 г. составил 23 %. Ожидается, что и в дальнейшем с 2024 по 2030 гг. продолжится рост этого сегмента со среднегодовыми показателями в 15 % [14].

Ущерб от киберпреступлений в России составил около 200 млрд рублей в 2024 г. По данным Центробанка России, в 2024 г. было отражено 16,3 млн попыток злоумышленников похитить деньги клиентов на 2,3 трлн рублей. Только за период апреля-июня 2024 г. были зафиксированы 257 тысяч мошеннических операций.

Проведём SWOT-анализ экономических аспектов цифрового суверенитета (табл. 3).

Таблица 3

SWOT-анализ экономических аспектов цифрового суверенитета.

Table 3

SWOT analysis of the economic aspects of digital sovereignty.

Сильные стороны (Strengths)	Слабые стороны (Weaknesses)
• в 2022 г. Минцифры РФ объявил о достижении Россией цифрового суверенитета; • успешные случаи импортозамещения (развитие российских процессоров (Байкал, Эльбрус) и серверов (Ядро, Kraftway); • развитие российских процессоров (Байкал, Эльбрус) и серверов (Ядро, Kraftway); • развитие российского сегмента Интернета (Rutube и другие платформы), принятие закона о «суверенном Интернете»	• в сегментах электронного оборудования и программного обеспечения практически все потребности внутреннего российского рынка восполняются за счёт импорта; • нехватка чипов и оборудования, которые раньше поставлялись иностранными компаниями; • из-за необходимости переписывать код под новые платформы на первоначальном этапе растут IT-разработки; • необходимы значительные финансовые вложения
Возможности (Opportunities)	**Угрозы (Threats)**
• государственная поддержка импортозамещения; • осуществление национального проекта «Цифровая экономика»; • уход иностранных компаний даёт возможность российским компаниям нарастить своё производство в данной сфере	• в условиях санкций возможны блокировки приобретённого импортного оборудования и деформация программного оеспечения; • участившиеся кибератаки на государственные структуры, корпорации и частный бизнес, • противозаконный съём информации из телекоммуникационных систем

Выводы

В настоящее время большое значение имеет создание мер по укреплению цифрового суверенитета России. Можно использовать и опыт других стран, которые также в последние годы направляют значительные усилия на развитие собственного цифрового суверенитета. Например, в ЕС проводятся меры по улучшению координации между участвующими странами. Россия также могла бы развивать координацию мер с дружественными странами. Особенности китайской системы предполагают создание файрволла для фильтрации контента и использование системы социальных кредитов. Отчасти это можно использовать и в России, хотя отношение общества к социальным кредитам может быть и неоднозначным. В США делается акцент на развитие передовых технологий в области кибербезопасности, и государство в России также может давать льготы и субсидии предприятиям, внедряющим передовые технологии.

Важно отметить развитие импортозамещения в области цифровых технологий и развитие отечественного IT-сектора, поскольку это снижает зависимость страны от поставок компонентов и программного обеспечения зарубежными партнёрами и делает страну независимой. В качестве примера можно привести развитие российских процессоров (Байкал, Эльбрус) и серверов (Ядро, Kraftway). Происходит замена иностранного программного обеспечения и увеличение спроса на российские облачные платформы. В качестве экономической выгоды от хранения данных внутри страны можно назвать снижение рисков санкционных блокировок (например, связанных с ограничением SWIFT или отключением облачных сервисов AWS, Google Cloud), а также отмену оплаты зарубежным сервисам.

Вместе с тем, есть и определённые сложности на пути создания цифрового суверенитета. Одна из сложностей заключается в нехватке чипов и оборудования, которые раньше поставлялись иностранными компаниями. Из-за необходимости переписывать код под новые платформы на первоначальном этапе растут IT-разработки. В последнее время участились кибератаки на государственные структуры и корпорации, потому необходимо уже в настоящее время принимать меры.

При создании систем защиты от кибератак необходимо концентрироваться на ключевых направлениях, поскольку это требует значительных финансовых вложений. В перспективе цифровой суверенитет России позволит снизить влияние санкций, развить новые технологические направления, достичь экономии бюджетных средств за счёт цифровизации.

Список источников

1. Авдийский В.И., Иванов А.В., Царегородцев А.В. Взаимосвязь цифрового суверенитета и цифрового пространства: новые вызовы и перспективы // Вестник Евразийской науки. 2024. Т. 16. № s3 URL: https://esj.today/PDF/21FAVN324.pdf (дата обращения: 30.04.2025)

2. Авдийский В.И., Иванов А.В. Особенности влияния деструктивных событий цифрового пространства на экономическую безопасность в условиях цифрового суверенитета государства // Развитие и безопасность. 2024. № 3. С. 4 – 25.

3. Müllner V., Nečas K., Olejníček A., Šmídová V. Economic aspects of cybersecurity in the public sector // ACTA STING. 2023. Vol. 12. № 3. С. 39 – 70.

