Май 2026

Рынок информационной безопасности Российской Федерации

текущее состояние и перспективы развития до 2031 года

Оглавление

Ключевые выводы **3**

Методика проведения исследования **5**

Введение **6**

Глобальные тренды рынка информационной безопасности 6

Тренды российского рынка информационной безопасности 8

Оценка российского рынка информационной безопасности **11**

Динамика российского рынка прогноз его развития до 2031 года **19**

Основные факторы, влияющие на динамику рынка до 2031 г. 20

Взгляд ключевых игроков рынка **23**

Авторы **28**

Ключевые выводы

Российский рынок информационной безопасности сохраняет устойчивую положительную динамику, несмотря на макроэкономическое давление и замедление ИТ-рынка в целом. По итогам 2025 года **объем рынка ИБ в России превысил 364 млрд рублей**, увеличившись на **16,1%** год к году. Это выше мировой динамики и темпов роста большинства сегментов российского ИТ-рынка. При сохранении текущих параметров рынок может превысить **1 трлн рублей к 2031 году**, а прогнозируемый среднегодовой темп роста в 2026-2031 годах оценивается на уровне **19,4% CAGR**.

Основу рынка по-прежнему формируют средства защиты информации (СЗИ): в 2025 году на них пришлось около **74%** совокупного объема рынка, тогда как услуги ИБ составили около **26%**. Сегмент СЗИ достиг **271 млрд рублей** и вырос на **18,1%**, однако темпы роста немного замедлились по сравнению с предыдущим периодом. Это отражает не только макроэкономическую ситуацию, но и переход от ускоренного импортозамещения к более системной пересборке ИТ- и ИБ-архитектур. Крупнейшими категориями СЗИ остаются сетевая безопасность, защита инфраструктуры и защита конечных точек; при этом наиболее быстро в 2025 году рос сегмент защиты приложений (application security), что указывает на повышение значимости защиты прикладного контура.

Российские поставщики занимают доминирующее положение: их доля на рынке СЗИ превышает **94%**. Иностранные вендоры представлены в числе крупнейших участников лишь единичными исключениями, а их доля в новых продажах продолжит снижаться. При этом доля установленной базы иностранных решений в инфраструктуре организаций оценивается на уровне **27%.** Это формирует дополнительный потенциал роста для отечественных поставщиков — не только в новых закупках, но и в проектах миграции, замены и сопровождения перехода на российские решения.

Рынок услуг ИБ в 2025 году составил **93,5 млрд рублей** и вырос на **10,7%**. Дефицит специалистов и бюджетные ограничения усиливают спрос на управляемые сервисы (managed services) — MSS, MDR, SOC-as-a-Service и другие модели предоставления услуг защиты. Для многих компаний создание собственной технологически зрелой функции мониторинга и управления ИБ остается слишком дорогостоящим и длительным мероприятием. Управляемые сервисы все чаще воспринимаются не только как способ закрыть кадровый разрыв, но и как инструмент повышения киберустойчивости при оптимизации затрат.

Регуляторика остается одним из главных факторов развития рынка. Усиление требований к ГИС, КИИ, персональным данным, доверенным ПАК, реестровому ПО и использованию ИИ в государственных системах поддерживает спрос на российские решения, сертификацию, аудит, мониторинг, управление доступом и защиту данных. Одновременно импортозамещение крупных ИТ-систем, включая ERP и другие глубоко интегрированные в ИТ-инфраструктуру бизнес-платформы, становится новым вызовом для ИБ-команд: такие проекты меняют архитектуру, модели доступа и потоки данных, повышая риск конфигурационных ошибок, появление избыточных привилегий и новых технических уязвимостей.

Российские организации все чаще рассматривают ИБ не только как набор технических мер или инструмент соответствия требованиям, а как элемент операционной устойчивости бизнеса — способность противостоять атакам, сохранять непрерывность процессов, быстро восстанавливаться и снижать финансовый ущерб компании. Дальнейшая динамика рынка будет определяться не только импортозамещением, но и развитием новых технологических контуров: облачных и гибридных сред, защиты ИИ-сценариев и конфиденциальной обработки данных, автономного SOC и доверенных ПАК.

В долгосрочной перспективе российский рынок ИБ будет развиваться за счет сочетания внутреннего спроса, регуляторных требований, технологического суверенитета, сервисных моделей и усложнения цифровой инфраструктуры. При этом в ближайшие три года рынок будет переживать фазу глубокой

технологической трансформации, связанной с распространением искусственного интеллекта. ИИ меняет не только бизнес-процессы, но и ИТ-архитектуру, модели разработки ПО, эксплуатации и управления данными, что требует переосмысления подходов к защите информации. Привычные классы ИБ-решений и практики, формировавшиеся на протяжении десятилетий, все чаще будут сталкиваться с ограничениями в новых технологических контурах.

В этих условиях конкурентное преимущество получат вендоры, способные первыми предложить не точечные доработки существующих продуктов, а новые архитектуры и классы решений для обеспечения безопасности бизнеса в ходе ИИ-трансформации — включая специализированные решения для защиты ИИ-систем и ИИ-агентов, современные платформы безопасности данных, системы управления экспозицией рисков и учетными данными, интеллектуальную защиту конечных узлов, а также новые подходы к сетевой безопасности в условиях гибридных инфраструктур.

Методика проведения исследования

Исследование проводилось с февраля по май 2026 года на основе анализа открытых источников о выручке разработчиков решений (производителей средств защиты, вендоров) информационной безопасности для бизнеса (корпоративный сегмент, B2B), анализа конкурсных закупок на различных площадках, опросов и интервью с представителями ключевых игроков российского сегмента рынка.

Для целей исследования рынок корпоративных средств защиты информации (СЗИ) в России структурирован по укрупненным функциональным категориям решений. Предложенная группировка позволяет, с одной стороны, отразить специфику российского рынка, а с другой — сохранить сопоставимость с международной аналитической практикой и обеспечить по необходимости возможность сравнения российской динамики с мировым рынком информационной безопасности.

В рамках исследования выделены следующие крупные категории ИБ-решений[1]:

- **средства сетевой безопасности** *(network security);*
- **средства защиты конечных точек** *(endpoint security);*
- **средства защиты инфраструктуры** *(infrastructure security);*
- **средства защиты приложений** *(application security);*
- **средства защиты данных** *(data security);*
- **средства управления доступом** *(access management).*

В исследовании представлена информация о наиболее заметных игроках российского рынка средств защиты информации, продукты которых внесены в Реестр российского ПО, предназначены для широкого коммерческого распространения и имеют признаки коммерческих внедрений. Основной акцент в исследовании сделан на рынке СЗИ, рынок услуг рассматривается укрупненно.

Объем рынка оценивался *«в деньгах заказчика»* и включает затраты конечных пользователей на средства защиты информации и связанные с ними услуги, в том числе накладные расходы, связанные с дистрибуцией решений. При оценке и интерпретации результатов в спорных случаях рабочая группа авторов исследования исходила из принципа добросовестности участников рынка и доверяла предоставленным сведениям.

