

Роль технологического суверенитета в обеспечении устойчивого развития Российской Федерации

The Role of Technological Sovereignty in Ensuring the Sustainable Development of the Russian Federation

DOI: 10.12737/2306-627X-2026-15-3-30-37

Получено: 11 ноября 2025 г. / Одобрено: 19 ноября 2025 г. / Опубликовано: 30 сентября 2025 г.

Чернышев А.К.

Стажер-исследователь, Институт экономической политики и проблем экономической безопасности факультета экономики и бизнеса, ФГБОУ ВО «Финансовый университет при Правительстве Российской Федерации», г. Москва
e-mail: chernysheva.tk@rea.ru

Chernyshev A.K.

Intern Researcher, Institute of Economic Policy and Economic Security Problems of the Faculty of Economics and Business, Financial University under the Government of the Russian Federation, Moscow
e-mail: chernysheva.tk@rea.ru

Поршнева И.И.

Стажер-исследователь, Институт экономической политики и проблем экономической безопасности факультета экономики и бизнеса, ФГБОУ ВО «Финансовый университет при Правительстве Российской Федерации», г. Москва

Porshneva I.I.

Intern Researcher, Institute of Economic Policy and Economic Security Problems of the Faculty of Economics and Business Financial University under the Government of the Russian Federation, Moscow

Аннотация

В статье исследуется роль технологического суверенитета и научно-технологической безопасности как ключевых условий устойчивого развития Российской Федерации. Уточняется содержание понятия «угроза технологическому развитию» и предлагается ее классификация по источникам на внешние (санкционные ограничения, разрывы цепочек поставок, киберриски, снижение международной кооперации) и внутренние (недостаток финансирования НИОКР, инфраструктурные ограничения, дефицит компетенций и кадров). На примере импорта и производства серверов и хранилищ за 2020–2024 гг. показано применение статистического инструментария: расчет относительного стандартного отклонения и сопоставление динамики с базисным годом, что позволяет интерпретировать степень риска как низкую, среднюю или высокую. Дополнительно предложен экспертно-опросный подход с начислением «баллов риска» с учетом наличия отечественных аналогов, структуры импорта и платежных ограничений. Также обобщены результаты контент-анализа материалов зарубежных аналитических агентств и институтов развития, где среди наиболее значимых угроз выделяются ограничение доступа к передовым технологиям, отставание в критических направлениях, отток специалистов и цифровая изоляция.

Ключевые слова: технологический суверенитет, научно-технологическая безопасность, устойчивое развитие, угрозы технологическому развитию, санкции, киберугрозы оценка риска, импортозамещение.

Abstract

The article examines the role of technological sovereignty and scientific-technological security as key prerequisites for the sustainable development of the Russian Federation. The authors specify the concept of a “threat to technological development” and classify such threats by their sources into external (sanctions-driven restrictions, supply-chain disruptions, cyber risks, and declining international cooperation) and internal (insufficient R&D funding, infrastructure constraints, and shortages of skills and talent). A step-by-step framework for threat analysis is proposed, including data collection, contextual analysis, quantitative assessment, integration of findings, and continuous monitoring. Using the case of imports and domestic production of servers and storage systems in 2020–2024, the paper illustrates a statistical approach to risk measurement based on the relative standard deviation and comparison with a selected base year, enabling interpretation of risk levels as low, medium, or high. In addition, an expert-survey scoring method (“risk points”) is suggested, accounting for the availability of domestic substitutes, import structure, and payment restrictions. The study also summarizes a content analysis of reports by foreign analytical agencies and development institutions, highlighting restricted access to advanced technologies, lagging performance in critical areas, talent outflow, and digital isolation as major risks.

Keywords: technological sovereignty, scientific and technological security, sustainable development, threats to technological development, sanctions, cyber threats, risk assessment, import substitution.

ВВЕДЕНИЕ

Научно-технологическая безопасность играет ключевую роль в обеспечении устойчивого развития нашей страны и её способности к инновациям. Угрозы, возникающие в этой сфере, могут существенно повлиять на конкурентоспособность национальной экономики и её способность адаптироваться к быстро меняющимся условиям глобального рынка. Угрозы технологическому развитию представляют собой факторы, способные препятствовать или замедлять прогресс в области технологий. Эти угрозы могут быть как внешними, так и внутренними, охватывая экономические, социальные, политические и экологические аспекты. В новой Стратегии национальной безопасности Российской Федерации опре-

деляются современные угрозы, включая ужесточение внешних факторов. Понимание природы и источников таких угроз является ключевым для разработки стратегий их минимизации и предотвращения, что особенно актуально в условиях глобальной технологической конкуренции.

В нормативных правовых актах Российской Федерации термин «угроза технологическому развитию» не определён. Однако в официальных документах используются схожие понятия, связанные с угрозами технологической безопасности и факторами, препятствующими технологическому развитию. Согласно энциклопедии МЧС Российской Федерации, «угрозы технологической безопасности» представляют собой реальную возможность наступ-

ления опасного состояния в технологическом развитии страны, региона, отрасли или предприятия, которое грозит причинением ущерба технологической базе, технологическому укладу и технологической независимости [18].

