Научная статья / Original research article
УДК 394:314.15
DOI:10.31660/1993-1824-2025-3-92-108
EDN: AYMGBA

Экономико-социологический анализ рынка кибербезопасности как фактора устойчивой динамики хозяйственной жизни российского общества

С. Г. Симонов, М. А. Хаматханова, И. В. Лысенко

Тюменский индустриальный университет, Тюмень, Россия
**simonovsg@tyuiu.ru*

Аннотация. Цель статьи — рассмотреть российский рынок продуктов и услуг кибербезопасности, проанализировать ключевые модели его развития на перспективу. Определены роль и место кибербезопасности в системе наиболее динамично развивающихся технологических индустрий современной России и изучены основные сегменты киберрынка. Отмечено, что доминирование отечественных игроков на рынке кибепродуктов и киберуслуг является важным фактором развития технологического суверенитета России. Охарактеризованы применяемые методы исследования отечественного рынка продуктов и услуг кибербезопасности, проведен анализ количества и качества его участников. Изучены необходимость, возможности и процедура возвращения иностранных IT-компаний на рынок кибербезопасности России в разрезе ключевых моделей его развития. Обоснована необходимость перехода на отечественные решения в области обеспечения безопасности информационно-цифрового пространства. Детализирован алгоритм импортозамещения иностранных киберпродуктов и киберуслуг отечественными аналогами и указаны трудности его практической реализации в России в условиях экономических санкций Запада. Составлен рейтинг трудностей, имеющих место при внедрении модели импортозамещения иностранных киберпродуктов и киберуслуг отечественными аналогами в современной России. Выявлены факторы улучшения инновационно-технологического ландшафта российского рынка кибербезопасности на период до 2030 года.

Ключевые слова: рынок продуктов и услуг кибербезопасности, модели развития российского рынка кибербезопасности, параллельный импорт киберпродуктов, программное обеспечение, инновационно-технологический ландшафт

Для цитирования: Симонов, С. Г. Экономико-социологический анализ рынка кибербезопасности как фактора устойчивой динамики хозяйственной жизни российского общества / С. Г. Симонов, М. А. Хаматханова, И. В. Лысенко. – DOI 10.31660/1993-1824-2025-3-92-108 // Известия высших учебных заведений. Социология. Экономика. Политика. – 2025. – № 3. – С. 92–108. – EDN: AYMGBA

An economic and sociological analysis of the cybersecurity market as a factor of sustainable economic dynamics in russian society

Sergey G. Simonov*, Makka A. Khamatkhanova, Igor V. Lysenko

Industrial University of Tyumen, Tyumen, Russia
**simonovsg@tyuiu.ru*

Abstract. This paper aims to examine the Russian market for cybersecurity products and services while analyzing key models for its future development. The study highlights the role and significance of cybersecurity within Russia's rapidly advancing high-tech industries and identifies the main segments of the domestic cyber market.

It emphasizes the dominance of Russian companies in the cybersecurity sector as a critical factor in achieving technological sovereignty. The paper describes the methods used to study the domestic cybersecurity market and presents an analysis of both the quantity and quality of market participants. It explores the necessity, potential, and methods for the return of foreign IT companies to the Russian cybersecurity market in light of its key development models. The authors argue for the strategic importance of transitioning to domestic cybersecurity solutions to secure the country's digital information space. The paper provides a detailed framework for replacing foreign cyber products and services with Russian alternatives while discussing the challenges of implementing this model within the context of Western economic sanctions. A ranking of the main difficulties encountered during the implementation of import substitution in Russia is also presented. Finally, the paper identifies factors that could enhance the innovation and technology landscape of the Russian cybersecurity market by 2030.

Keywords: cybersecurity, cybersecurity products and services market, models of development of the Russian cybersecurity market, parallel import of cybersecurity products, import substitution of foreign cybersecurity products and services, software (SW), innovation and technology landscape

For citation: Simonov, S. G., Khamatkhanova, M. A., & Lysenko, I. V. (2025). Economic and sociological analysis of the domestic cybersecurity market as a factor of sustainable economic dynamics in Russian society. Proceedings of Higher Educational Institutions. Sociology. Economics. Politics, (3), pp. 92-108. (In Russian). DOI : 10.31660/1993-1824-2025-3-92-108

Введение

По оценкам Cybersecurity Ventures, количество ежегодных хакерских атак в мире за последние десять лет удвоилось, а глобальный ущерб от них вырос в 3,3 раза и в 2025 году составил 10 трлн долларов [1]. В нашей стране только за 2024 год было зафиксировано 486 тыс. подобных преступлений, финансовые потери от которых превысили 200 млрд рублей, что на 36 % больше показателя предыдущего года [2]. Эти и другие статистические данные, как и многочисленные аналитические материалы, свидетельствуют о выходе проблемы кибербезопасности за пределы технологической сферы и ее становлении объектом стратегического управления. Сегодня наукой и хозяйственной практикой кибербезопасность не сводится лишь к решению относительно узкой задачи защиты ведомственной или корпоративной IT-инфраструктуры. Она рассматривается как ключевой фактор динамики цифровой экономики страны, интегрально отражающий финансовую стабильность, конкурентные преимущества и операционную устойчивость хозяйствующих субъектов на макроэкономическом уровне. В настоящее время, согласно данным российского Фонда развития интернет-инициатив, кибербезопасность входит в десятку наиболее динамично развивающихся технологических индустрий страны (рис. 1).

