



апрель 2025

Рынок NGFW в Российской Федерации 2024-2030

Оглавление

Оглавление..... 2

Введение 3

 Определение сегмента рынка..... 3

 Методика проведения исследования 4

Оценка рынка NGFW по результатам 2024 года..... 5

 Основные участники рынка NGFW в России 5

 Специфика регулирования 7

 Оценка объема рынка по результатам 2024 года 7

 Ключевые факторы влияния на рынок NGFW в РФ в 2024 году 9

 Темпы импортозамещения в 2024 году 11

Прогноз рынка NGFW до 2030 года 12

 Прогноз объема рынка NGFW 12

 Ключевые факторы влияния на рынок NGFW в РФ до 2030 года 12

Выводы 15

Введение

Рынок кибербезопасности России по результатам 2023 года оценивается в 248,5 млрд. рублей¹, рынок средств защиты информации (СЗИ) Российской Федерации в 2023 году составил 182,6 млрд. рублей, при этом на категорию средств защиты сетей (network security) приходилось 64,9 млрд рублей.

Целью настоящего исследования является формирование оценки рынка межсетевых экранов «нового поколения» - Next-Generation Firewall (NGFW) в России и прогноза его развития на перспективу ближайших 5 лет, выявление тенденций развития рынка, а также оценка процессов замещения зарубежных продуктов.

Рынок NGFW существует уже довольно долго и является важной частью экосистемы информационной безопасности и сетевой безопасности в частности. NGFW представляет собой эволюцию традиционных межсетевых экранов, предлагая более продвинутые функции, такие как глубокая инспекция пакетов, контроль приложений, предотвращение вторжений (IPS), а также интеграцию с другими решениями по безопасности. Рынок NGFW является одним из крупных и ключевых сегментов в области сетевой безопасности.

Мировой рынок NGFW в 2022 году оценивается в 8,4 млрд долларов США². Прогнозируется, что к 2032 году этот рынок достигнет 25,6 млрд долларов США, среднегодовой темп прироста рынка составит 12,1%.

\$8,4 млрд

12,1%

объем мирового рынка NGFW в 2022 году и его прогнозируемый темп прироста

Определение сегмента рынка

Рассматривая NGFW-решения и соответствующий сегмент рынка, стоит остановиться на определении классов смежных продуктов сетевой безопасности: FW (Firewall, межсетевой экран), UTM (Unified Threat Management, универсальный шлюз безопасности) и NGFW (Next-Generation Firewall, межсетевой экран нового поколения). Каждый из них относится к сетевой безопасности, но имеет свои особенности и функции.

Исторически, первой линией обороны сетевой инфраструктуры в конце 1980-х – начале 1990-х годов стали классические межсетевые экраны (firewall). В них применялась базовая фильтрация сетевых пакетов, помогавшая контролировать трафик на основе сетевых IP-адресов и портов. По мере эволюции решений в середине 1990-х годов появились механизмы, которые учитывали состояние соединений и позволяли более эффективно фильтровать пакеты и сессии.

В начале 2000-х годов, когда сетевые атаки усложнились, а инфраструктура предприятий становилась всё более разветвленной, появилась необходимость использовать дополнительные инструменты безопасности. Так сформировалась концепция UTM (Unified Threat Management), объединившая в одном устройстве функции межсетевого экрана, антивирусной защиты, антиспам-

¹ Прогноз развития рынка кибербезопасности в Российской Федерации на 2024-2028 годы – октябрь 2024 года – Фонд «ЦСР» – url: <https://www.csr.ru/upload/iblock/f14/bnl532lqmqd0u23s1ftuzw4n3ycm1to1.pdf>

² Next-Gen Firewall Market Outlook 2023 to 2033 – февраль 2023 года – url: <https://www.alliedmarketresearch.com/enterprise-network-firewall-market-A178203>

модуля, веб-фильтрации и VPN-шлюза. Хотя UTM-решения упростили управление безопасностью за счет централизации функций, и остаются популярны среди компаний среднего и малого бизнеса, они часто уступают специализированным решениям по эффективности анализа и производительности.