Согласно распоряжению Правительства Российской Федерации от 20 мая 2023 г. № 1315-р «Об утверждении Концепции технологического развития на период до 2030 года», «вызовы технологического развития» представляют собой объективно требующую реакции со стороны государства и общества совокупность проблем, угроз и возможностей в сфере разработки и внедрения технологий, сложность и масштаб которых таковы, что их решение, устранение или реализация невозможны без структурных изменений и не могут быть достигнуты исключительно за счет увеличения ресурсов [2]. Согласно Концепции технологического развития на период до 2030 г., ключевыми угрозами для технологического развития России являются следующие факторы.

1. Ограниченная способность национальной экономики адаптироваться к глобальным системным тенденциям, включая:
 - ускоренное развитие и распространение новых технологий, в том числе цифровых, кардинально изменяющих рыночные и производственные системы;
 - воздействие климатических изменений на глобальную экономику, включая реализацию политики энергоперехода в развитых странах;
 - дисбаланс спроса и предложения на отдельных глобальных товарных рынках, включая продовольственный сектор;
 - установление в передовых экономиках новых стандартов качества жизни (в сферах здравоохранения, образования, жилищного обеспечения и безопасности), недоступных для государств, находящихся в процессе догоняющего развития.
2. Замедление темпов инновационно-ориентированного экономического роста по сравнению с ведущими мировыми державами, что снижает конкурентоспособность российской экономики.
3. Отток высококвалифицированных специалистов и талантливых кадров за рубеж, что ограничивает возможности научно-технологического развития страны и ослабляет её позиции в глобальной экономике.
4. Нарушение функционирования производственных систем, вызванное санкционными ограничениями в сфере технологий, что ведёт к разрыву производственных цепочек и усложнению доступа к критически важным технологиям.

Исходя из представленных определений и перечня ключевых угроз для технологического развития России, «угроза технологическому развитию» — это совокупность факторов и условий, способных привести к дестабилизации научно-технического прогресса, снижению конкурентоспособности экономики и технологической независимости страны. Таким образом, цель настоящей работы заключается в исследовании роли научно-технологической безопасности в обеспечении устойчивого развития Российской Федерации.

МАТЕРИАЛЫ И МЕТОДЫ ИССЛЕДОВАНИЯ

Эмпирическую базу исследования составили материалы и статистические данные, опубликованные в аналитических отчетах, и размещенные на официальных сайтах органов законодательной и исполнительной власти. При написании работы был применен широкий набор методов, в частности: системный анализ для увязки технологического суверенитета с устойчивым развитием и научно-технологической безопасностью; формально-юридический и сравнительный методы для интерпретации терминов и сопоставления подходов в документах и практиках; ретроспективный анализ для оценки динамики показателей; контент-анализ зарубежных отчетов.

РЕЗУЛЬТАТЫ

В первую очередь рассмотрим вопрос на рубеже теории и современной практики, что позволит дать основу для алгоритма расчета рисков реализации угроз. В рамках исследования угроз технологическому развитию страны, стоит рассмотреть данный вопрос в двух аспектах. Классификация угроз по источникам позволяет выделить внутренние и внешние угрозы. Внутренние угрозы включают недостаток финансирования, слабую инфраструктуру и низкий уровень компетенций.

Внешние угрозы связаны с глобальными вызовами, такими как киберугрозы, которые, по данным Всемирного экономического форума, в 2024 г. были названы одной из крупнейших угроз технологическому развитию. Возрастающая сложность киберфизических систем в критической инфраструктуре требует внедрения инновационных и адаптивных подходов для обеспечения их безопасности и устойчивости. Рассмотрим основные этапы анализа угроз технологическому развитию более подробно. В табл. 1 отражена детализация процессов в рамках каждого из представленного выше этапа.

Как было отмечено ранее, с одной стороны, угрозы могут приходить извне, т.е. быть внешними. В таком случае риск угрозы будет напрямую связан с между-

Таблица 1

Описание этапов проведения анализа

Наименование этапа	Описание этапа
Сбор данных	Первым этапом является сбор данных. Источниками данных служат различные отчеты разведки, аналитические центры (например, RAND), данные из Интернета, исследования крупных корпораций и т.д. Информацию анализируют в следующих форматах: тексты, таблицы, графики
Контекстный анализ	В рамках контекстного анализа проходят несколько шагов: 1) предварительная обработка текстов; 2) выделение ключевых тем и угроз; 3) классификация угроз; 4) составление отчета по контекстному анализу; 5) обобщение основных выводов и выделение ключевых угроз
Количественный анализ	В рамках количественного анализа проходят несколько шагов: 1) извлечение количественных данных; 2) анализ данных; 3) оценка влияния; 4) составление отчета по количественному анализу
Интеграция результатов	На основании интегрированных данных разрабатываются рекомендации по действиям, направленные на минимизацию потенциальных угроз. Эти рекомендации должны быть конкретными, реалистичными и адаптированными к текущим условиям
Мониторинг и обновление	Важно проводить повторный анализ по мере появления новых отчетов и информации, что позволит своевременно реагировать на изменения в ситуации и корректировать стратегию. Такой подход обеспечивает постоянное совершенствование процессов и адаптацию к новым вызовам, что в конечном итоге способствует более эффективному управлению рисками

Источник: составлено авторами.