ЦСР выражает благодарность всем участникам опроса за предоставленные сведения и конструктивную обратную связь.

[1] *Детализация приведенной таксономии приведена в* ***Приложении 1****.*

Введение

Глобальные тренды рынка информационной безопасности

Информационная безопасность остается одним из наиболее устойчивых сегментов мирового ИТ-рынка и продолжает расти двузначными темпами. В 2025 году расходы конечных заказчиков на информационную безопасность, по данным Gartner, оценивались[2] примерно в 213 млрд долларов против 193 млрд долларов годом ранее (+10,4%), а в 2026 году ожидается их рост до 240 млрд долларов (+12,7%). Сопоставимую картину, с учетом различий в методиках, дают и другие оценки: так, например, компания IDC указывает[3] на рост мировых расходов на безопасность на 12,2% в 2025 году, а компания Forrester — на 13,1%, с перспективой преодоления отметки в 300 млрд долларов уже к 2029 году.[4]

Мировой рынок: $213 млрд, +10,4%

Объем мирового рынка информационной безопасности и его прирост в 2025 г.

Облачная трансформация является одним из ключевых драйверов роста мирового рынка ИБ. Глобальный ИТ-рынок продолжает развиваться с опорой на облачную инфраструктуру и облачные сервисы (SaaS, IaaS, PaaS и др.), которые становятся базой для модернизации бизнес-приложений, внедрения искусственного интеллекта (ИИ) и масштабирования цифровых услуг. По некоторым оценкам, мировые расходы на публичные облачные сервисы в 2026 году превысят 1 трлн долларов, увеличившись более чем на 21% год к году[5] — всё это непосредственным образом влечет за собой увеличение сопутствующих расходов на информационную безопасность.

Перенос инфраструктуры и приложений из локальных сред в облачные и гибридные архитектуры расширяет поверхность возможной атаки и усиливает потребность в новых специализированных инструментах защиты. На этом фоне расходы на программное обеспечение для информационной безопасности (security software) растут быстрее (+11,6%), чем расходы на сетевое оборудование для безопасности (+9,2%) и сервисы (+10,7%). Внутри мирового сегмента ПО для информационной безопасности спрос поддерживается прежде всего разнообразными предложениями по управлению облачной безопасностью, включая CNAPP/CSPM- и CASB-решения.

Кроме того, взрывное распространение генеративного ИИ (GenAI) в мире в последние несколько лет, действует как сквозной фактор роста для индустрии. Организации вынуждены активнее защищать как растущее количество бизнес-сценариев, использующих ИИ, так и растущую ИИ-инфраструктуру. При этом аналогичные ИИ-технологии с успехом эксплуатируются и злоумышленниками. Всё это повышает интерес компаний к современным решениям по управлению уязвимостями, экспозицией рисков (exposure management) и сервисам непрерывного мониторинга безопасности, расследования и реагирования, в том числе и с применением ИИ.

---

[2] *Gartner Forecasts Worldwide End-User Spending, Gartner, 2025*
[3] *Worldwide Security Spending Guide, IDC, 2025*
[4] *Global Cybersecurity Market Forecast 2024 To 2029, Forrester, 2025*
[5] *Global Public Cloud Spending, IDC, 2026*

Распространение прикладных сценариев использования генеративного ИИ становится сквозным фактором роста мирового рынка кибербезопасности.

Важно отметить, что ИИ-технологии сегодня не воспринимаются рынком как «надстройка» над отдельными функциями продуктов информационной безопасности. Спрос формируется уже вокруг конкретных сценариев применения ИИ в процессах обеспечения информационной безопасности с измеримым эффектом: ускорение триажа, обогащение событий ИБ и повышению качества их корреляции, подготовка аналитики, поиск уязвимостей и поддержка расследований. Но одновременно, или даже в первую очередь, технологии ИИ становится частью атакующего инструментария, снижая порог входа в социальную инженерию, ускоряя подготовку фишинговых кампаний, анализ кода, поиск и эксплуатацию уязвимостей в нём.

Таким образом, необходимость защищать не только традиционную ИТ-инфраструктуру, но и растущий ИИ-контур — RAG-системы, ИИ-агентов, обучающие и эксплуатационные данные, секреты и связанные с ИИ цепочки поставок — всё это приводит к необходимости менять подходы к защите активов, данных и контролю доступов.

В контексте защиты данных спрос постепенно смещается от DLP-решений, ориентированных на предотвращение отдельных каналов утечки данных, к DSPM- и современным DSP-платформам, где ключевыми становятся обнаружение и классификация чувствительных данных, оценка их экспозиции, маскирование и непрерывный анализ доступов в облачных, гибридных и ИИ-средах. В результате на рынке формируется запрос на интегрированный контур защиты, объединяющий анализ и управление доступом к данным, политики использования данных и предотвращение утечек. Этот спрос подстегивается кратным ростом машинных учетных записей (идентичностей) в инфраструктуре организаций: сервисных аккаунтов, API-ключей, токенов, сертификатов, секретов и временных привилегий, не связанных напрямую с конкретными сотрудниками организации. По данным некоторых исследований, в 2025 году в организациях в среднем приходилось 82 машинные идентичности на одну человеческую; при этом 42% из них имели чувствительный или привилегированный доступ к данным.[6] В то же время, только 44% машинных идентичностей оказались под контролем соответствующих IAM-команд в подразделениях организаций.[7]

Современная архитектура безопасности формирует спрос на DSP-решения, объединяющие контроль обработки чувствительных данных и непрерывный анализ доступа к ним для предотвращения утечек.

Параллельно меняется подход к управления уязвимостями. Классическая итеративная концепция, сосредоточенная на выявлении брешей, оценке их критичности и контроле в процессе устранения, все хуже отвечают масштабу и динамике современных ИТ-сред. В быстро меняющихся облачных, гибридных и ИИ-ориентированных архитектурах заказчикам важно понимать не только наличие уязвимости, но и реальную экспозицию риска: доступность актива извне, наличие атакующих инструментов (эксплойтов) в публичном пространстве, связь актива с критичными бизнес-системами, привилегиями, конфигурационными ошибками и возможными путями развития атаки. Поэтому спрос на рынке смещается от управления уязвимостями в узком смысле к управлению экспозицией рисков (exposure assessment and management) — более широкому подходу по управлению ИБ-рисками, который объединяет данные об активах, уязвимостях, конфигурациях, идентичностях и угрозах для приоритизации исправления или изоляции тех дефектов системы, которые действительно повышают вероятность успешной атаки.

[6] *Machine Identities Outnumber Humans, CyberArk, 2025*
[7] *Top Cybersecurity Trends for 2025, Gartner, 2025*

Рынок консолидирует задачи смежных классов решений по управлению уязвимостями в единый подход по управлению экспозицией рисков для нейтрализации реальных угроз.