Развитие веб-приложений и рост доли зашифрованного трафика в начале 2010-х годов потребовали нового уровня контроля и детектирования угроз, выходящих за рамки традиционной фильтрации. Так появились межсетевые экраны нового поколения (Next-Generation Firewall, NGFW), способные определять трафик конкретных приложений, использовать механизмы глубокого анализа (DPI), расшифровывать и анализировать HTTPS-трафик, а также интегрироваться с системами обнаружения вторжений (IDS/IPS) и облачными сервисами Threat Intelligence (TI). Это позволило NGFW-решениям выявлять и блокировать сложные виды атак, распознавая аномальную активность и используя оперативные данные сервисов TI. Виртуализированные версии NGFW обеспечили гибкое развёртывание в облачной среде, став востребованными в среднем бизнесе и на уровне крупных корпоративных сетей и дата-центров.

Таким образом, классические межсетевые экраны прошли путь от фильтрации до глубокого анализа трафика, UTM привнёс идею единого многофункционального решения, а NGFW объединил в себе оба подхода, добавив к ним интеллектуальные механизмы и интеграцию с источниками данных о киберугрозах.

Методика проведения исследования

Исследование проводилось с октября 2024 года по февраль 2025 года на основе анализа открытых источников о выручке разработчиков решений (вендоров), относящихся к категории NGFW, опроса и интервью с представителями ключевых игроков российского рынка NGFW, интеграторов, а также заказчиков (пользователей) продуктов.

Так как границы между UTM- и NGFW-решениями довольно абстрактны и зачастую их отнесение к тем или иным классам является субъективным, в рамках исследования рассматривались как продукты, заявленные производителями как UTM, так и непосредственно NGFW.

В данном исследовании объем рынка оценивался «в деньгах заказчика». При оценке и интерпретации результатов в спорных случаях мы исходили из принципа добросовестности игроков рынка и доверяли предоставленным сведениям.

Результаты исследования структурированы следующим образом:

- Обзор рынка NGFW в период 2021-2024 гг. (состав участников, ключевые факторы развития);
- Оценка рынка NGFW по результатам 2024 года;
- Прогноз развития рынка на 5 лет (2025–2030 гг.);

ЦСР выражает благодарность всем участникам опроса за предоставленные сведения.

Оценка рынка NGFW в России

Основные участники рынка NGFW в России

Геополитические события 2022 года значительно повлияли на российский рынок NGFW-решений - произошел массовый уход западных производителей (вендоров) средств сетевой защиты и сопутствующих решений. При этом процесс ухода зарубежных компаний не был одномоментным и финальным: многие проекты продолжают идти за счет «серых» поставок и поддержки уже развернутых систем усилиями внутренних команд заказчиков. Кроме того, некоторые вендоры (например, Check Point Software Technologies) по-прежнему официально присутствуют на российском рынке или продолжают продажи оборудования российским заказчикам, но без предоставления технической поддержки.

>72 %

объема рынка NGFW в России занимали зарубежные решения в 2021 году

В 2021 году зарубежные решения, по нашей оценке, занимали более 72% рынка NGFW и вплоть до 2022 года отечественные игроки довольствовались нишевыми позициями, связанными с реализацией отдельных функций безопасности, обычно интегрированных в «полноценные» NGFW-решения, или обслуживающими специфические требования государственных регуляторов.

Таблица 1. Основные участники рынка NGFW в России до 2022 года

Вендор	Юрисдикция	Продажи NGFW на рынке РФ		Примечания
		до 2022 г	в 2024 г	
User Gate	РФ	да	да	UserGate NGFW на рынке с 2016 года. Внесен в реестр сертифицированных средств защиты информации ФСТЭК России (Сертификат ФСТЭК России № 3905) и в реестр Российского ПО (№ 1194).
ИнфоТеКС	РФ	да	да	«ViPNet xFirewall 4» на рынке с 2019 года.
Код Безопасности	РФ	да	да	«Континент 4» на рынке с 2019 года.
Фактор-ТС	РФ	да	да	Решения Dionis DPS/NX на рынке с 2020 года. Позиционируется как UTM.
Нума Технологии	РФ	да	да	Продукт Numa Edge на рынке с 2020 года.
Codemaster	РФ	да	да	Продукт Mirada на рынке с 2016 года.
TCC	РФ	да	да	Diamond VPN/FW на рынке с 2016 года. Позиционируется как UTM.
Ideco	РФ	да	да	Межсетевой экран Ideco позиционирован как NGFW в ноябре 2023 года.