народными связями, глобальными изменениями в мире. Пример реализации подобной внешней угрозы технологическому развитию страны — осложненная логистическая ситуация в 2020–2021 гг. из-за ковидных ограничений. Более актуальным примером является санкционное давление со стороны недружественных стран, что представляет собой комплексный барьер для технологического развития, и, соответственно, порождает угрозы, риск реализации которых увеличивается с ужесточением ограничений.

Также внешние угрозы влекут за собой снижение роли международного сотрудничества в разработке отечественных технологий, что может значительно замедлить процесс. Исходя из вышесказанного отметим, что внешние угрозы сопряжены с такими показателями, как импорт технологий, экспорт технологий, международная кооперация в научно-технической сфере, доступ к зарубежным рынкам, инвестиции из-за рубежа [4].

Снижение импорта оборудования уже является негативным знаком, но важно оценивать и спрос, так как закупки могут снижаться из-за падения спроса у населения или бизнеса [20]. В рамках технологий спрос падает лишь на устаревшие технологии, инновации всегда остаются востребованными. Стоит отметить, что в 2024 г. импорт техники в России упал на 3%. С учетом ежегодного повышения спроса на технику и электронику в связи с повсеместной цифровизацией, снижение импорта даже на относительно небольшой процент является тревожным сигналом с учетом того, что даже в 2022–2023 гг. был зафиксирован рост импорта [12].

На данный момент аналитики отмечают, что данная тенденция может продолжиться, прогнозируя падение до 30% от импорта 2023 г. [12]. В качестве влияющих факторов выделяют ключевую ставку, а также проблемы с проведением платежей в Китай [6]. Соответственно, учитывая все перечисленные обстоятельства, можно сделать вывод, что наблюдается высокий риск угрозы технологическому развитию страны, так как будет наблюдаться недостаток технологий. Высокий спрос приведет к повышению цен на ограниченное число уже ввезенных технологий, что также негативно отразится на общей экономической ситуации.

С другой стороны, помимо внешних угроз, есть и внутренние, органические угрозы, которые порождаются функционирующим обществом, а также действиями самого государства. Внутренние угрозы имеют иную специфику, корреляция происходит с такими показателями, как уровень финансирования инноваций (как бизнесом, так и государством), уровень образования для соответствующих квалифицированных кадров, доступ к кредитным ресурсам [4]. При этом оценка внутренних угроз сопряжена с более глубинным анализом, так как сопряженные показатели могут отразить ситуацию только в сравнении с другими показателями.

В качестве примера внутренней угрозы проанализируем риск недостаточного финансирования инноваций и НИОКР в сфере высокотехнологичных проектов. Правительство Российской Федерации, благодаря указаниям Президента Российской Федерации, в настоящее время особое внимание уделяет вопросам технологического развития страны. В частности, отмечается, что к 2030 г. доля отечественных высокотехнологичных товаров и услуг на внутреннем рынке должна увеличиться в 1,5 раза. Около 120 млрд руб. направят на субсидии для НИОКР до 2030 г. [21]. Соответственно, риск недостатка финансирования инноваций снижается, так как функционируют механизмы получения средств на развитие

высокотехнологичных проектов, в том числе через Фонд развития промышленности (далее — ФРП). Важно, чтобы деньги использовались целевым образом, существовал контроль расходования средств. В таком случае риск угрозы технологическому развитию в рассмотренном случае будет минимален.

Риск реализации угроз по ограничениям поставок технологий включает в себя снижение импорта высокотехнологичного оборудования, импорт комплектующих для обслуживания, импорт программного обеспечения. В некоторых случаях, как, например, с программным обеспечением, в России существуют компании, занимающиеся разработкой аналогов. При этом многие позиции в списке высокотехнологичного оборудования не имеет отечественного аналога, что является дополнительным фактором риска. Перечень подобного оборудования перечислен в Постановлении Правительства Российской Федерации от 30 апреля 2009 г. № 372 [1]. Стоит упомянуть в качестве дополнительной особенности, что данные товары не облагаются НДС. И так в случае, если компонент включен в список, не имеющих аналогов, то риск реализации угрозы технологическому развитию страны возрастает, так как российские экспортеры находятся в зависимости от поставок, общей экономической ситуации.

На рис. 1 отображены данные по импорту и производству серверов и хранилищ, которые в настоящий момент являются важным элементом ИТ-инфраструктуры. На основе представленных данных будет проведен показательный статистический анализ, связанный с внешним риском уменьшения импорта серверов, как часть алгоритма для определения риска угроз технологическому развитию. При этом, стоит отметить, что аналог импортных серверов разрабатывается и продается в России, из-за чего риск будет ниже. В рамках статистического анализа данный фактор не влияет на конечный результат, но его необходимо учитывать при последующей обработке данных.



Рис. 1. Импорт и производство серверов и хранилищ с 2020 по 2024 гг., тыс. шт.