Будучи включенной в систему рыночных отношений, кибербезопасность в Российской Федерации (РФ) представлена сложной экосистемой отечественных игроков, которая насчитывает свыше 300 специализирующихся на этом секторе компаний, и несколькими международными игроками, сохранившими свое присутствие на российской территории. В качестве объектов купли-продажи здесь выступают киберпродукты и киберуслуги, что, на наш взгляд, дополняет картину реально сформировавшегося рынка кибербезопасности в нашей стране.

Рис. 1. ***Наиболее динамично развивающиеся технологические индустрии современной России [3]***

Хотя сегодня Россия выступает одним из лидеров по емкости рынка киберпродуктов и киберуслуг, соотношение доли расходов на безопасность в информационно-цифровом пространстве и объема валового внутреннего продукта у нее значительно уступает ведущим европейским странам, Соединенным Штатам Америки (США) и Канаде. Тем не менее за три последних года (2022–2024) отечественный рынок кибербезопасности ежегодно прирастал почти на 25 %, что делает его одним из наиболее динамичных сегментов рынка информационных технологий, и к началу 2025 года годовой доход достиг 299 млрд рублей [4]. Это делает его одним из наиболее динамично развивающихся звеньев единого IT-рынка страны.

Как отмечалось выше, российский рынок кибебезопасности представлен двумя основными сегментами: на 70 % киберпродуктами и на 30 % киберуслугами. В свою очередь, эти киберпродукты дифференцируются на такие подсегменты, как сетевая и облачная безопасность; решения анализа, контроля и реагирования на киберугрозы и

уязвимости бизнес-деятельности компаний; защита данных, конечных точек; решения управления киберрисками; предотвращения кибермошенничества. Дифференциацию последних иллюстрирует рисунок 2.

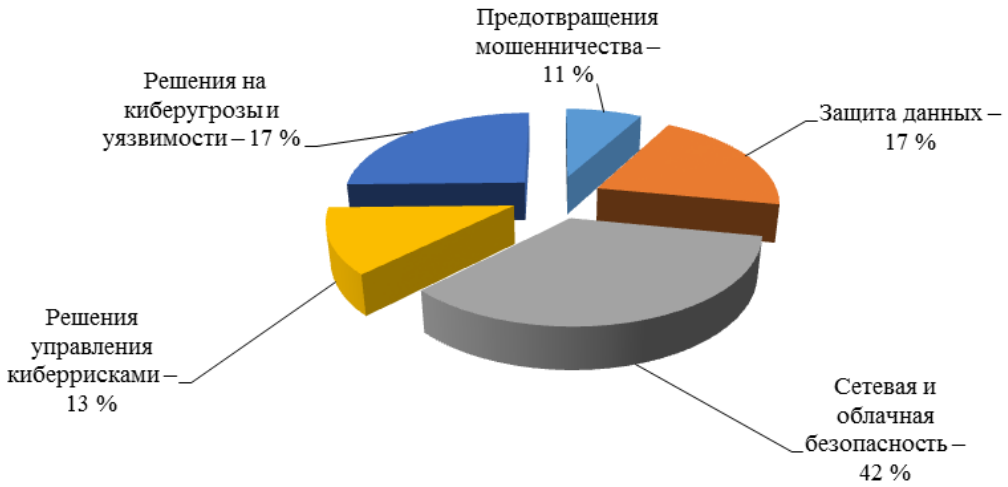

Рис. 2. ***Дифференциация продуктов кибербезопасности на подсегменты (в процентах к итогу)***

Другой сегмент рынка кибербезопасности РФ включает набор киберуслуг, дифференцированных на три подсегмента (в процентах к итогу):

- услуги мониторинга и обеспечения кибербезопасности (MDR) — 48 %;
- услуги аутсорсинга и управляемые сервисы кибербезопасности — 37 %;
- услуги SOC — 15 % [5].

Доминирование отечественных игроков на рынке кибепродуктов и киберуслуг является важным фактором развития технологического суверенитета России. Пожалуй, к наиболее крупным из них можно отнести в части киберпродуктов «Лабораторию Касперского», Positive Technologies, ИнфоТеКС, «Код Безопасности», UsetGate, а в части киберуслуг — ГК «Солар», «Инфосистемы Джет», BI.Zone, Innostage, Angara Security [6].

С начала 2022 года значительная часть зарубежных игроков ушла с российского рынка кибербезопасности. В настоящее время этот процесс замедлился. Более того, некоторые из ушедших иностранных вендоров не прочь вернуться назад. Отметим, что несмотря на ощутимое уменьшение присутствия зарубежных компаний на отечественном рынке кибербезопасности до 7 %, доля их киберпродуктов в РФ в установленной базе средств защиты остается высокой — от 10–20 % для отдельных классов программного обеспечения (ПО) и до 40–50 % в сфере сетевой безопасности [7].

Методы исследования

В настоящей статье для сбора эмпирического материала, лежащего в основе исследования проблемы феномена российского рынка продуктов и услуг кибербезопасности и

основных трендов его развития, использовались такие методы, как анализ вторичных данных, экспертная оценка, анкетирование.

Первый из указанных методов состоит в том, чтобы первоначально подробно изучить как отечественные, так и зарубежные материалы по исследуемой тематике. На следующем этапе проводится анализ, верификация полученных данных и интерпретация результата. Кроме того, метод позволяет заложить основы построения некоего алгоритма реализации определенной модели развития рынка кибербезопасности.

Методом экспертной оценки проведено исследование двух групп экспертов:

- управленцев среднего и высшего звена различных хозяйствующих субъектов, принявших участие в федеральной программе «Производительность труда и поддержка занятости», для реализации которой Тюменская область была выбрана пилотной территорией;
- представителей различных некоммерческих территориальных органов и структур, которые напрямую не осуществляют бизнес-деятельность (органов власти, научных и общественных организаций).