Вендор	Юрисдикция	Продажи NGFW на рынке РФ		Примечания
		до 2022 г	в 2024 г	
CheckPoint	Израиль	да	да	Продукты компании доступны в свободной продаже в РФ.
Cisco	США	да	нет	Cisco официально объявила об остановке бизнес-операций в РФ и Республике Беларусь в 2022 году.
PaloAlto	США	да	нет	Продукты продолжают поставляться по схемам параллельного импорта, но официальной поддержки на территории РФ нет.
Fortinet	США	да	нет	Продукты продолжают поставляться по схемам параллельного импорта, но официальной поддержки на территории РФ нет.

К 2024 году состав участников рынка существенно изменился (см. таблицу 2) за счет выхода продуктов ряда отечественных игроков, включая таких крупнейших вендоров, как Positive Technologies, ГК Солар и InfoWatch. Кроме того, о разработке собственных NGFW-решений заявили Лаборатория Касперского, RED Security (ранее MTC RED), ГК Гарда, С-Терра и другие компании.

Таблица 2. Новые участники рынка NGFW в России после 2022 года

Вендор	Юрисдикция	Продажи NGFW на рынке РФ		Примечания
		до 2022 г	в 2024 г	
ГК Солар	РФ	нет	да	Solar NGFW в виртуальном исполнении представлен в апреле 2023 года, а в мае 2024 года - модельный ряд аппаратных платформ средней и высокой производительности. Сертифицирован ФСТЭК России (ИТ.МЭ.Б4.ПЗ). В реестре российского ПО (№25781 от 20.12.2024, №20043 от 27.11.2023)
Positive Technologies	РФ	нет	да	PT NGFW доступен с июня 2024 года. В ноябре 2024 первым среди российских производителей прошел сертификацию ФСТЭК по новым требованиям на «Многофункциональный межсетевой экран уровня сети». ³
Лаборатория Касперского	РФ	нет	нет	«Лаборатория Касперского» представила бета-версию Kaspersky NGFW в июне 2024 года. Официальные продажи начнутся в 2025 году.
InfoWatch	РФ	нет	да	В июне 2024 года запущены первые пилотные проекты продукта InfoWatch ARMA Стена.
MTC RED	РФ	нет	нет	В августе 2024 года продемонстрирован прототип MTC RED NGFW.

³ На момент выхода исследования является единственным продуктом, имеющим данный сертификат.

Вендор	Юрисдикция	Продажи NGFW на рынке РФ		Примечания
		до 2022 г	в 2024 г	
ГК Гарда	РФ	нет	да	Продукт Гарда NGFW анонсирован в январе 2024 года.
С-Терра СиЭсПи	РФ	нет	нет	Продукт анонсирован в 2023 году.

Специфика регулирования

С учетом назревшей необходимости в регулировании сегмента рынка, в июле 2023 года ФСТЭК выпустил «Требования по безопасности информации к многофункциональным межсетевым экранам уровня сети»⁴, ранее утвержденные приказом ФСТЭК России от 7 марта 2023 г. № 44.

Указанный документ предназначен для организаций, осуществляющих в том числе разработку **многофункциональных межсетевых экранов уровня сети (ММСЭ)**, и регламентирует минимально необходимые требования по безопасности информации, предъявляемые к уровню доверия NGFW, управлению доступом, фильтрации сетевого трафика, блокированию атак и вредоносного ПО, централизованному управлению и так далее.

С 14 июня 2023 сертификация многофункциональных межсетевых экранов уровня сети осуществляется в соответствие с указанными требованиями.

В ноябре 2024 года РТ NGFW от Positive Technologies стал первым решением на рынке, сертифицированным по новым требованиям ФСТЭК, и на момент выхода данного исследования остается единственным таковым.

Кроме того, известно о 3-х заявках на сертификацию по новым требованиям от ООО «С-Терра СиЭсПи», ООО «Русплатформа» и ООО «СИС Групп». Также, согласно информации ФСТЭК, пятью организациями проводятся работы по оценке соответствия решений требованиям, среди них: АО «Инфотекс», ООО «Код Безопасности», ООО «Солар Секьюрити», ООО «Юзергейт» и ООО «Айдеко».

Оценка объема рынка по результатам 2024 года

Рынок решений NGFW в Российской Федерации по результатам 2024 года оценивается⁵ в 52,2 млрд рублей, прирост объема рынка по сравнению с 2023 годом составил 30,1%.