Составлено авторами по материалам [7; 9].

В 2020 г. импорт серверов был осложнен пандемией, к 2021 г. импорт вырос до 126 тыс. шт., почти в два раза по сравнению с 2020 г. Начиная с 2022 г., наблюдается значительное снижение импорта серверов и хранилищ, вплоть до 67 тыс. шт. в 2024 г. При снижающемся импорте увеличивается производство отечественных серверов и хранилищ — показатель достиг пика в 2023 г., составив 121 тыс. шт., что сопоставимо с импортом товара за 2021 г. Данных по производству серверов и хранилищ за 2024 г. пока нет, но с учетом нынешних тенденций, показатель будет только расти за счет развития российского рынка, а также увеличения производства ключевых компонентов.

Систематически оценить риск всех угроз технологическому развитию представляется невозможным в силу большого числа факторов, необходим индивидуальный подход с учетом особенностей каждой угрозы. Как было рассмотрено ранее, разные виды угроз сопряжены с различными показателями и обстоятельствами, которые необходимо учитывать при анализе. Статистически мера риска оценивается с помощью такого показателя, как среднее квадратическое отклонение.

В целом стандартное отклонение представляет собой меру степени изменчивости значений переменной относительно её среднего как в большую, так и в меньшую сторону. С помощью данного показателя можно провести общую оценку риска, при котором $\sigma \rightarrow 0$ (стандартное отклонение, стремящееся к нулю) будет отражать наименьший уровень риска, так как волатильность показателя будет минимальна. Для оценки угрозы независимо от величин ее абсолютных показателей, используем относительное стандартное отклонение, которое отражает в процентном отношении изменчивость показателя по отношению к ее среднему значению [3]:

$$\sigma = \sqrt{\frac{(x_i - \bar{x})}{n}}.$$

Относительное стандартное отклонение

$$(OCO) = \frac{\sigma}{\bar{x}},$$

где σ — среднее квадратическое отклонение;

$\bar{x}$ — среднее арифметическое анализируемого показателя.

Будем считать, что значения относительного стандартного отклонения от 0% до 20% будут рассматриваться как низкая степень риска, от 20% до 50% средняя степень риска, а свыше 50% — высокая степень риска, так как волатильность слишком вы-

Таблица 2
Расчет показателей риска для импорта и производства серверов и хранилищ

	Импорт	Производство
Стандартное отклонение	22,6	16,2
Среднее значение	81,6	95,75
ОСО	28%	17%

Источник: расчеты авторов по материалам [7; 9].

сока. Исходя из указанной информации, проанализируем результаты расчетов. Относительное стандартное отклонение по импорту составило 28%, что соответствует средней степени риска. При этом у производства серверов и хранилищ стандартное отклонение ниже при более высоком среднем значении, из-за чего относительное стандартное отклонение будет ниже – 17%. Соответственно, и риск в производстве данных товаров ниже, так как присутствует стабильный постепенный рост, не наблюдается значительной волатильности. Таким образом, приведенные показатели компенсируют друг друга, доводя уровень риска до низкой степени.

Для анализа риска реализации угроз в динамике также можно рассматривать изменения по сравнению с базисным значением. В таком случае встает дискуссионный вопрос о выборе упомянутого базисного значения. В рамках анализа упрощенной модели, которая включает в себя данные за период с 2020 по 2024 г., за базис рациональнее взять 2021 г. – санкции 2014 г. уже не оказывают такого сильного влияния, так как экономика и бизнес уже адаптировались, пандемия и связанные с ней логистические ограничения практически перестали влиять на торговлю [16].

По сравнению с 2021 г., в 2022 г. наблюдалось снижение экспорта на 40%. К 2023 г. импорт уменьшился на 41%, а в 2024 г. – на 47% по отношению к базисному периоду. Учитывая подобные тенденции, при которых за три года наблюдается снижение импорта важнейшего элемента современной информационной инфраструктуры, можно сделать вывод о высоком уровне риска угрозы технологическому развитию страны. При этом наращиваются темпы роста внутреннего производства серверов и хранилищ. В 2022 г. был зафиксирован рост в 21%, а к 2023 г. рост производства достиг 48% по отношению к 2021 г. На данном этапе темпы роста производства выше, чем темпы падения импорта данных технологий, из-за чего риск угрозы значительно снижается до низкого уровня.

Для более достоверной оценки риска можно также использовать метод экспертных оценок. В та-

ком случае экспертам предоставляются данные по конкретной отрасли в рамках технологий (в том числе импорт/экспорт, финансирование инноваций), на основе которых, с учетом нынешних обстоятельств, составляется экспертное заключение с итоговым подсчетом вероятности реализации конкретных угроз технологическому развитию страны.

Также, в том числе с участием экспертов, возможна разработка предварительного опросника с учетом общих факторов, которые могли бы увеличить или уменьшить риск угрозы. При выборе варианта, который потенциально увеличивает риск реализации угрозы, будет начисляться определенные «баллы риска», который оценивается эмпирически экспертами в специально установленном. В конце опросника необходимо просуммировать «баллы риска». В качестве базисного риска, который присваивается каждой угрозе, предлагается взять уровень в 0,01, так как согласно теории вероятности вероятность никогда не равна нулю. Пример алгоритма в рамках опросного листа приведен на рис. 2.