Благодаря применению метода удалось дать рейтинговую оценку наиболее динамично развивающимся технологическим индустриям в регионах современной России, представление об инновационно-технологическом ландшафте ее рынка киберпродуктов и киберуслуг.

Анкетирование позволило осуществить дифференциацию киберпродуктов и киберуслуг на подсегменты, выявить ожидания российских субъектов хозяйствования в деле выполнения указов президента РФ об импортозамещении ПО на объектах критической информационной инфраструктуры и обязательном отказе от использования произведенных в недружественных странах средств защиты, выяснить причины неполного и медленного перехода на отечественное ПО.

Результаты и обсуждение

На наш взгляд, решение проблемы развития в стране рынка продуктов и услуг в области кибербезопасности кроется в анализе:

- количества и качества его участников;
- необходимости, возможности и процедуры возвращения иностранных IT-компаний на рынок кибербезопасности РФ в разрезе ключевых моделей его развития.

I. Анализ количества и качества участников отечественного рынка кибербезопасности. За последнее пятилетие в нашей стране число участников рынка кибербезопасности увеличилось более чем на 1/3, однако подобный рост сопровождается нехваткой профильной экспертизы и структурных решений, квалифицированных кадров и профильной экспертизы. Кроме того, отмеченный тренд, на наш взгляд, в разрезе регионов далеко не всегда отражает реальную картину присутствия в них бизнеса по причине регистрации юридических лиц с целью получения налоговых льгот.

Так, на начало июня 2025 года компаний-участников рынка кибербезопасности в РФ насчитывалось 11,5 тыс. против 8,4 тыс. в январе 2020 года. Лидерами по регионам выступили Москва (4,2 тыс. юрлиц), Санкт-Петербург (1 тыс.) и Московская область (0,9 тыс. юрлиц). Но если сравнивать по темпам роста, то «впереди планеты всей» оказались Калмыкия (+566 %), Чечня (+333 %) и Ингушетия (+200 %), что связано с административными и налоговыми стимулами [8].

Количественно самый большой прирост (+91,4 %) показывают компании, которые занимаются производством средств киберзащиты, информационных и телеком-систем. Вместе с тем сюда входят не только периферийные устройства и инфраструктурные решения, но и защищенные планшеты, смартфоны, ноутбуки, системы связи и специализированное оборудование, которое активно используется всеми хозяйствующими субъектами, включая силовые ведомства. Следовательно, во многом поступательная динамика численности участников отечественного рынка кибербезопасности обеспечивается госзаказом, создающим системный спрос на защищенную технику российского производства, поддержкой федеральных властей, усложнением киберугроз и ужесточением требований к обеспечению защиты информационно-цифрового пространства.

Еще одним фактором увеличения числа компаний, функционирующих в сфере кибербезопасности, выступают изменения структуры спроса на киберпродукты и киберуслуги, вызванные появлением на этом рынке бизнес-структур малого и среднего форматов. Последние до 2022 года почти не работали с киберпродуктами и киберуслугами, а ограничивались использованием Open Source — решений. Сегодня, когда для бизнеса «второго эшелона» жизненно важно достижение баланса между реализацией собственной риск-стратегии и уровнем ее защищенности, ситуация существенно поменялась, обусловив рост числа участников отечественного рынка кибербезопасности.

Наметившийся тренд на увеличение количества компаний, функционирующих на российском рынке киберпродуктов и киберуслуг, сопровождается известными подвижками в средней численности киберспециалистов по отдельным группам бизнес-структур страны (рис. 3).

Наши исследования по бизнес-структурам различных форматов показали, что у субъектов малых форм хозяйствования (микропредприятия, индивидуальные предприниматели, самозанятые, классические малые предприятия) специалисты по кибербезопасности, как правило, отсутствуют; в среднем бизнесе чаще всего их имеется от 3 до 5, в редких случаях немногим больше; на отечественных крупных предприятиях диапазон числа специалистов по кибербезопасности гораздо шире и имеет ярко выраженную отраслевую зависимость.

Однако, как отмечают аналитики, поступательное развитие киберотрасли в стране приводит к дефициту ИБ-кадров, а наиболее востребованными выступают senior-специалисты, способные выстраивать сложные защитные стратегии и принимающие стратегические архитектурные решения. В настоящее время российский бизнес

массово ищет специалистов по кибербезопасности, которых реально мало, поскольку большинство кандидатов не проходят отбор из-за низкого уровня подготовки. Уже в первом квартале 2025 года на отечественном рынке труда появилось 41,8 тыс. вакансий в сфере кибербезопасности, что составляет почти половину (47 %) общего числа таких предложений за весь 2024 год, когда их насчитывалось 89,9 тыс. [10].

Рис. 3. ***Средняя численность специалистов по кибербезопасности по группам бизнес-структур в РФ [9]***

Рост вакансий сопровождается повышением зарплат, которые в киберотрасли растут опережающими темпами по сравнению с IT-сферой в целом. Медианная зарплата в отрасли за период 2021–2025 годов увеличилась на 28 %, поднявшись с 77,8 тыс. фактически до 100,0 тыс. рублей в месяц. Еще более высока она у киберспециалистов с опытом: сегодня среднее зарплатное предложение составляет при стаже от 3 до 6 лет 158,9 тыс. рублей, свыше 6 лет — до 259,2 тыс. рублей [11]. Очевидно, для опытных

кандидатов на должности киберспециалистов, особенно на позиции middle и senior, бизнес предлагает уровень оплаты, зачастую превышающий их рыночные ожидания. В то же время те соискатели, у которых стаж и опыт работы в киберотрасли незначительны или их вообще нет, не говоря уже о наличии сертификатов, рассчитывать на высокие предложения по заработной плате не могут.