На фоне усложнения ИТ-ландшафта заказчики все чаще переходят от экстенсивного расширения набора средств защиты к оптимизации технологического стека. При общем количестве поставщиков ИБ-решений, превышающем 3 тыс. производителей в мире, крупные организации[7] в среднем используют 45 различных инструментов кибербезопасности. Это усиливает фрагментацию защитного контура, усложняет интеграцию и повышает операционные издержки. Вследствие этого на рынке растет спрос на консолидацию базовых контролей, устранение функционального дублирования и расширение интеграционных возможностей решений, в том числе кросс-вендорных: открытые API, переносимость телеметрии, совместимость с различными верхнеуровневыми системами, например, SIEM/SOAR/XDR и так далее. Такой сдвиг поддерживает развитие как платформенных, нативно-интегрированных решений, так и сервисных моделей ИБ, позволяющих заказчикам снижать сложность эксплуатации защитного контура.

Стоит также отметить, что усиление регулирования, ранее выступавшее значимым драйвером спроса преимущественно в отдельных юрисдикциях, также становится общеотраслевой мировой тенденцией. Ведущие экономики рассматривают кибербезопасность как обязательный элемент операционной устойчивости, управления рисками, защиты цепочек поставок и безопасности цифровых сервисов. Это формирует устойчивый спрос на GRC, управляемые сервисы непрерывного мониторинга, реагирование на инциденты, аудит защищенности и практическое управление киберрисками.

Тренды российского рынка информационной безопасности

Уход иностранных производителей стал для российского рынка ИБ катализатором появления и ускоренного развития большого числа отечественных решений. В 2022–2024 годах этот процесс сопровождался стремлением заказчиков быстрее закрыть реальные и потенциальные разрывы в защитном контуре и заменить отдельные зарубежные продукты российскими аналогами — прежде всего в сегментах с высокой зависимостью от внешних поставщиков, например, в сетевой безопасности. Однако к 2025 году подход стал заметно более прагматичным: формальное российское происхождение продукта или его наличие в реестре уже не является достаточным аргументом для выбора. Заказчики значительно тщательнее оценивают решения по функциональности, надежности, производительности, масштабируемости, эффективности от внедрения, качеству поддержки и способности гибко интегрироваться в уже сложившуюся архитектуру защиты.

Одновременно с этим меняется понимание результата, которого российские заказчики ожидают от ИБ. Если раньше акцент делался на минимизации технических рисков, внедрении защиты от отдельных угроз или выполнении формальных требований, то теперь все большее значение для бизнеса приобретает *«киберустойчивость»* — способность организации противостоять атакам, сохранять непрерывность ключевых процессов, быстро восстанавливаться и снижать финансовый ущерб от киберинцидентов. Этот сдвиг уже заметен в крупных отраслях, где на первый план сегодня выходит практическая готовность к реальным кризисным сценариям. Так, согласно распоряжению Правительства Российской Федерации № 373-р «Об утверждении стратегического направления в области цифровой трансформации топливно-энергетического комплекса до 2036 г.»[8], уже в ближайшие 5 лет 100 компаний топливно-энергетического комплекса должны принять участие в кибериспытаниях, а к 2036 году их количество должно составить 500.

Регуляторная повестка традиционно является для отечественного рынка ИБ одним из ключевых факторов изменений. Так, например, приказ ФСТЭК России №117 от 11 апреля 2025 (вступил в силу с 1 марта 2026 года) существенно усиливает[9] требования к защите информации в государственных и

[8] *Распоряжение Правительства Российской Федерации от 26 февраля 2026 г. № 373-р. Правительство РФ, 2026*
[9] *Приказ Федеральной службы по техническому и экспортному контролю от 11.04.2025 № 117, ФСТЭК, 2025*

критически значимых системах. При этом документ расширяет и ужесточает требования к информационной безопасности, охватывая не только государственные структуры, но и все системы, взаимодействующие с ГИС, включая муниципальные службы, банки и финансовые ИТ- инфраструктуры.

Важные для рынка регуляторные изменения уже сегодня включают в себя запрет обработки данных критической значимости в публичных облаках (при несоблюдении соответствующих требований ФСТЭК), требование применения исключительно сертифицированных средств защиты, а также ответственность владельцев систем за безопасность данных, в том числе при их передаче третьим лицам. Нарушение этих требований может привести к приостановке или полному запрету эксплуатации систем, что в теории влечёт за собой серьёзные операционные, репутационные и юридические риски. В этой ситуации функции информационной безопасности, связанные с прозрачностью обработки и доступа к чувствительным данным становятся критически важными для бизнеса.

Ускоренное замещение критичных ИТ-систем новыми, менее зрелыми решениями повышает требования к их защите и превращает кибербезопасность в элемент управления операционной устойчивостью бизнеса.

Следует отметить, что регуляторное давление не только повышает спрос на российские решения, но и увеличивает нагрузку на команды безопасности. Государственная политика предполагает переход 80% компаний ключевых отраслей на отечественное ПО к 2030 году[10], а для большинства объектов КИИ устанавливается более близкий горизонт перехода на отечественное ПО и ПАК — до 1 января 2028 года, с возможностью продления для отдельных организаций до 1 декабря 2030 года. Дополнительное значение здесь имеет утверждение перечней[11] типовых отраслевых объектов КИИ: в них включаются, в частности, ERP-системы, используемые в химической, металлургической, горнодобывающей, ракетно-космической, оборонной и других отраслях. Это означает, что данный этап импортозамещения нацелен не только на отдельные прикладные продукты, но и на крупные, глубоко интегрированные ИТ-системы, от которых зависит непрерывность ключевых бизнес- и производственных процессов. По информации, опубликованной в ноябре 2025 года, Минцифры рассматривает[12] возможность введения ежегодных оборотных штрафов для компаний, которые не проведут классификацию значимых объектов КИИ и не обеспечат их перевод на отечественное ПО в установленные сроки. Штрафы предполагается применять как за отсутствие самой классификации, так и за несвоевременный переход на решения из реестра.

Для ИБ-команд такая миграция в рамках ИТ-ландшафта становится самостоятельным вызовом. Замена крупных ИТ-систем меняет архитектуру инфраструктуры, логику интеграций, моделей доступа, потоков данных и контуров ответственности между организацией и её партнерами. При сжатых сроках перехода и высокой сложности внедрений возрастает риск конфигурационных ошибок, делегирования избыточных прав доступа, неучтенных интеграций, уязвимостей в новых компонентах и недостаточно зрелых процессах эксплуатации. Очевидно, что часть российских решений и компонентов пока не обладает таким же объемом накопленной промышленной эксплуатации, как зрелые зарубежные системы, что повышает требования к более тщательному тестированию, аудиту, мониторингу и сопровождению с точки зрения ИБ. Поэтому оперативное импортозамещение крупных ИТ-систем одновременно становится драйвером рынка ИБ и источником новых задач по управлению рисками, уязвимостями и киберустойчивостью.

---

[10] Заявление Михаила Мишустина о переходе на российское ПО, ЦИПР, 2024
[11] Распоряжение Правительства РФ от 26 февраля 2026 г. № 360-р, 2026
[12] «Минцифры предложило оборотные штрафы за просрочку перевода значимых объектов КИИ…», Интерфакс, 2025

Дефицит компетенций и давление на бюджеты усиливают спрос на управляемые сервисы и платформенные модели, позволяющие быстрее закрывать ключевые функции защиты.