₽52,2 млрд

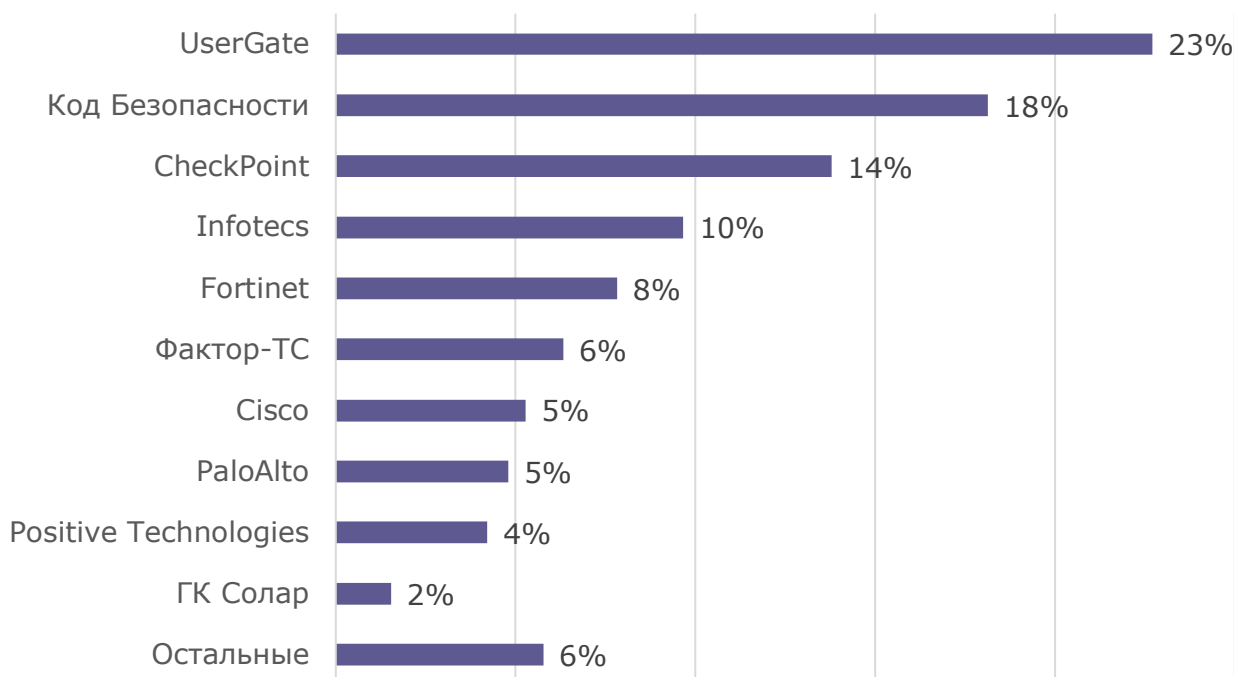
30,1%

объем рынка NGFW России по итогам 2024 года и его прирост относительно 2023 года

К 2024 году распределение долей участников рынка в новых продажах существенно изменилось в пользу отечественных решений. Тем не менее, зарубежные решения всё еще присутствуют и сохраняют серьезные позиции на российском рынке.

⁴ Информационное сообщение ФСТЭК от 19.07.2023 г. № 240/24/3584

⁵ Оценка объема рынка 2024 года носит предварительный характер

Диаграмма 1. Распределение долей участников рынка в 2024 году

При этом доля зарубежных решений составляет весомые 31,6%. Это обусловлено рядом таких факторов, как незрелость отечественных решений в ряде сценариев применения, сложность перехода с одного решения на другое и существенные финансовые затраты на такое переоборудование.

до 31,6 %

сократилась доля продаж зарубежных решений на рынке NGFW России в 2024 году

Во второй половине 2024 года стартовали продажи NGFW-решений от Positive Technologies и ГК Солар, что позволило им сразу занять весомые 4% и 2% рынка соответственно.

Ключевые факторы, влияющие на рынок NGFW в РФ в 2024 году

Активная цифровизация всех аспектов жизни и бизнеса в России, увеличение числа цифровых сервисов и онлайн-услуг приводит к большому количеству потенциальных уязвимостей, росту числа угроз и требует внедрения более надежных средств защиты, отвечающих современным вызовам.