Добавим, что спрос на специалистов в области кибербезопасности повышается не только из-за развития IT-технологий, но и вследствие усиления нормативного давления, например, внедрения оборотных штрафов для компаний, допустивших повторные утечки персональных данных своих сотрудников. Это заставляет бизнес пересматривать корпоративную политику безопасности и стабильно увеличивать число вакансий в среднем на 4–6 % в месяц.

Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации запустило [12] новый проект, позволяющий разработчикам программного обеспечения пройти сертификацию своих навыков и получить официальный документ о квалификации. Эксперимент призван предоставить современный инструмент для объективной оценки профессиональных компетенций.

Программа доступна для всех желающих — участие не требует определенного уровня образования или привязки к конкретному месту работы. Процесс полностью добровольный и бесплатный. Чтобы получить сертификат, нужно зарегистрироваться на платформе, пройти тесты и выполнить практические задания. Документ выдается в электронном формате через «Госуслуги». Личная информация участников защищена — доступ к данным будет только у самого разработчика. Полученный сертификат можно использовать для подтверждения квалификации перед работодателем или проверки собственных знаний.

Эксперимент поможет соискателям и компаниям быстрее находить друг друга, акцентируя внимание на актуальных навыках, востребованных на рынке. Для разработчиков это станет дополнительным шансом подтвердить квалификацию или улучшить карьерные перспективы. Проект действует до 31 декабря 2026 года. Оператор платформы будет выбран из числа организаций, предложивших свои кандидатуры.

Завершая анализ количества и качества участников отечественного рынка кибербезопасности, заметим, что мнения о том, стоит ли ожидать на нем продолжения роста количества вендоров, у IT-специалистов разделились. Одна их часть, основу которой составили представители ГК «Солар», стоит на позиции существования хронического дефицита киберразработчиков, в результате чего многие сегменты рынка кибербезопасности, на их взгляд, монополизированы, а качество предлагаемых киберпродуктов и киберуслуг уступает тому, что было у ушедших из России зарубежных компаний. Другая часть IT-специалистов (например, представители отечественного ООО «Системный софт») считает, что в настоящее время на рынке кибербезопасности появилось много вендоров, которые часто не способны предложить зрелые решения. Согласно нашему прогнозу дилемма

может разрешиться в течение ближайших лет, когда компании-лидеры консолидируются, усилят свои рыночные позиции за счет поглощений или слияний с другими, а компании-аутсайдеры, недостаточно зрелые и применяющие устаревшие, неэффективные бизнес-модели, не выдержат конкуренции и уйдут с рынка кибербезопасности.

II. Анализ необходимости, возможности и процедуры возвращения иностранных IT-компаний на рынок кибербезопасности РФ в разрезе ключевых моделей его развития

- По нашему мнению, прологом к этому анализу выступает рассмотрение ключевых моделей отечественного рынка кибербезопасности и выявление их преимуществ и недостатков.
- Сервисная модель, имманентная крупному бизнесу с большим количеством юридических лиц, позволяющая справиться с масштабом путем предоставления единого набора стандартных услуг для всех бизнес-единиц, помогающая оптимизировать издержки и безболезненно масштабирующаяся при покупке новых активов. При ее использовании бизнес, не способный самостоятельно заменить или наладить все свои информационные системы, делегирует данный сегмент защиты профильному провайдеру киберуслуг, но оставляет за собой администрирование и владение ими. Пожалуй, одним из главных ее недостатков выступает, на наш взгляд, тот факт, что для повышения или хотя бы сохранения своего интегрального уровня киберзащищенности корпорации может понадобиться более глобальная переконфигурация ее IT-архитектуры. Что касается преимуществ сервисной модели развития киберрынка, то главным из них является получение предприятием-заказчиком готовых процессов обеспечения защиты в информационно-цифровой пространстве. На практике это выглядит следующим образом: внешний провайдер в границах своих сервисов закупает технические средства, аппаратные платформы и программное обеспечение (ПО), а предприятие-заказчик получает доступ к компетенциям и экспертизе специалистов с возможностью проконсультироваться по вопросам обеспечения кибербезопасности.
- Модель, основанная на параллельном импорте киберпродуктов и киберуслуг, активно применяемая российскими бизнес-структурами с апреля 2022 года. Ее популярность в значительной степени объясняется уходом иностранных IT-компаний с рынка кибербезопасности России и частичной или даже полной приостановкой поставок своих товаров. Согласно этой модели компании-дистрибьюторы строго по легитимно установленному Министерством промышленности и торговли Российской Федерации перечню ввозят киберпродукты из-за границы, не спрашивая разрешения производителя. За год (с апреля 2022 года по март 2023-го) объем их поставок в нашу страну по параллельному импорту достиг 20 млрд долларов [13]. Проведенный нами SWOT-анализ основанной на параллельном импорте киберпродуктов и киберуслуг модели позволяет утверждать, что она имеет преимущества в кратко- и среднесрочной перспективе (помогает избежать риска дефицита киберпродуктов в период оттока запад-

ных брендов, возможность самостоятельно выбирать страну закупки: Европы, Америки или Азии, на ввозимые по параллельному импорту киберпродукты действуют гарантии сроком на один год с момента продажи). Недостатки данной модели развития рынка кибербезопасности в нашей стране дают о себе знать в долговременной перспективе под влиянием низкоэффективной из-за СВО, международных санкций и ограничений логистики российского бизнеса, значительно усложнившейся за последние годы цепочки закупок, отсутствия скидок и ретро-бонусов от зарубежных компаний-производителей, девальвации рубля [14].