4. SAP. Cybersecurity overview. 2023. URL: https://www.sap.com/products/financial-management/what-is-cybersecurity.html (дата обращения: 30.04.2025)

5. Зорина Е.Г. Информационный суверенитет современного государства и основные инструменты его обеспечения // Известия Саратовского университета. Новая серия. Серия: Социология. Политология. 2017. Т. 17. № 3. С. 345 – 348

6. Бухарин В.В. Компоненты цифрового суверенитета Российской Федерации как техническая основа информационной безопасности // Вестник МГИМО-Университета. 2016. № 6. С. 76 – 91.

7. Грибин Н.П., Кохтюлина И.Н., Соболев И.И., Седунов Д.И. Информационный суверенитет: материалы научной дискуссии // Россия и мир: научный диалог. 2022. № 2(4). Сс. 100-131

8. Ефремов А.А. Государственный суверенитет в условиях цифровой трансформации // Правоведение. 2019. Т. 63. № 1. С. 47 – 61.

9. Бегларян М.Е., Астафьева М.В., Астапчик И.В. Социально-экономические отношения и цифровой патриотизм // Вестник института дружбы народов Кавказа. 2023. №1 (65). С. 39 – 47.

10. Антропов К.Ю., Ахмадеев Р.Г., Косов М.Е. Киберезопасность и сохранение цифрового суверенитета экономики // Вестник экономической безопасности. 2021. № 5. С. 268 – 273.

11. Стали известны расходы бюджета на «Цифровую экономику» по итогам 2024 г. URL: https://d-russia.ru/stali-izvestny-rashody-bjudzheta-na-cifrovuju-jekonomiku-po-itogam-2024-goda.html (дата обращения: 30.04.2025)

12. Затраты на развитие цифровой экономики в 2023 г. URL: https://issek.hse.ru/news/984068213.html (дата обращения: 30.04.2025)

13. Россия вошла в топ-10 стран мира по расходам на безопасность URL: https://b1.ru/insights/news/b1-materials-in-media/b1-forbes-russian-information-security-market-survey-19-march-2025/ (дата обращения: 30.04.2025)

14. Мошенники установили рекорд по похищению у россиян денег с банковских счетов URL: https://www.cnews.ru/news/top/2024-08-22_moshenniki_pohitili_pochti (дата обращения: 30.04.2025)

References

1. Avdiyskiy V.I., Ivanov A.V., Tsaregorodtsev A.V. The relationship between digital sovereignty and digital space: new challenges and prospects. Bulletin of Eurasian Science. 2024. Vol. 16. No. s3 URL: https://esj.today/PDF/21FAVN324.pdf (date of access: 30.04.2025)

2. Avdiyskiy V.I., Ivanov A.V. Features of the influence of destructive events in the digital space on economic security in the context of the digital sovereignty of the state. Development and Security. 2024. No. 3. P. 4 – 25.

3. Müllner V., Nečas K., Olejníček A., Šmídová V. Economic aspects of cybersecurity in the public sector. ACTA STING. 2023. Vol. 12. No. 3. P. 39 – 70.

4. SAP. Cybersecurity overview. 2023. URL: https://www.sap.com/products/financial-management/what-is-cybersecurity.html (date of access: 30.04.2025)

5. Zorina E.G. Information sovereignty of the modern state and the main instruments for ensuring it. Bulletin of the Saratov University. New series. Series: Sociology. Political Science. 2017. Vol. 17. No. 3. P. 345 – 348

6. Bukharin V.V. Components of the digital sovereignty of the Russian Federation as a technical basis for information security. Bulletin of MGIMO-University. 2016. No. 6. P. 76 – 91.

7. Gribin N.P., Kokhtyulina I.N., Sobolev I.I., Sedunov D.I. Information sovereignty: materials of scientific discussion. Russia and the World: scientific dialogue. 2022. No. 2(4). P. 100 – 131

8. Efremov A.A. State sovereignty in the context of digital transformation. Jurisprudence. 2019. Vol. 63. No. 1. P. 47 – 61.

9. Beglaryan M.E., Astafieva M.V., Astapchik I.V. Socio-economic relations and digital patriotism. Bulletin of the Institute of Friendship of the Peoples of the Caucasus. 2023. No. 1 (65). P. 39 – 47.

10. Antropov K.Yu., Akhmadeev R.G., Kosov M.E. Cybersecurity and Preservation of Digital Sovereignty of the Economy. Bulletin of Economic Security. 2021. No. 5. P. 268 – 273.

11. Budget expenditures on the “Digital Economy” for 2024 have become known. URL: https://d-russia.ru/stali-izvestny-rashody-bjudzheta-na-cifrovuju-jekonomiku-po-itogam-2024-goda.html (accessed on 30.04.2025)

12. Expenditures on the development of the digital economy in 2023. URL: https://issek.hse.ru/news/984068213.html (accessed on 30.04.2025)

13. Russia entered the top 10 countries in the world in terms of security spending. URL: https://b1.ru/insights/news/b1-materials-in-media/b1-forbes-russian-information-security-market-survey-19-march-2025/ (date of access: 30.04.2025)

14. Fraudsters set a record for stealing money from Russians' bank accounts URL: https://www.cnews.ru/news/top/2024-08-22_moshenniki_pohitili_pochti (date of access: 30.04.2025)

Информация об авторе

Козлова М.А., кандидат экономических наук, доцент, Московский государственный институт международных отношений, г. Москва, пр. Вернадского, д. 76, michandy@mail.ru