На этом фоне кадровый дефицит и бюджетные ограничения усиливают спрос на сервисные модели обеспечения ИБ. В 2025 году кадровые проблемы в сфере ИБ испытывали 80% российских компаний[13], а доля организаций с нехваткой более чем 10 ИБ-специалистов за три года выросла с 17% до 32%. Для значительной части организаций, особенно малого и среднего бизнеса, самостоятельное построение технологически зрелого SOC и связанных с ним процессов, включая круглосуточный мониторинг и реагирование, оказывается слишком дорогим и длительным проектом. Это ведет к органическому росту управляемых сервисов безопасности — MSSP, SOC-as-a-Service, MDR и других видов услуг. По различным оценкам[14, 15], отдельные сегменты российского рынка управляемых сервисов безопасности растут на 20–30% в год, опережая в среднем общий рост рынка.

В контексте необходимых шагов по ускоренному импортозамещению ИТ-систем, глобальный тренд на «платформизацию» ИБ-решений приобретает в России отличительные черты, когда к задачам унификации и сокращения количества ИБ-инструментов добавляется необходимость быстрого покрытия обновленного ИТ-ландшафта организации, с учетом специфики новых отечественных систем, возможностей локальных инфраструктурных и сервисных провайдеров.

В отличие от глобального рынка, где облачная трансформация бизнеса давно стала одним из ключевых направлений развития ИТ и фактором быстрорастущего спроса на облачные ИБ-решения, в России проникновение облачных технологий в бизнес пока остается ниже уровня развитых рынков. По оценке Apple Hills Digital и Yandex B2B Tech, российский рынок облачного ПО отстает от развитых рынков по темпам развития примерно на 5–7 лет. При этом ожидается, что этот сегмент будет расти быстрее ИТ-рынка в целом — около 22% CAGR.[16] Это означает, что спрос на облачную информационную безопасность в России будет усиливаться, но развиваться преимущественно в логике перехода к гибридным архитектурам.

Развитие ИИ и гибридных сред формирует новый контур рисков, связанных с защитой данных, моделей, доступов и облачной инфраструктуры.

С облачной инфраструктурой тесно связана и тема искусственного интеллекта, который становится для мирового и российского рынка ИБ не только инструментом автоматизации, но и самостоятельным объектом защиты и регулирования. Упомянутый ранее приказ ФСТЭК России №117, прямо закрепляет требования к использованию ИИ в государственных информационных системах: контроль запросов и ответов, выявление недостоверных результатов, ограничение нерегламентированного влияния ИИ на работу систем и запрет передачи информации ограниченного доступа разработчику модели для ее дообучения. Параллельно в 2025 году обсуждался стандарт безопасной разработки ИИ-систем, учитывающий специфические риски машинного обучения, а постановление Правительства РФ №2001 от 9 декабря 2025 года[17] ввело специальные требования к ПАК для генеративных моделей при включении в реестр российского ПО. В результате безопасность ИИ в России постепенно оформляется как отдельный регулируемый контур — с требованиями к данным, моделям, инфраструктуре, доверенности компонентов и подтверждению соответствия.

---

[13] *80% российских компаний столкнулись с дефицитом кадров в 2025 году, Инфосистемы Джет, 2026*
[14] *Российский рынок сервисов безопасности "по подписке" может удвоиться к 2028 г., ComNews.ru, 2025*
[15] *Рынок SOC в 2025 году вырос на треть, VolgaBlob, 2026*
[16] *The view of software, AHD, Yandex B2B Tech, 2026*
[17] *Постановление Правительства Российской Федерации от 09.12.2025 № 2001, Правительство РФ, 2025*

Оценка российского рынка информационной безопасности

В 2025 году объем российского рынка информационной безопасности превысил 364 млрд рублей, показав рост на 16,1% год к году — выше среднемировой динамики рынка ИБ и темпов роста большинства сегментов российского ИТ-рынка.

> 364,4 млрд рублей

Объем российского рынка информационной безопасности в 2025 году

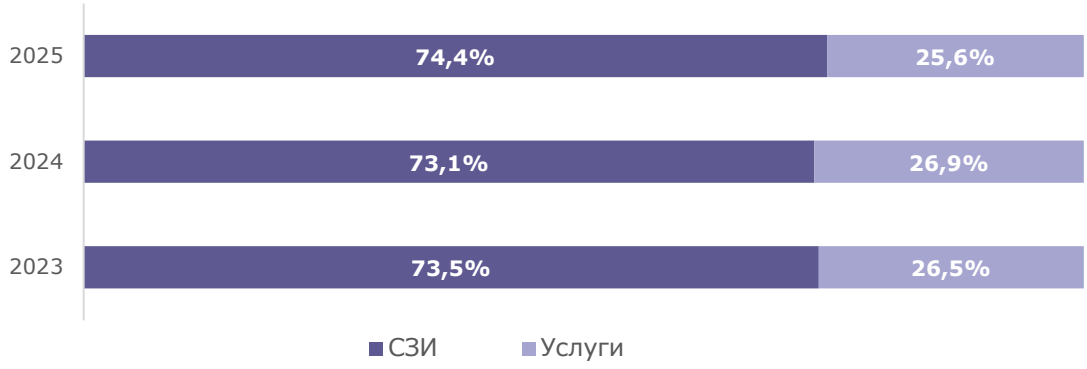
+ 16,1%

Прирост объема российского рынка информационной безопасности в 2025 году

Даже с учетом ожидавшейся ранее коррекции[18], связанной прежде всего с макроэкономической ситуацией, рынок информационной безопасности сохраняет высокую динамику и продолжает расти быстрее отечественного ИТ-рынка, для которого прогнозы и оценки по итогам 2025 год, варьируются от стагнационных сценариев до широкого диапазона в 3-14% роста.[19,20,21,22]

Соотношение поставок СЗИ и услуг, связанных с обеспечением информационной безопасности, остается стабильным на протяжении последних трех лет: около 74% рынка приходится на средства защиты информации, еще около 26% — на услуги.

Рис. 1. Доля поставок средств защиты информации и услуг (сервисов) ИБ в объеме рынка, %



[18] *Прогноз развития рынка кибербезопасности в Российской Федерации на 2025-2030 годы, ЦСР, 2025*
[19] *ИТ-Рынок в России 2025-2026, Т1, 2025*
[20] *Рост российского IT-рынка в 2025 году может замедлиться, Коммерсант, 2025*
[21] *Совокупная выручка российских ИТ-компаний впервые за несколько лет снизилась, Коммерсант, 2026*
[22] *Российский IT-сектор получил почти 1,7 трлн рублей прибыли в 2025 году, ТАСС, 2026*

Рис. 2. Доли российских и зарубежных вендоров средств защиты информации, %

В 2025 году сохраняется тенденция к снижению доли зарубежных вендоров и доминированию российских поставщиков: их доля уже превышает 94%. Совокупные затраты организаций на иностранные ИБ-решения по итогам года составили менее 6% общей емкости рынка СЗИ. При этом остаточный спрос на зарубежные решения сохраняется за счет официального присутствия отдельных иностранных вендоров, поставок по каналам параллельного импорта (даже с учетом повышения затрат на приобретение решений и услуг технической поддержки) и наличия ниш, где полноценная замена на отечественные аналоги пока затруднена, прежде всего в отдельных категориях сетевого оборудования, включая многофункциональные межсетевые экраны.