- Модель импортозамещения с постепенным полным переходом на отечественные решения, нацеленная на уменьшение зависимости от иностранных технологий, ПО и оборудования, а также на развитие отечественных аналогов и альтернативных подходов к обеспечению кибербезопасности. Ее актуальность для динамичного развития отечественного рынка кибербезопасности и цифровой экономики РФ в целом связана с тремя главными приоритетами — сохранением стратегической независимости на основе защиты жизненно важных сферы и отраслей народного хозяйства от влияния геополитических факторов; наиболее полной реализацией экономических интересов хозяйствующих субъектов нашей страны в целях повышения благосостояния ее граждан; минимизацией хозяйственных, социальных и киберрисков, связанных с введением экономических санкций недружественных стран в отношении России.

Как процесс импортозамещение зарубежных киберпродуктов и киберуслуг отечественными аналогами легко моделируется с разбивкой на ряд этапов, что, несомненно, с макроэкономических позиций является его важным преимуществом.

I этап: анализ информационной инфраструктуры, позволяющий реально оценить текущие средства кибербезопасности и определить потребности в них;

II этап: подбор потенциальных решений в виде выбора отечественных аналогов с учетом отраслевой и региональной специфики бизнес-структуры;

III этап: внедрение и настройка (установка) средств киберзащиты с минимальным воздействием на корпоративные бизнес-процессы;

IV этап: обучение сотрудников российских корпораций посредством повышения квалификации и сертификации в целях эффективного использования новых средств киберзащиты [15].

Однако то, что легко в теории, не всегда безболезненно и быстро реализуется на практике. Именно это и происходит сегодня при внедрении модели импортозамещения иностранных киберпродуктов и киберуслуг отечественными аналогами. Нами составлен рейтинг трудностей, имеющих место при внедрении модели импортозамещения иностранных киберпродуктов и киберуслуг отечественными аналогами в современной России (табл.1).

Таблица 1

Рейтинг трудностей, имеющих место при внедрении модели импортозамещения иностранных киберпродуктов и киберуслуг отечественными аналогами в современной России

№ п/п	Наименование трудностей внедрения модели импортозамещения иностранных киберпродуктов и киберуслуг отечественными аналогами	Ранг значимости трудностей внедрения модели импортозамещения иностранных киберпродуктов и киберуслуг отечественными аналогами
1	Неотлаженность механизма государственной поддержки импортозамещения продуктов и услуг в области кибербезопасности	I
2	Несовместимость отечественных средств киберзащиты с последними версиями российских операционных систем и платформами виртуализации	V
3	Неиспользование российскими предприятиями-разработчиками зарубежных практик безопасной разработки ПО	X
4	Нехватка решений в области средств защиты от DDoS-атак	III
5	Недостаточная развитость и слабая функциональность отечественных средств киберзащиты по сравнению с ушедшими иностранными решениями	VII
6	Дефицит квалифицированных и сертифицированных специалистов в области IT в целом и кибербезопасности в частности	II
7	Практически полное отсутствие в России компаний, создающих сигнатуры для решения классов «предотвращения и обнаружения вторжений», антивирусных средств, баз URL-адресов и баз данных о киберугрозах	VI
8	Появление в РФ «черных» разработчиков свободно распространяемого ПО для нанесения ущерба IT-инфраструктуре отечественных компаний	VIII
9	Хронический недостаток кибернавыков и компетенций	IV
10	Несовершенство законодательной базы в РФ	IX

Недавно в России вышли два президентских указа, касающихся запрета органам госвласти и госкорпорациям использовать иностранное ПО на принадлежащих им значимых объектах критической информационной инфраструктуры, а также запрета на применение отечественным бизнесом средств киберзащиты, иностранных сервисов и киберуслуг из недружественных стран [16]. В связи с этим ассоциация BISA (Business Information Security Association) провела опрос представителей российского бизнеса на предмет их выполнения. Его результаты приведены на рисунке 4.

Рис. 4. ***Результаты опроса Business Information Security Association (BISA) российских субъектов хозяйствования о выполнении указов президента РФ об импортозамещении ПО на объектах критической информационной инфраструктуры и запрете на применение отечественным бизнесом средств киберзащиты, иностранных сервисов и киберуслуг из недружественных стран (в процентах к итогу) [17]***

Как видно из рисунка 3, ожидания представителей российского бизнеса были весьма оптимистичными. Однако на начало 2025 года лишь 60 % отечественных бизнес-структур смогли осуществить импортозамещение иностранных технологий, включая системы кибербезопасности. При этом доля внедрения российского софта на объектах критической информационной инфраструктуры компаний нефтегазового сектора страны оказалась значительно меньше — в среднем 30–40 % [18].

Достаточно дискуссионным, по нашему мнению, является вопрос: «Как относиться к возможному возвращению зарубежных вендоров на отечественный рынок киберпродуктов и киберуслуг?». С одной стороны, очевидно, что этого не стоит опасаться, поскольку возникающая при этом конкуренция на рынке программных и киберпродуктов есть необходимое условие его развития. С другой стороны, для киберрынка России возвращение крупных зарубежных вендоров в стратегически важные секторы национальной экономики (энергетику, транспорт, нефтегазовый сектор) должно контролироваться государством и, что не менее важно, происходить на условиях последнего. Иначе, во-первых, будет невозможно защитить достигнутые на начало 2025 года позиции отечественных решений, когда российские программные продукты и киберпродукты покрыли 80 % рыночных потребностей [19]. Во-вторых, продукция иностранных компаний оперативно займет значительную долю рынка кибебезопасности, чему в определенной мере способствуют экономические санкции недружественных стран и отсутствие законодательного запрета на деятельность зарубежных вендоров в РФ. Поэтому, на наш взгляд, достаточно эффективны будут протекционистские меры в обла-

сти кибербезопасности отечественных бизнес-структур от обязательной регистрации до ограничений зарубежных вендоров в стратегически важных секторах экономики стран.