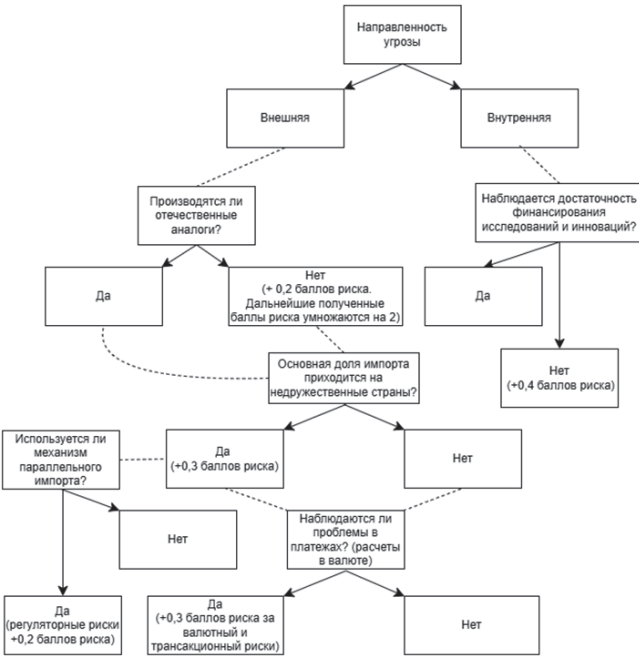


Рис. 2. Опросный лист для определения риска угрозы технологическому развитию
Составлено авторами по материалам [4].

Внешняя угроза подразумевает под собой больший риск, как уже было упомянуто, так как в этом случае существует зависимость от контрагента, валютных рисков, экономической и социальной ситуации, а также прочих обстоятельств. В случае внешней угрозы, к примеру, ограничению поставок, тоже существуют факторы, которые могут отягощать ситуацию, увеличивая риск угрозы. К примеру, от-

сутствие отечественных аналогов, за что в опроснике начисляются дополнительные 0,2 баллов риска, а также присутствует условие, при котором полученные в дальнейшем баллы риска умножаются на коэффициент 2.

Далее рассматривается вопрос локализации страны-экспортера. В случае, если основная доля импорта приходится на недружественные страны, то начисляются баллы риска (+0,2), так как увеличиваются такие риски, как санкционный, валютный, торговый. От данного ответа также существует ответвление на вопрос про использование механизмов параллельного импорта. Параллельный импорт представляет из себя ввоз в страну товаров без разрешения правообладателя торговой марки, что влечет за собой значительное число рисков — регуляторные, риск обслуживания, локализации, подделки. В рамках некоторых сфер, в том числе технологических, планируется запрет параллельного импорта. Необходимо учитывать данные факторы при последующем анализе.

После ответа на дополнительный вопрос (при необходимости) надо вернуться к основному вопросу про проблемы в платежах, в первую очередь в валюте. С некоторыми странами, по договоренностям, ведутся расчеты в рублях, что с одной стороны под-

держивает национальную валюту, а с другой стороны нивелирует валютные риски. При этом доля рубля в расчетах за импорт составляют около 30% [8]. Не стоит забывать и об ограничениях в сторону России в рамках международных платежей, отключение от системы *SWIFT*, а также приостановление деятельности *Visa* и *Mastercard*. Отдельные запреты накладывались на расчеты непосредственно с банками, что также осложняло расчеты с поставщиками.

В рамках внутренних угроз, как уже было упомянуто, анализ должен быть более обширным и глубоким. Основной вопрос, ответ на который мы можем оценить с точки зрения расчета риска угрозы, это наличие достаточного финансирования инноваций и НИОКР как от самого бизнеса в данной сфере, так и от государства в целом. Для ответа необходимо задать следующие дополнительные вопросы — существуют ли проекты, получающие субсидии от государства в рамках разработки технологий? Участвуют ли они в технологических кластерах? Поддерживаются ли они ФРП или другими фондами подобной направленности?

Соответственно, чем больше баллов риска у рассматриваемой угрозы, тем больше вероятность ее наступления. Угроза технологическому развитию, набравшая 0,8 баллов риска, становится более реа-

Таблица 3

Результаты контент-анализа угроз технологическому развитию России, проведенного на основании отчетов иностранных институтов развития