Лидерами рынка, с заметным отрывом от остальных участников, остаются «Лаборатория Касперского» и Positive Technologies. К крупнейшим игрокам российского рынка кибербезопасности также относятся ГК «Солар» и BI.ZONE, в значительной степени фокусирующиеся на предоставлении сервисов ИБ, а также производители средств сетевой безопасности — «ИнфоТеКС», «Код Безопасности» и UserGate.

Лидеры рынка кибербезопасности РФ, 2025 год[23]

1	**Лаборатория Касперского**	11	**Infowatch**	21	**Киберпротект**
2	**Positive Technologies**	12	**F6**	22	**Атлас-карт**
3	**ГК Солар**	13	**Security Vision**	23	**WMX**
4	**BI.ZONE**	14	**Фактор-ТС**	24	**Cisco**
5	**ИнфоТеКС**	15	**Гарда Технологии**	25	**Аладдин Р.Д.**
6	**Код Безопасности**	16	**Актив-Софт**	26	**IDECO**
7	**UserGate**	17	**R-Vision**	27	**Индид**
8	**Check Point**	18	**Амикон**	28	**АйТи Бастион**
9	**Search Inform**	19	**S-Terra**	29	**DrWeb**
10	**Крипто-Про**	20	**Qrator Labs**	30	**Swordfish Security**

[23] *Среди производителей СЗИ*

По результатам 2025 года иностранные производители, ранее занимавшие высокие позиции на российском рынке, включая Fortinet, Palo Alto Networks и других, представлены в числе 30 крупнейших участников лишь единичными исключениями. Израильская Check Point сохраняет официальное присутствие в РФ и продолжает занимать довольно крупную долю в отдельных сегментах рынка. Cisco, несмотря на уход с российского рынка, также остается в числе заметных игроков за счет сохраняющегося спроса на оборудование и поставок по каналам параллельного импорта.

Оценка сегмента СЗИ по результатам 2025 года

Сегмент средств защиты информации (СЗИ) в 2025 году продолжил активно расти, достигнув объема в 271 млрд рублей с совокупным приростом к 2024 году в 18,1%.

271 млрд руб. **+18,1%**

Объем российского рынка СЗИ по итогам 2025 года и его прирост

В сегменте СЗИ общее лидерство сохраняет «Лаборатория Касперского», демонстрируя стабильное увеличение доли рынка (+0,5 п.п. год к году). При этом наиболее заметное усиление позиций по результатам 2025 года показывает Positive Technologies: доля компании в рынке средств защиты информации выросла на 3,2 п.п. год к году.

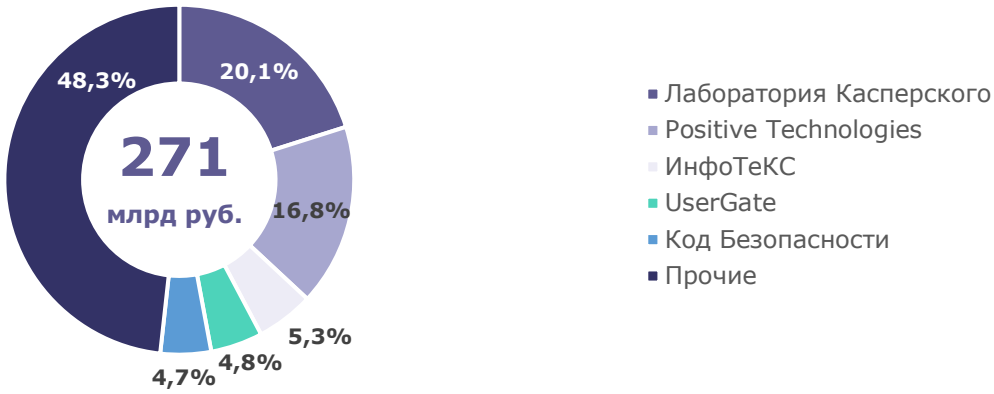
Таблица 1. Топ-5 производителей по выручке от продаж СЗИ в 2025 году

Позиция	Вендор	Юрисдикция	Рост год к году (YoY)[24]
1	Лаборатория Касперского	РФ	21%
2	Positive Technologies	РФ	46%
3	ИнфоТеКС	РФ	7%
4	UserGate	РФ	17%
5	Код Безопасности	РФ	8%

Большинство лидеров рынка сохраняют высокие темпы роста. У ряда крупных игроков, наблюдается замедление, связанное прежде всего со спецификой клиентского портфеля, сдвигом проектов внедрения и более осторожной инвестиционной активностью в отдельных отраслях в течении 2025 года. Пятерка лидеров рынка СЗИ представлена исключительно российскими компаниями. Тем не менее, продажи единственного зарубежного вендора среди 10 крупнейших участников рынка — израильской Check Point — оцениваются как стабильно высокие, несмотря на заметно возросшую конкуренцию со стороны отечественных компаний.

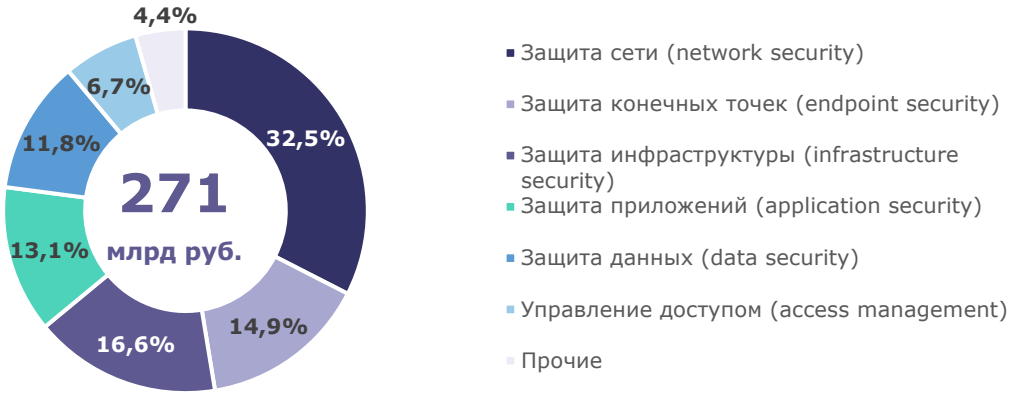
[24] *Рост выручки от продаж средств защиты информации в 2025 году без учета услуг*

Рис. 3. Доли рынка ключевых производителей СЗИ в 2025 году[25], %



Рынок средств защиты информации вырос до 271 млрд рублей, однако темпы роста замедлились с 25,5% до 18%. Это отражает переход от ускоренного закрытия разрывов после ухода иностранных поставщиков к более системной пересборке ИБ-архитектуры на фоне макроэкономического давления, осторожности заказчиков в инвестициях и общего замедления проектной активности на ИТ-рынке.