Выводы

В настоящее время в функционировании отечественного рынка кибербезопасности задействованы, хотя и в разной степени, все три названные модели. Однако в долговременной перспективе упор будет сделан на импортонезависимость, где вначале главным фактором будет финансовая господдержка. Она будет осуществляться через особо значимые национальные проекты — решения, способные заменить зарубежные программные продукты и киберпродукты отечественными аналогами в условиях санкционного давления на российскую экономику со стороны недружественных стран. Финансовая поддержка модели импортозамещения на рынке программных и киберпродуктов страны предполагает на период 2025–2027 годов направлять ежегодно на развитие и внедрение отечественных IT-решений, в том числе решений по кибербезопасности, из федерального бюджета по 4,5 млрд рублей [20]. Однако одной лишь государственной финансовой подушки будет, на наш взгляд, недостаточно для устойчивого и поступательного развития рынка кибербезопасности России. Потребуются консолидированные усилия региональных и местных органов власти, а также отечественного бизнеса разного формата. Только совместно можно достичь девятого уровня технологической готовности и улучшить инновационно-технологический ландшафт российского рынка кибербезопасности.

Проведенный нами в начале 2025 года опрос более 250 IT-специалистов Тюменской области позволил выявить, под влиянием каких факторов в ближайшие 5 лет может улучшиться инновационно-технологический ландшафт российского рынка кибербезопасности (рис. 5).

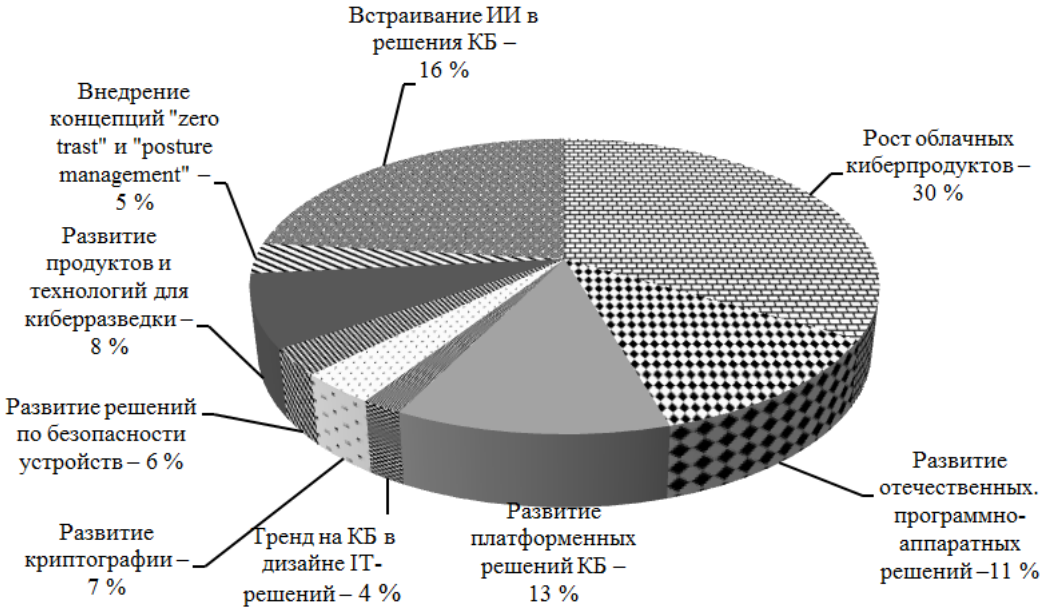

Рис. 5. ***Факторы улучшения инновационно-технологического ландшафта российского рынка кибербезопасности на период до 2030 года (в процентах к итогу)***

Таким образом, эффективное использование выделенных средств из федерального бюджета, привлечение денежных ресурсов из региональных, муниципальных и корпоративных источников, а также учет влияния факторов улучшения инновационно-технологический ландшафта российского рынка кибербезопасности обеспечат высокую динамику его развития на период до 2030 года.

Список источников

1. «No honor among thieves»: M&S hacking group starts turf war/ URL: /https://arstechnica.com/security/2025/07/ (дата обращения 07.07.2025). – Текст : электронный.

2. В Госдуме поддержали законопроект о защите россиян от кибермошенников. – URL: //https://cisoclub.ru/chislo-uchastnikov-rynka-informacionnoj-bezopasnosti-vyroslo-na-41-za-5-let/ (дата обращения : 20.03.2025). – Текст : электронный.

3. Прибыль российских ИКТ-компаний за год выросла на 22,6% и достигла 1,17 триллионов. – URL: //https://www.cnews.ru/news/top/2025-03-10_v_rossii_pribyl_ikt-kompanij (дата обращения: 10.03.2025). – Текст : электронный.

4. Информационная безопасность (рынок России). – URL://https:// www.tadviser.ru/index.php/ (дата обращения: 19.03.2025). – Текст : электронный.

5. Информационная безопасность — один из ключевых драйверов роста ИТ-рынка и может достигнуть порядка 681 млрд рублей или 14 % от общего объема ИТ-рынка к 2030 году. – Текст : электронный // b1.ru : сайт. – 2025. – 19 марта. – URL: //https://b1.ru/insights/news/media-center/b1-russian-information-security-market-survey-press-release-19-march-2025/ (дата обращения: 19.03.2025)

6. Российский рынок информбезопасности вырастет в 2,3 раза к 2030 году. — Текст : электронный // Прайм : сайт. – 2025. – 20 марта. – URL: https://1prime.ru/20250320/informbezopasnost-855964660.html (дата обращения: 20.03.2025)

7. Информационная безопасность к 2030 г. может достичь 681 млрд руб. или 14 % от общего объема ИТ-рынка. – URL: //https://www.comnews.ru/content/238392/2025-03-20/2025-w12/1010/ (дата обращения: 20.03.2025). – Текст : электронный.