Наименование угрозы технологическому развитию России	Содержание угрозы и ее потенциальная реализация на практике	Агентства и институты развития, опубликовавшие отчет
1. Ограничение доступа к передовым технологиям	- США и ЕС ужесточили ограничения на поставки высокотехнологичной продукции в Россию (чипы, оборудование для полупроводникового производства, системы ИИ, квантовые вычисления); - Россия остается зависимой от зарубежных технологий в микроэлектронике, станкостроении, промышленном ПО	<i>U.S. Bureau of Industry and Security (BIS)</i> [15]; <i>McKinsey</i> [12]
2. Отставание темпов развития критических технологий	- Россия не имеет собственного передового производства чипов (аналогичного <i>TSMC</i> или <i>Samsung</i>); - нехватка вычислительных мощностей (ограничения на поставки <i>GPU</i> от <i>NVIDIA</i>, <i>AMD</i>) и данных для обучения моделей; - западные компании (<i>IBM</i>, <i>Google</i>) и Китай активно развивают квантовые технологии, тогда как Россия отстает в данном направлении; - ограниченный доступ к современным сенсорам и чипам для автономных беспилотных систем	<i>Boston Consulting Group (BCG)</i> [13]; <i>Gartner</i> [14]
3. Отток высококвалифицированных кадров и снижение кооперации с мировыми научными центрами	- После 2022 года десятки тысяч российских <i>IT</i>-специалистов уехали, что ослабило инновационный потенциал нашей страны; - российские ученые и компании исключены из многих глобальных проектов (<i>CERN</i>, <i>ITER</i>, <i>Horizon Europe</i>)	<i>Bloomberg</i> [5]; <i>Nature</i> [11]
4. Киберугрозы и цифровая изоляция	- Западные аналитики (<i>Mandiant</i>, <i>CrowdStrike</i>) прогнозируют рост киберконфликтов; <i>Microsoft</i>, <i>Oracle</i>, <i>SAP</i> свернули или ограничили работу в России, что создает проблемы для представителей бизнеса	<i>Mandiant (Google Cloud)</i> [13]; <i>Reuters</i> [19]
5. Снижение инвестиций в инновации и разработки (<i>R&D</i>)	- Многие западные корпорации (<i>Intel</i>, <i>Siemens</i>, <i>GE</i>) свернули или заморозили <i>R&D</i>-центры в России; - сокращение венчурного финансирования: российские стартапы теряют доступ к международным инвестициям (<i>Sequoia</i>, <i>Y Combinator</i>)	<i>Financial Times</i> [10]; <i>Crunchbase</i> [17]

Источник: составлено авторами.

листичной, чем угроза с 0,4 баллами риска. Опросник может представлять собой лишь предварительный этап анализа угроз, давая представление о возможных критических факторах, которые необходимо учесть в дальнейшем анализе. Также в него можно внести результаты оценки стандартного отклонения и динамического анализа, что позволит комплексно оценить риск.

ОБСУЖДЕНИЕ И ЗАКЛЮЧЕНИЕ

Резюмируя, основными угрозами технологическому развитию России, по мнению авторов, являются кибератаки, зависимость от иностранных технологий и недостаточная защищенность критической инфраструктуры. Решение этих проблем требует комплексного подхода, включая развитие отечественных технологий и усиление мер кибербезопасности. В табл. 3 представлены ключевые угрозы технологическому развитию для Российской Федерации, выявленные при проведении контент-анализа отчетов крупнейших иностранных аналитических агентств и институтов развития.

Таким образом, технологический суверенитет выступает практическим механизмом укрепления научно-технологической безопасности и, как следствие, устойчивого развития страны. Угрозы технологическому развитию целесообразно анализировать отдельно как внешние и внутренние, поскольку они связаны с разными индикаторами и управленческими инструментами. Количественная оценка риска через показатели волатильности (относительное стандартное отклонение) и динамику относительно базисного года позволяет получить сопоставимую «шкалу риска» для отдельных направлений или технологий.

Также в рамках исследования было выявлено, что рост внутреннего производства по критическим позициям способен снижать риск, компенсируя падение импорта, однако эффект зависит от наличия отечественных аналогов и устойчивости цепочек компонентов. Для повышения достоверности управленческих решений статистические расчеты следует дополнять экспертными оценками и регулярным мониторингом, особенно в условиях санкций и роста киберугроз.

Литература

1. Постановление Правительства Российской Федерации от 30 апреля 2009 г. № 372 «Об утверждении перечня технологического оборудования (в том числе комплектующих и запасных частей к нему), аналоги которого не производятся в Российской Федерации, ввоз которого на территорию Российской Федерации не подлежит обложению налогом на добавленную стоимость» [Электронный ресурс]. — URL: https://www.consultant.ru/document/cons_doc_LAW_87496 (дата обращения: 25.01.2026).
2. Распоряжение Российской Федерации от 20.05.2023 № 1315-р (ред. от 21.10.2024) «Об утверждении Концепции технологического развития на период до 2030 года» (ред. от 21 октября 2024 года) [Электронный ресурс]. — URL: https://www.consultant.ru/document/cons_doc_LAW_447895 (дата обращения: 25.01.2026).
3. Ивин Е.А. Учебно-методическое пособие по математической статистике: для социально-экономических специальностей [Текст] / Е.А. Ивин, А.Н. Курбацкий, Д. В. Артамонов. — Вологда: ИСЭРТ РАН, 2017. — 141 с.
4. Гохберг Л.М., Кузьминов Я.И. «Мы часто отстаем не на годы, а в разы» // НИУ ВШЭ [Электронный ресурс]. — URL: <https://issek.hse.ru/news/487052227.html> (дата обращения: 19.01.2026).
5. Более 30% IT-специалистов уехали из России или планируют релокацию // Forbes [Электронный ресурс]. — URL: <https://www.forbes.ru/svoi-biznes/477957-bolee-30-it-specialistov-uehali-iz-rossii-ili-planiruyut-relokaciu> (дата обращения: 17.01.2026).
6. В России из-за высокой ключевой ставки обвалился импорт ПК, смартфонов и бытовой техники // ИА C-News [Электронный ресурс]. — URL: https://www.cnews.ru/news/top/2025-02-17_v_rossii_iz-za_klyuchevoj_stavki (дата обращения: 25.01.2026).