Рис. 4. Долевое распределение продаж различных категорий СЗИ в 2025 году, %



Крупнейшими сегментами по объему рынка остаются сетевая безопасность (32,5%), защита инфраструктуры (16,6%) и защита конечных точек (14,9%). При этом наибольший рост относительно предыдущего периода показал сегмент защиты приложений (+45% YoY).

[25] *Оценка рынка в исследовании приведена в деньгах конечного заказчика, согласно принятой методологии*

Таблица 2. Декомпозиция объемов рынка по категориям СЗИ

Категория СЗИ	Доля категории в рынке (%)	Объем категории (млрд руб.)	Прирост за 2025 год (%)
Средства защиты сетей (network security)	32,5%	88,13 ₽	7,3%
Средства защиты «конечных точек» (endpoint security)	14,9%	40,32 ₽	15,6%
Средства защиты инфраструктуры (infrastructure security)	16,6%	45,00 ₽	14,0%
Средства защиты приложений (application security)	13,1%	35,42 ₽	45,6%
Средства защиты данных (data security)	11,8%	32,04 ₽	7,4%
Средства управления доступом (access management)	6,7%	18,06 ₽	21,0%

Структура рынка по категориям СЗИ в целом остается устойчивой на протяжении трехлетнего периода.

Рис. 5. Распределение долей продаж по категориям СЗИ, в 2023-2025 годах, %

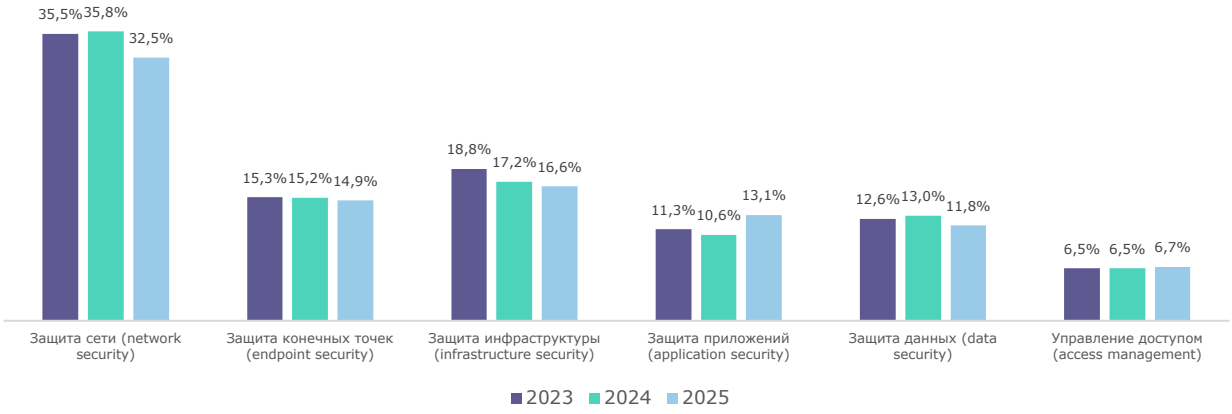


Таблица 3. Топ-5 вендоров в разрезе категорий средств защиты информации по итогам 2025 года

Позиция	Вендор/Сегмент	Юрисдикция
	Средства защиты сетей (network security)	
1	UserGate	РФ
2	Positive Technologies	РФ
3	Код Безопасности	РФ
4	ИнфоТеКС	РФ
5	Check Point	Израиль
	Средства защиты «конечных точек» (endpoint security)	
1	Лаборатория Касперского	РФ
2	DrWeb	РФ
3	Positive Technologies	РФ
4	Код Безопасности	РФ
5	ИнфоТеКС	РФ
	Средства защиты инфраструктуры (infrastructure security)	
1	Positive Technologies	РФ
2	Лаборатория Касперского	РФ
3	Security Vision	РФ
4	R-Vision	РФ
5	F6	РФ
	Средства защиты приложений (application security)	
1	Positive Technologies	РФ
2	ГК Солар	РФ
3	Qrator Labs	РФ
4	BI.ZONE	РФ
5	WMX	РФ
	Средства защиты данных (data security)	
1	Infowatch	РФ
2	ГК Солар	РФ
3	ИнфоТеКС	РФ
4	Гарда Технологии	РФ
5	Search Inform	РФ
	Средства управления доступом (access management)	
1	Актив-Софт	РФ
2	Крипто-Про	РФ
3	Индид	РФ
4	АйТи Бастион	РФ
5	Avanpost	РФ

Оценка рынка услуг по результатам 2025 года

Объем рынка услуг в области информационной безопасности по итогам 2025 года составил 93,5 млрд рублей, увеличившись на 10,7% год к году. По сравнению с предыдущим годом, динамика заметно снизилась. Это отражает влияние макроэкономических условий: на фоне бюджетных ограничений и повышенной неопределенности организации осторожнее подходят к запуску новых инициатив и откладывают инвестиции в крупные проекты по проектированию, внедрению и развитию инфраструктур.

93,5 млрд руб. **+10,7%**

Объем российского рынка ИБ-услуг по итогам 2025 года и его годовой прирост

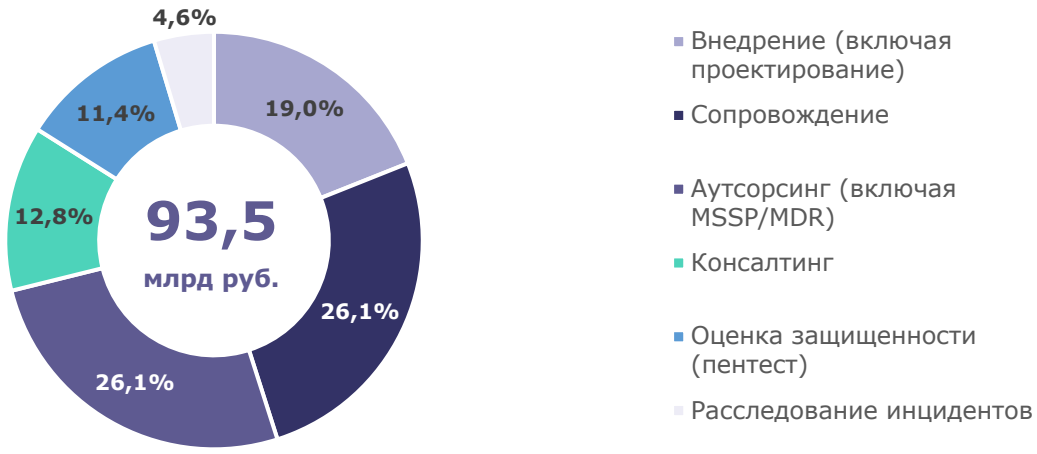
В отличие от сегмента СЗИ, в сегменте услуг ИБ важны не только объем и уровень диверсификации собственного продуктового портфеля, но и сервисная экспертиза, масштабируемость команд мониторинга и реагирования, а также способность работать в режиме гарантированных SLA при сопровождении сложных ИБ-контуров крупных организаций.