8. Крупанин, Ф. В безопасности становится тесно / Ф. Крупанин. – Текст : электронный // Коммерсантъ : сайт. – 2025. – 9 июля. – URL: // https://www.kommersant.ru/doc/7872228 (дата обращения: 09.07.2025).

9. Курс на киберустойчивость: как изменились стратегии CISO / А. Морковчин, Е. Агеева, А. Мусаев, И. Павлова. – Текст : электронный // jetcsirt.su : сайт. – URL: https://jetcsirt.su/upload/%D0%9A%D0%B0%D0%BA%20%D0%B8%D0%B7%D0%BC%D0%B5%D0%BD%D0%B8%D0%BB%D0%B8%D1%81%D1%8C%20%D1%81%D1%82%D1%80%D0%B0%D1%82%D0%B5%D0%B3%D0%B8%D0%B8%20CISO.pdf (дата обращения : 11.01.2025)

10. Сизова, Н. Спрос на специалистов по кибербезопасности растет на 18 % год к году / Н. Сизова. – Текст : электронный // URL: https://www.vedomosti.ru/technology/articles/2025/06/06/1115445 (дата обращения: 06.06.2025)

11. Литвинов, Р. В России почти удвоилось число вакансий в сфере кибербезопасности / Р. Литвинов. – Текст : электронный // Инфобезопасность : сайт. – 2025. – 6 июня. – URL: https://infobezopasnost.ru/blog/news/ (дата обращения: 06.06.2025).

12. Проект Постановления Правительства Российской Федерации «О проведении эксперимента по предоставлению разработчикам программного обеспечения возможности добровольного подтверждения компетенций». – Текст : электронный //Федеральный портал проектов нормативных правовых актов: сайт. – URL: https://regulation.gov.ru/Regulation/Npa/PublicView?npaID=152861 (дата обращения: 03.12.2024).

13. Перцева, Е. На сером фоне: власти сокращают параллельный импорт товаров в РФ / Е. Перцева. – Текст : электронный // Известия : сайт. – 2025. – 17 апр. – URL: https://iz.ru/1871753/evgeniia-pertceva/ (дата обращения: 17.04.2025).

14. Параллельный импорт — потому что всем параллельно… или перпендикулярно. – Текст : электронный // habr.com: сайт. – 2023. – 1 ноября. – URL: https://habr.com/ru/ companies/x-com/articles/771190/ (дата обращения: 01.11.2023).

15. Еронин, В. Реализация стратегии импортозамещения в сфере ИБ по версии «Крайон» / В. Еронин. – Текст : электронный // Инфобезопасность : сайт. – 2024. – 11 сент. – URL: https://infobezopasnost.ru/blog/articles/ (дата обращения: 11.09.2024).

16. Хакеры после запрета западных средств защиты пытаются привлечь специалистов РФ. – Текст : электронный // ТАСС : сайт. – 2025. – 21янв. – URL: // https://tass.ru/ekonomika/22932489 (дата обращения: 21.01.2025).

17. Импортозамещение в сфере информационной. – URL: https://www.tadviser.ru/index.php/ (дата обращения: 24.09.2024). – Текст : электронный.

18. Гурьянов, С. С КИИ – бди: большинство кибератак приходится на критическую инфраструктуру / С. Гурьянов. – Текст : электронный // Известия : сайт. – 2025. – 17 янв. – URL: https://iz.ru/1822780/sergei-guranov/ (дата обращения: 17.01.2025).

19. Арялина, М. IT-отрасль прорабатывает условия возвращения иностранных компаний в Россию / М. Арялина. – Текст : электронный // Ведомости : сайт. – 2025. – 24 апр. – URL: https://www.vedomosti.ru/technology/articles/2025/04/24/1106343-it-otrasl-prorabativaet-usloviya-vozvrascheniya-inostrannih-kompanii (дата обращения: 24.04.2025).

20. Устинова, А. РФРИТ получит более 13 млрд рублей на гранты для IT-компаний / А. Устинова. – Текст : электронный // Ведомости : сайт. – 2025. – 13 мая. – URL: https://www.vedomosti.ru/technology/articles/2025/05/13/1109612-rfrit-poluchit-bolee-13-mlrd-rublei (дата обращения: 13.05.2025).

References

1. «No honor among thieves»: M&S hacking group starts turf war. (In English). Available at : //https://arstechnica.com/security/2025/07/ (accessed on 07/07/2025)

2. V Gosdume podderzhali zakonoproekt o zashchite rossiyan ot kibermoshennikov. (In Russian). Available at : //https://cisoclub.ru/chislo-uchastnikov-rynka-informacionnoj-bezopasnosti-vyroslo-na-41-za-5-let

3. The profit of Russian ICT companies increased by 22.6% over the year and reached 1,17 trillion. (In Russian). Available at : https://www.cnews.ru/news/top/2025-03-10_v_rossii_ pribyl_ikt-kompanij (accessed on March 10, 2025)

4. Informatsionnaya bezopasnost' (rynok Rossii). (In Russian). Available at : https://www.tadviser.ru/index.php/ (accessed on 19.03.2025)

5. Informatsionnaya bezopasnost' — odin iz klyuchevykh drayverov rosta IT-rynka i mozhet dostignut' poryadka 681 mlrd rubley ili 14 % ot obshchego ob"ema IT-rynka k 2030 godu.