В 2024 году продолжилась интенсивная атака на ИТ-инфраструктуру российских организаций. Эксперты в области информационной безопасности расходятся во мнении относительно динамики роста инцидентов: некоторые отмечают значительное увеличение интенсивности кибератак⁶, другие сообщают об умеренном приросте и сопоставимости значений с предыдущими периодами⁷. Но, несмотря на различие позиций в оценке, все эксперты сходятся во мнении о высокой интенсивности кибератак на российскую ИТ-инфраструктуру и отмечают тенденции к росту их количества. При этом кибератаки качественно меняются с массовых на точечные и хорошо подготовленные. Так или иначе, рост числа, интенсивности и сложности кибератак вызывает стремление организаций усиливать свою защиту, что способствует спросу в том числе на NGFW-решения, являющиеся первым рубежом противодействия злоумышленникам. Таким образом, важным аспектом развития рынка NGFW в России является **высокий уровень киберугроз**.

Стоит отметить, что на российском рынке NGFW до настоящего времени все еще достаточно широко представлены зарубежные решения (в частности, от CheckPoint, Fortinet, PaloAlto, Cisco, Sangfor). Однако, со стороны государства отмечается активная позиция по стимулированию развития отечественных ИТ-продуктов в целом и ИБ в частности. Производителям (разработчикам) продуктов и решений оказывается активная поддержка как экономического плана (гранты, субсидии, налоговые льготы и т.п.), так и нефинансового. Кроме того, регуляторами внедряются требования по импортозамещению, ужесточаются требования в области информационной безопасности и в части применения отечественного программного обеспечения. Таким образом, важными факторами, повлекшими рост рынка NGFW в России в 2024 году, являются: **стимулирование импортозамещения со стороны государства** - требования по импортозамещению, в том числе по локализации производства, требования в области информационной безопасности, в том числе в части применения отечественных продуктов (в частности на объектах критической информационной инфраструктуры), а также **регуляторные требования** - ужесточение законодательства в области кибербезопасности требует от компаний внедрения эффективных решений, в том числе NGFW-решений.

Текущее состояние российского рынка NGFW-продуктов, по мнению экспертов, обусловлено различными сдерживающими факторами. В первую очередь геополитическими событиями, повлекшими наложение на Россию и российские компании беспрецедентного количества санкций. Санкции оказали драматическое влияние и на российский рынок решений NGFW. Они повлекли ограничение не только поставок продуктов, к которым привыкли и которые эксплуатируют по сей день российские потребители (заказчики), но и ограничение поддержки (сопровождения) ранее приобретённых и развернутых потребителями (заказчиками) решений – попытка навязать технологическую изоляцию. Стремительный исход зарубежных поставщиков с российского рынка NGFW-продуктов повлек активное их замещение отечественными. Однако, зачастую, в связи с недостаточно развитым функциональным наполнением отечественных продуктов, недостаточной стабильностью работы, а также с их высокой стоимостью, российские потребители (заказчики) в настоящее время не спешат переходить на российские NGFW-решения.

Крупные потребители (заказчики), у которых была развернута комплексная система сетевой безопасности, неохотно переходят на новые отечественные NGFW-продукты, стремясь сохранить

⁶ Кибератаки на российские компании во II квартале и I полугодии 2024 года -2024 г-ГК Солар url: https://rt-solar.ru/upload/iblock/ea1/c5cpl3rj2d3vzbvw8hsxbxf3644q374d/Kiberataki_na_rossiyskie_kompanii_vo_IIkvartale_iIpolugodii2024-_1_.pdf

⁷ Анализ ландшафта угроз кибербезопасности за 2024 год – 17.12.2024 – Jet CSIRT- url: <https://jetcsirt.su/analytics/analiz-landshafta-ugroz-kiberbezopasnosti-2024/>

работоспособность существующей системы различными способами, т.к. такой переход требует качественной перестройки инфраструктуры и существенных вложений. Кроме того, многие заказчики отмечают несовершенство российских продуктов, и на первых этапах адаптации к новым реалиям рынка заказчики заняли в целом выжидательную позицию. В то же время, у российских потребителей (заказчиков) остается запрос на покрытие потребностей в NGFW-продуктах ушедших зарубежных разработчиков. Такой запрос повлечет развитие схем «серого» импорта зарубежных продуктов, переход на сопровождение систем внутренними командами и т.д.

Российские разработчики, несмотря на активное развитие отечественных продуктов и по объективным причинам, все еще не покрывают запросы потребителей в части функциональности и стабильности в сравнении с зарубежными продуктами.

Таким образом, важными факторами, сдерживающими рост рынка NGFW в России в 2024 году, является аспект **недостаточной зрелости отечественных NGFW решений**, а также **высокая ресурсоемкость проектов внедрения решений** (замещения) в уже развернутых инфраструктурах сетевой безопасности.