Лидеры сегмента услуг информационной безопасности в 2025 году[26]

1. **ГК Солар**
2. **BI.ZONE**
3. **ИнфоТеКС**
4. **Лаборатория Касперского**
5. **Positive Technologies**

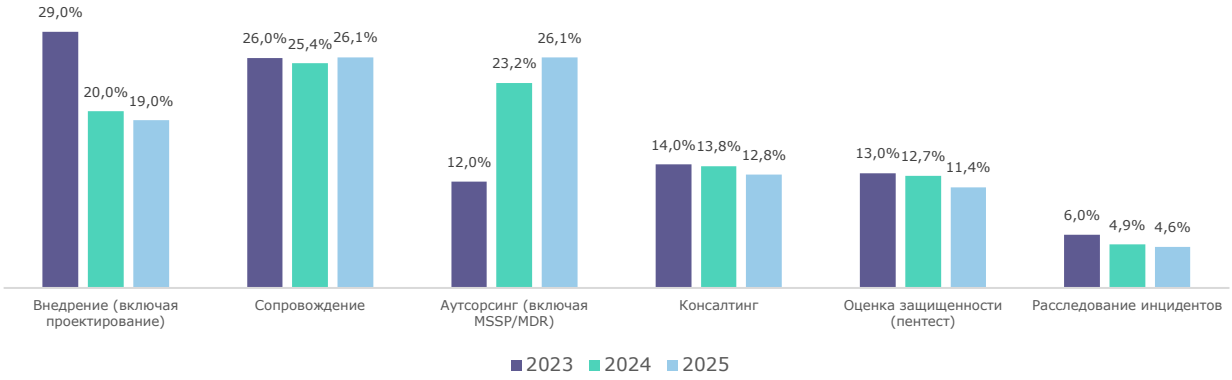
При этом на рынке услуг сильные позиции у классических интеграторов ИТ- и ИБ-решений. Учитывая это, к лидерам рынка оказания услуг информационной безопасности в 2025 году можно отнести также такие компании как ГК Innostage, Jet Infosystems, Информзащита, Ангара, Газинформсервис и другие.

Рис. 6. Долевое распределение услуг ИБ по результатам 2025 года



[26] *Среди производителей средств защиты информации*

Рис. 7. Долевое распределение основных видов услуг ИБ в 2023-2025 годах, %



После резкого сокращения объема проектов внедрения, связанного с макроэкономической ситуацией, рынок услуг перешел к более стабильной динамике. На фоне дефицита специалистов, усложнения атак и давления на бюджеты заказчики все чаще выбирают управляемые сервисы — MSS/MDR, SOC-as-a-Service и др. — как способ быстро получить доступ к экспертизе без дорогостоящего развертывания полноценной внутренней команды и связанных с этим процессов. Если ранее такие сервисы чаще рассматривались как способ закрыть отдельные кадровые разрывы, то теперь они воспринимаются как полноценный инструмент повышения киберустойчивости: мониторинг, реагирование и восстановление после инцидента становятся частью операционной модели бизнеса.

Динамика российского рынка прогноз его развития до 2031 года

С учетом экспертных оценок, при сохранении текущих параметров российский рынок ИБ к 2031 году может превысить 1 трлн рублей. Среднегодовой темп роста (CAGR) в текущем прогнозе оценивается на уровне 19,4%.

> 1 трлн рублей

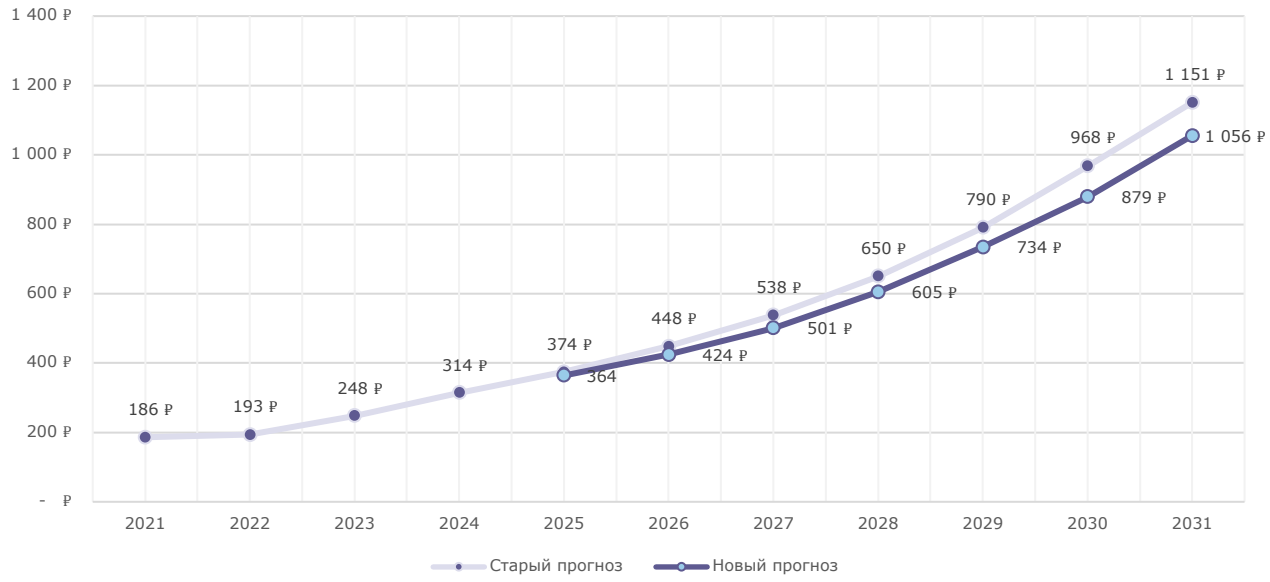
Объем российского рынка информационной безопасности к 2031 году

19,4%

Прогнозируемый среднегодовой темп роста в 2025–2031 гг.

Такая динамика учитывает текущий макроэкономический контекст, но одновременно отражает структурный спрос на безопасность как обязательный элемент цифровой инфраструктуры в долгосрочной перспективе.

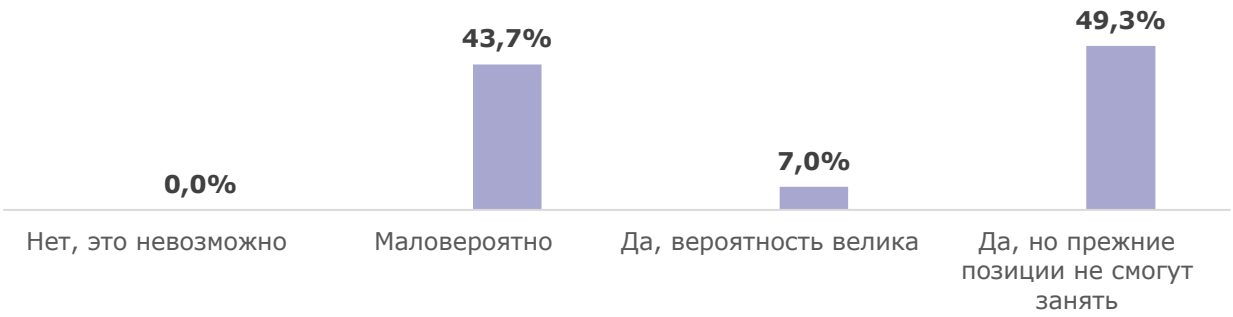
Рис. 8. Прогноз развития рынка ИБ до 2031г.