(2025). (In Russian). Available at : https://b1.ru/insights/news/media-center/b1-russian-information-security-market-survey-press-release-19-march-2025/ (accessed on 19 March 2025)

6. Rossiyskiy rynok informbezopasnosti vyrastet v 2,3 raza k 2030 godu. (2025). (In Russian). Available at : https://1prime.ru/20250320/informbezopasnost-855964660.html (accessed on March 20, 2025)

7. Informacionnaya bezopasnost' k 2030 g. mozhet dostich' 681 mlrd rub. ili 14 % ot obshchego ob"ema IT-rynka. (In Russian). Available at : //https://www.comnews.ru/content/238392/2025-03-20/2025-w12/1010/ (accessed on March 20, 2025)

8. Krupanin, F. V bezopasnosti stanovitsya tesno. (In Russian). Available at: https://www.kommersant.ru/doc/7872228 (accessed on: 09.07.2025)

9. Morkovchin, A., Ageeva, E., Musaev, A., Pavlova, I. (2025). Kurs na kiberustoychivost': kak izmenilis' strategii CISO. (In Russian). Available at : // https://jetcsirt.su/upload/%D0%9A%D0%B0%D0%BA%20%D0%B8%D0%B7%D0%BC%D0%B5%D0%BD%D0%B8%D0%BB%D0%B8%D1%81%D1%8C%20%D1%81%D1%82%D1%80%D0%B0%D1%82%D0%B5%D0%B3%D0%B8%D0%B8%20CISO.pdf (accessed on: 11.01.2025)

10. Sizova, N. The demand for cybersecurity specialists is growing by 18% year-on-year. (In Russian). Available at : https://www.vedomosti.ru/technology/articles/2025/06/06/1115445- (accessed on 06.06.2025)

11. Litvinov, R. (2025). V Rossii pochti udvoilos' chislo vakansiy v sfere kiberbezopasnosti. (In Russian). Available at : https://infobezopasnost.ru/blog/news/ (accessed on 06.06.2025)

12. Proekt Postanovleniya Pravitel'stva Rossiyskoy Federatsii «O provedenii eksperimenta po predostavleniyu razrabotchikam programmnogo obespecheniya vozmozhnosti dobrovol'nogo podtverzhdeniya kompetentsiy». (In Russian). Available at : https://regulation.gov.ru/Regulation/Npa/PublicView?npaID=152861 (accessed on 03.12.2024)

13. Pertseva, E. (2025). Na serom fone: vlasti sokrashchayut parallel'nyy import tovarov v RF. (In Russian). Available at : https://iz.ru/1871753/evgeniia-pertceva/ (accessed on 17.04.2025)

14. Parallel'nyj import — potomu chto vsem parallel'no… ili perpendikulyarno. (In Russian). Available at : https://habr.com/ru/companies/x-com/articles/771190/ (accessed on 01.11.2023)

15. Eronin, V. Realizatsiya strategii importozameshcheniya v sfere IB po versii «Krayon». (In Russian). Available at : https://infobezopasnost.ru/blog/articles/ (accessed on 11.09.2024)

16. Khakery posle zapreta zapadnykh sredstv zashchity pytayutsya privlech' spetsialistov RF. (In Russian). Available at : https://tass.ru/ekonomika/22932489 (accessed on January 21, 2025)

17. Import substitution in the field of information security. (In Russian). Available at : https://www.tadviser.ru/index.php/ (accessed on 24.09.2024)

18. Guryanov, S. (2025). Guryanov, S. S KII – bdi: bol'shinstvo kiberatak prikhoditsya na kriticheskuyu infrastrukturu. (In Russian). Available at : https://iz.ru/1822780/sergei-guranov/ (accessed on 17.01.2025)

19. Aryalina, M. (2025). IT-otrasl prorabativaet usloviya vozvrascheniya inostrannih kompanii v Rossiyu. (In Russian). Available at : https://www.vedomosti.ru/technology/articles/2025/04/24/1106343- (accessed on 24.04.2025)

20. Ustinova, A. RFRIT poluchit bole 13 mlrd rublei na granty dlya IT-kompaniy. (In Russian). Available at : https://www.vedomosti.ru/technology/articles/2025/05/13/1109612-rfrit (accessed on May 13, 2025)

Информация об авторах / Information about authors

Симонов Сергей Геннадьевич, доктор социологических наук, кандидат экономических наук, профессор кафедры экономики и организации производства, Тюменский индустриальный университет, г. Тюмень, v.simonova.67@mail.ru

Хаматханова Макка Алаудиновна, кандидат социологических наук, доцент кафедры экономики и организации производства, Тюменский индустриальный университет, г. Тюмень

Лысенко Игорь Вячеславович, кандидат экономических наук, доцент кафедры экономики и организации производства, Тюменский индустриальный университет Россия, г. Тюмень

Sergey G. Simonov, Doctor of Sociology, Candidate of Economics, Professor at the Department of Economics and Organization of Production, Industrial University of Tyumen, v.simonova.67@mail.ru

Makka A. Khamatkhanova, Candidate of Sociology, Associate Professor at the Department of Economics and Organization of Production, Industrial University of Tyumen

Igor V. Lysenko, Candidate of Economics Sciences, Associate Professor at the Department of Economics and Organization of Production, Industrial University of Tyumen, phone: 89129237656, e-mail: liwyaches@bk.ru

Статья поступила в редакцию 07.07.2025; одобрена после рецензирования 22.07.2025; принята к публикации 06.08.2025.
The article was submitted 07.07.2025; approved after reviewing 22.07.2025; accepted for publication 22.08.2025.