Экономические санкции и общая нестабильность вызывают перераспределение и ограничение бюджетов организаций на IT-безопасность в целом, и на решения NGFW в частности, что, в свою очередь, сдерживает рост рынка. Кроме того, расширение бизнеса заказчиков и сопутствующее расширение их инфраструктуры безопасности зачастую осуществляется за счет заемных (привлекаемых) средств. Их высокая стоимость в 2024 году сказывается и на ограничениях бюджетов, в том числе на покупке новых решений, таких как NGFW. Следовательно, к фактору, сдерживающему рост рынка NGFW в России, следует отнести **высокую стоимость заемных средств**.

Темпы импортозамещения по результатам 2024 года

В рамках данного исследования был проведен опрос компаний крупного и среднего бизнеса:

- 76,8 % респондентов отметили, что продолжают использовать зарубежные решения.
- 65% респондентов рассчитывают завершить процесс импортозамещения NGFW-решений в 2025-2026 гг.
- 42% респондентов указали «незрелость отечественных решений» основной причиной отказа от импортозамещения до 2025 года.

Диаграмма 2. Планируете ли менять зарубежные NGFW-решения на отечественные в следующие 5 лет?

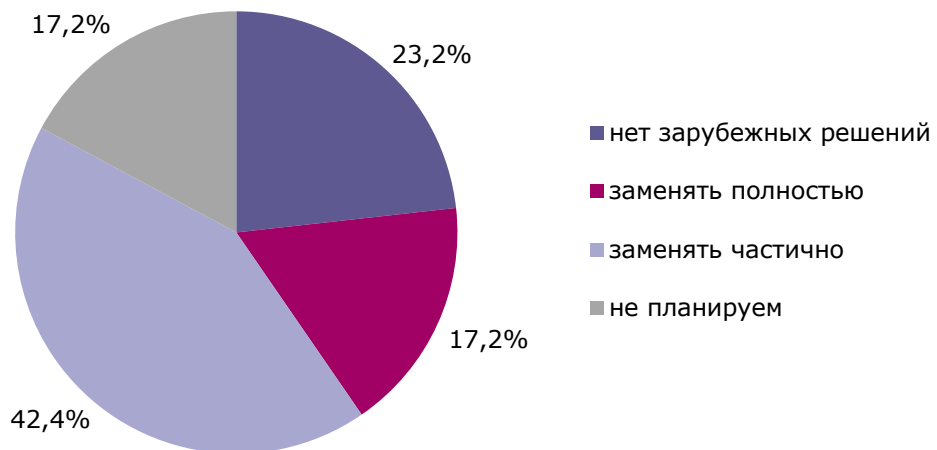
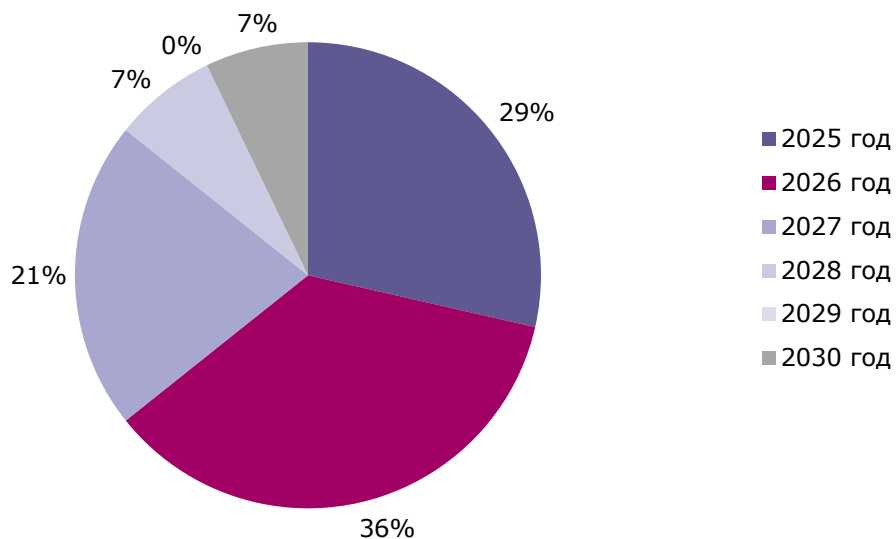


Диаграмма 3. Планируемые сроки окончания импортозамещения



Прогноз рынка NGFW в России до 2030 г

Прогноз объемов рынка

Рынок решений NGFW в Российской Федерации к 2030 году достигнет 146,3 млрд рублей, со средним ежегодным приростом в 18,3%.