References

1. Decree of the Government of the Russian Federation of April 30, 2009 No. 372 "On approval of the list of technological equipment (including components and spare parts for it), analogues of which are not produced in the Russian Federation, the import of which into the territory of the Russian Federation is not subject to value-added tax" [Electronic resource]. URL: https://www.consultant.ru/document/cons_doc_LAW_87496 (accessed: 25.01.2026).
2. Decree of the Russian Federation dated 05/20/2023 No. 1315-r (as amended on 10/21/2024) "On Approval of the Concept of Technological Development for the period up to 2030" (as amended on October 21, 2024) [Electronic resource]. URL: https://www.consultant.ru/document/cons_doc_LAW_447895 (accessed: 25.01.2026).
3. Ivin E.A. Educational and methodical manual on mathematical statistics: for socio-economic specialties [Text] / E.A. Ivin, A.N. Kurbatsky, D.V. Artamonov. Vologda: ISERT RAS, 2017. 141 p.
4. Gokhberg L.M., Kuzminov Ya.I. "We often lag behind not by years, but by several times" // Higher School of Economics [Electronic resource]. URL: <https://issek.hse.ru/news/487052227.html> (accessed: 19.01.2026).
5. More than 30% of IT specialists have left Russia or are planning to relocate // Forbes [Electronic resource]. URL: <https://www.forbes.ru/svoi-biznes/477957-bolee-30-it-specialistov-uehali-iz-rossii-ili-planiruyut-relokaciu> (accessed: 17.01.2026).
6. In Russia, due to the high key rate, imports of PCs, smartphones and household appliances have collapsed // IA C-News [Electronic resource]. URL: https://www.cnews.ru/news/top/2025-02-17_v_rossii_iz-za_klyuchevoj_stavki (accessed: 25.01.2026).
7. In 2024, the import of servers and storage to Russia decreased by 9% to 67 thousand units // RBC [Electronic resource].