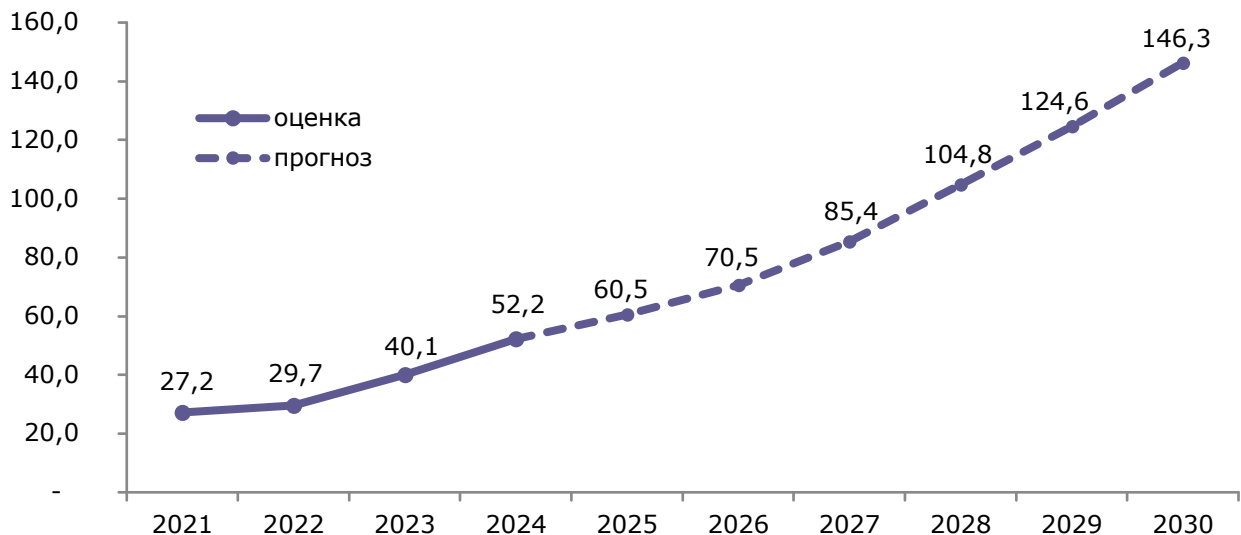
Доля продаж зарубежных решений продолжит сокращаться, достигнув стабилизации в пределах 10-15% к 2030 году.

₽146,3 млрд

18,3%

объем рынка NGFW России к 2030 году и прогнозируемый среднегодовой прирост

Диаграмма 4. Оценка и прогноз объема рынка NGFW, млрд рублей



Ключевые факторы, влияющие на рынок NGFW в РФ до 2030 года

Сохраняющиеся высокие темпы цифровизации в России, рост числа цифровых продуктов, развитие облачных технологий, увеличение числа сотрудников, работающих удаленно (переход на удаленные формы работы) влекут повышение требований к информационной безопасности. При этом **высокие риски киберугроз** (рост интенсивности кибератак, качественного изменения угроз и т.п.) продолжат стимулировать спрос потребителей (заказчиков) на средства сетевой безопасности и рост российского рынка NGFW-решений в прогнозном периоде.

Во всем мире отмечается серьезное влияние на рынок IT-продуктов в целом такого фактора, как стремительный рост объемов обрабатываемых данных: в 2023 году данный показатель оценивается в 120 зеттабайт (ежедневно создается около 330 млн терабайт данных), а уже к 2025 году прогнозируется его увеличение в 1,5 раза, до 181 зеттабайта⁸. Кроме того, в последнее время значительным аспектом воздействия на потребности в области IT-продуктов стала пандемия COVID-

⁸ Объем данных, созданных, потребленных и сохраненных в 2010-2023 гг., с прогнозами до 2028 г. – 21.11.2024 – url: <https://www.statista.com/statistics/871513/worldwide-data-created/>

19, когда вводимые ограничения привели к ускорению перехода на удаленную работу, инструментов мобильности и сохранению этих практик уже после карантинного периода. В связи с вышеперечисленным, у организаций возникает потребность в фильтрации всё больших объемов сетевого трафика (в том числе шифрованного), соответственно к NGFW-продуктам возрастают требования не только в части количества функций, но и в части способности обрабатывать большой поток данных, не теряя при этом в уровне качества защиты. Т.е. к NGFW-продуктам со стороны заказчиков (потребителей) формируется требование **высокой стабильности и производительности**.

На российском рынке, в борьбе за потребителя (заказчика), отмечается высокая конкуренция среди производителей NGFW-продуктов. Заказчики отмечают, что отечественные разработчики активно откликаются на запросы потребителей, дорабатывают свои решения, развивают функционал продуктов, повышается качество сопутствующих сервисов (техническая поддержка и т.п.). Появляются новые участники рынка, представляющие свои продукты и решения в данном сегменте рынка сетевой безопасности. Таким образом, в ближайшей перспективе важным аспектом, стимулирующим рост российского рынка NGFW, будет **повышение зрелости отечественных решений**.

Регуляторные требования в области обеспечения защиты информации и импортозамещения продолжают побуждать государственные компании и государственные корпорации, а также организации, управляющие критической информационной инфраструктурой, замещать зарубежные NGFW продукты в существующей инфраструктуре сетевой защиты. Таким образом, в прогнозном периоде **импортозамещение уже инсталлированных зарубежных NGFW-решений** продолжит оказывать существенное влияние на рост российского рынка NGFW.

Сохранение санкционного давления продолжают оказывать негативное влияние на отечественный рынок NGFW. В ближайшей перспективе ожидается сохранение высокой стоимости заемных средств, что, в свою очередь, продолжит влиять как на ограничение бюджетов у заказчиков (потребителей) на информационную безопасность, так и на производителей программных продуктов. В ближайшей перспективе аспекты **высокой стоимости отечественных решений и высокой стоимости заемных средств** продолжают оказывать сдерживающее влияние на российский рынок NGFW.

Проекты внедрения систем сетевой безопасности требуют от заказчиков системного подхода. Крупные проекты по внедрению NGFW требуют значительных финансовых вложений – на закупку самого оборудования, расходы на лицензии, обучение персонала, интеграцию с существующими системами безопасности и инфраструктурой. В условиях экономической нестабильности и неопределенности, дороговизны заемных средств, компании вынуждены тщательно оценивать свои возможности и готовность к таким инвестициям, зачастую откладывая такие проекты на дальнюю перспективу, при сохранении зарубежных решений в своей инфраструктуре. В итоге, **ресурсоемкость проектов внедрения и миграции** может существенно замедлить рост рынка в России в прогнозируемом периоде.

Выводы

В 2024 году объем рынка NGFW увеличился до **52,2 млрд руб.**, темпы роста составили **30,1%**. Это на 18% выше мировых темпов роста, что связано в первую очередь с резким изменением ландшафта российского рынка.

Доля продаж зарубежных решений сократилась с 72% в 2021 году до **31,6%** в 2024 году.

76,8% компаний продолжают использовать зарубежные решения. Пик импортозамещения еще не пройден и ожидается в 2025-2026 гг.

Незрелость отечественных решений являлась ключевым фактором отказа от импортозамещения в 2022-2024 гг.

За последние два года крупные российские игроки сумели серьезно нарастить потенциал своих решений. Эффект «холодного старта» играет на руку отечественным разработчикам, позволяя сразу внедрять современные решения для современных нужд, минуя необходимость поддерживать устаревшие технологии в своих продуктах.

К концу 2024 года в сегменте рынка насчитывалось более 30 игроков с продуктами различной степени готовности и зрелости. В 2025 году ожидается выход на рынок последнего крупного игрока (Лаборатория Касперского) и фаза активной консолидации предложения, признаки которой наблюдались уже во второй половине 2024 года.

К 2030 году рынок вырастет до 146,3 млрд руб. при CAGR 18,3%, что на 6,2% выше мировых темпов роста данного сегмента.

Авторы



Екатерина Кваша
Заместитель
генерального директора



Владимир Тютрин
Заместитель директора
центра цифрового развития



Выражаем благодарность **Роману Краснову**,
основателю Фонда Цифровых Исследований "КиберПрогноз"
за участие в подготовке данного материала



© 2025 Фонд «Центр стратегических разработок» (ЦСР).
Все права защищены. При использовании информации
из документа ссылка на ЦСР обязательна.

Москва, 125009, Газетный пер., 3–5 стр. 1, 3 этаж
Тел.: +7 (495) 725-78-06
Факс: +7 (495) 725-78-14
E-mail: info@csr.ru

csr.ru