7. В 2024 г. импорт серверов и хранилищ в Россию снизился на 9% до 67 тыс. шт. // РБК [Электронный ресурс]. — URL: <https://marketing.rbc.ru/articles/15649/> (дата обращения: 19.01.2026).
8. Доля рубля при расчетах за импорт с Азией поднялась выше 40% // РБК [Электронный ресурс]. — URL: <https://www.rbc.ru/finances/16/11/2024/673768959a7947856b961c93> (дата обращения: 19.01.2026).
9. За 2019–2023 гг. производство серверов и хранилищ в России выросло в 2,2 раза: с 56 до 121 тыс. шт. // Маркетинговое агентство BusinesStat [Электронный ресурс]. — URL: https://businesstat.ru/news/servers_and_storage (дата обращения: 19.01.2026).
10. Закрытие R&D-центров Siemens в России // РБК [Электронный ресурс]. — URL: <https://www.rbc.ru/business/12/05/2022/627c9d869a7947e1d9ecd922> (дата обращения: 17.01.2026).
11. Изгнание из ЦЕРН: исключение российских ученых из международных проектов // Российская академия наук [Электронный ресурс]. — URL: <https://www.ras.ru/digest/showdnews.aspx?id=fe095681-f570-4b29-978b-aa1315ea1361> (дата обращения: 17.01.2026).
12. Импорт техники в РФ сократился на 3% // ИА «Финмаркет» [Электронный ресурс]. — URL: <https://www.finmarket.ru/main/article/6343568> (дата обращения: 19.01.2026).
13. Прогноз развития киберугроз и средств защиты информации — 2026 // «АМ Медиа» [Электронный ресурс]. — URL: https://www.anti-malware.ru/analytics/Technology_Analysis/Cyber-Threat-and-Information-Security-Forecast-2026 (дата обращения: 17.01.2026).
14. Прогноз Gartner: к 2030 году ИИ поглотит весь ИТ-сектор // Хайтек+ [Электронный ресурс]. — URL: <https://hightech.plus/2025/09/09/prognoz-gartner-k-2030-godu-ii-poglotit-ves-it-sektor> (дата обращения: 17.01.2026).
15. Прогноз PwC о росте глобального рынка полупроводников в 2026-2030 годах на 8,6%. // DRussia [Электронный ресурс]. — URL: <https://d-russia.ru/prognoz-pwc-o-roste-globalnogo-rynka-poluprovodnikov-v-2026-2030-godah-na-8-6.html> (дата обращения: 17.01.2026).
16. Санкции и ограничения в области высоких технологий против России // TAdviser [Электронный ресурс]. — URL: https://www.tadviser.ru/index.php/Статья:Санкции_и_ограничения_в_области_высоких_технологий_против_России (дата обращения: 17.01.2026).
17. Стартапы заняли выжидающую позицию // Коммерсант [Электронный ресурс]. — URL: <https://www.kommersant.ru/doc/8360595> (дата обращения: 17.01.2026).
18. Угрозы технологической безопасности (технологическая угроза) // Энциклопедия терминов МЧС России [Электронный ресурс]. — URL: <https://mchs.gov.ru/ministerstvo/o-ministerstve/terminy-mchs-rossii/term/3084> (дата обращения: 19.01.2026).
19. Comindware заменит решения Terrasoft, SAP, Oracle, Microsoft и других уходящих компаний // TAdviser [Электронный ресурс]. — URL: https://www.tadviser.ru/index.php/Новости:Comindware_заменит_решения_Terrasoft%2C_SAP%2C_Oracle%2C_Microsoft_и_других_уходящих_компаний (дата обращения: 17.01.2026).
20. 98% импорта: почему Россия до сих пор зависит от иностранных станков? // IT-world [Электронный ресурс]. — URL: <https://www.it-world.ru/it-news/8upxdpvs8iskk400gcc4gw8koskk8c4.html> (дата обращения: 17.01.2026).
21. 120 млрд руб. направят на субсидии для НИОКР до 2030 года // Информационно-правовой портал «Гарант» [Электронный ресурс]. — URL: <https://www.garant.ru/news/1686073> (дата обращения: 25.01.2026).
- source]. URL: <https://marketing.rbc.ru/articles/15649> (accessed: 19.01.2026).
8. The share of the ruble in payments for imports from Asia has risen above 40% // RBC [Electronic resource]. URL: <https://www.rbc.ru/finances/16/11/2024/673768959a7947856b961c93> (accessed: 19.01.2026).
9. In 2019–2023, the production of servers and storage in Russia increased 2.2 times: from 56 to 121 thousand units // Marketing Agency Businesstat [Electronic resource]. URL: https://businesstat.ru/news/servers_and_storage (accessed: 19.01.2026).
10. Closure of Siemens R&D centers in Russia // RBC. [Electronic resource]. URL: <https://www.rbc.ru/business/12/05/2022/627c9d869a7947e1d9ecd922> (accessed: 17.01.2026).
11. Expulsion from CERN: exclusion of Russian scientists from international projects // Russian Academy of Sciences [Electronic resource]. URL: <https://www.ras.ru/digest/showdnews.aspx?id=fe095681-f570-4b29-978b-aa1315ea1361> (accessed: 17.01.2026).
12. Import of machinery to the Russian Federation decreased by 3% // IA “Finmarket” [Electronic resource]. URL: <https://www.finmarket.ru/main/article/6343568> (accessed: 19.01.2026).
13. Forecast of the development of cyber threats and information security tools – 2026 // “AM Media” [Electronic resource]. URL: https://www.anti-malware.ru/analytics/Technology_Analysis/Cyber-Threat-and-Information-Security-Forecast-2026 (accessed: 17.01.2026).
14. Gartner forecast: by 2030, AI will consume the entire IT sector // High-tech+ [Electronic resource]. URL: <https://hightech.plus/2025/09/09/prognoz-gartner-k-2030-godu-ii-poglotit-ves-it-sektor> (accessed: 17.01.2026).
15. PwC forecast the global semiconductor market to grow by 8.6% in 2026-2030 // DRussia [Electronic resource]. URL: <https://d-russia.ru/prognoz-pwc-o-roste-globalnogo-rynka-poluprovodnikov-v-2026-2030-godah-na-8-6.html> (accessed: 17.01.2026).
16. Sanctions and restrictions in the field of high technologies against Russia // TAdviser [Electronic resource]. URL: https://www.tadviser.ru/index.php/Статья:Sanctions And restrictions in the field of High Technology Against_Russia (accessed: 17.01.2026).
17. Startups have taken a waiting position // Kommersant [Electronic resource]. URL: <https://www.kommersant.ru/doc/8360595> (accessed: 17.01.2026).
18. Threats to technological safety (technological threat) // Encyclopedia of Terms of the Ministry of Emergency Situations of Russia [Electronic resource]. URL: <https://mchs.gov.ru/ministerstvo/o-ministerstve/terminy-mchs-rossii/term/3084> (accessed: 19.01.2026).
19. Comindware will replace the solutions of Terrasoft, SAP, Oracle, Microsoft and other outgoing companies // TAdviser [Electronic resource]. URL: https://www.tadviser.ru/index.php/Новости:Comindware_solution_terrasoft%2C_SAP%2C_Oracle%2C_MICROSOFT_AND other related companies (accessed: 17.01.2026).
20. 98% of imports: why does Russia still depend on foreign machines? // IT-world [Electronic resource]. URL: <https://www.it-world.ru/it-news/8upxdpvs8iskk400gcc4gw8koskk8c4.html> (accessed: 17.01.2026).
21. 120 billion rubles will be allocated for subsidies for R&D until 2030 // Information and legal portal “Garant” [Electronic resource]. URL: <https://www.garant.ru/news/1686073> (accessed: 01/25/2026).