До 2031 года российский рынок информационной безопасности, как ожидается, сохранит устойчивую положительную динамику, опираясь на внутренний спрос, регуляторные требования и курс на технологическую независимость. Импортозамещение останется одним из факторов роста не только в новых закупках, но и в уже установленной базе: согласно проведенному опросу, общая доля зарубежных решений в инфраструктуре организаций к концу 2025 года оценивается на уровне в 27%.

При этом сценарий полноценного возвращения иностранных вендоров на российский рынок участники опроса оценивают сдержанно. Лишь 7% респондентов считают вероятность такого возвращения высокой. Еще 43,7% называют его маловероятным, а 49,3% допускают возвращение зарубежных игроков, но не ожидают, что они смогут занять прежние позиции.

Рис.9. Перспективы возвращение зарубежных вендоров на рынок РФ до 2031 года



Таким образом, даже при частичном восстановлении присутствия иностранных поставщиков их роль, вероятно, останется ограниченной. При сохранении текущего курса на технологическую независимость и дальнейшем развитии отечественной продуктовой базы доля продаж иностранных решений к 2031 году, по прогнозу, может снизиться ниже 4% от общего объема рынка.

Потенциал сегмента киберстрахования участники рынка оценивают еще более сдержанно: 1,9 балла из 10 в 2026–2028 годах и 4,1 балла в 2029–2031 годах. Такая динамика подтверждает, что киберстрахование пока не воспринимается как самостоятельный крупный драйвер рынка ИБ, но может постепенно усиливать роль финансовой оценки киберрисков, требований к базовой кибергигиене и доказуемости процессов защиты.

Среди ключевых трендов развития рынка до 2031 года респонденты чаще всего выделяют облачные продукты — 67%, защиту ИИ и конфиденциальную обработку данных — 56%, а также автономный SOC и доверенные ПАК — по 44%. Эти оценки показывают, что дальнейший рост рынка будет связан не только с импортозамещением, но и с развитием новых технологических контуров — гибридной инфраструктуры, масштабирования прикладных сценариев применения ИИ, автоматизации мониторинга безопасности и перехода к доверенным программно-аппаратным платформам.

Основные факторы, влияющие на динамику рынка до 2031 г.

Основные факторы, определяющие положительную динамику рынка:

1. **Переход от импортозамещения к системному развитию.** Заказчики все меньше покупают отдельные решения “на замену” и все больше смотрят на совместимость, управляемость, производительность и стоимость владения.

2. **Рост роли киберустойчивости.** Фокус смещается от предотвращения отдельных инцидентов к способности бизнеса выдерживать атаки, быстро восстанавливаться и снижать финансовый ущерб.

3. **Регуляторное давление и рост ответственности.** Требования к защите данных, КИИ, взаимодействию с государственными системами и подрядчиками остаются важным стимулом закупок и модернизации ИБ.

4. **Сервисная модель и дефицит компетенций.** MSS/MDR, SOC-as-a-Service и управляемые сервисы растут как ответ на нехватку специалистов, усложнение атак и необходимость оптимизировать бюджеты.

5. **Консолидация решений и платформенный подход.** Крупные заказчики все чаще хотят не набор разрозненных инструментов, а связанный контур безопасности: от периметра и узлов до мониторинга, реагирования, защиты данных, облаков и приложений.

6. **ИИ-трансформация, облака и новые технологические риски.** ИИ становится одновременно инструментом защиты и источником новых угроз, а его распространение — одним из ключевых факторов пересборки ИТ- и ИБ-архитектур. Искусственный интеллект меняет модели разработки ПО, эксплуатации инфраструктуры, управления данными и принятия решений, формируя новые риски и требования к защите. Это усиливает спрос на новые подходы и классы решений — от специализированной безопасности ИИ-систем и ИИ-агентов до платформ безопасности данных, управления экспозицией рисков, защиты учетных данных, cloud-native-безопасности и новых моделей сетевой защиты в гибридных инфраструктурах.

Сдерживающие факторы:

1. **Макроэкономическое давление.** Высокая ключевая ставка, сокращение CAPEX и более короткие горизонты планирования ограничивают готовность заказчиков к крупным проектам.

2. **Бюджетная осторожность заказчиков.** Компании требуют понятного ROI/ТОЭ, измеримого эффекта и повышения отдачи от уже сделанных инвестиций в ИБ.

3. **Замедление после первой волны импортозамещения.** Часть срочных проектов уже завершена, поэтому дальнейший рост будет больше зависеть от качества решений и зрелости спроса, а не от экстренной замены иностранных продуктов.

4. **Дефицит специалистов.** Нехватка кадров ограничивает способность компаний внедрять и эксплуатировать сложные ИБ-системы, особенно вне крупнейших организаций.

5. **Санкционные и экспортные ограничения.** Они сдерживают международное масштабирование российских решений и ограничивают доступ к отдельным технологиям и компонентам.

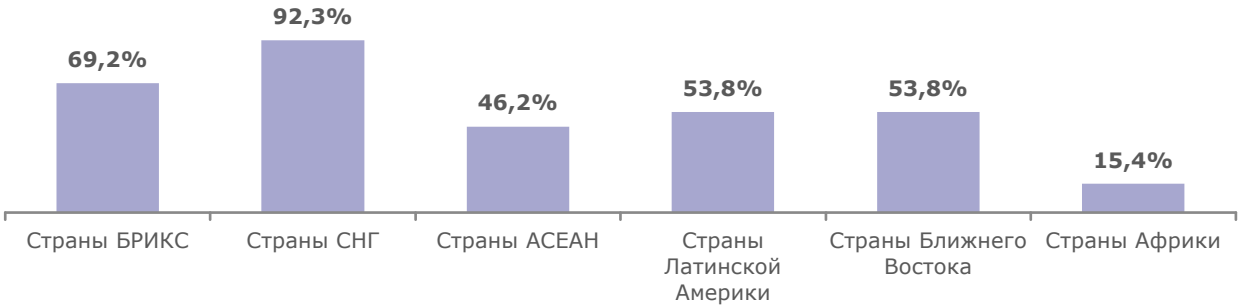
6. **Ужесточение требований к отрасли.** Повышение требований к реестрам, сертификации, доверенным ПАК и регулированию ИИ может поддерживать спрос, но одновременно повышает сложность вывода и эксплуатации продуктов.

Экспортный потенциал российских ИБ-решений

Оценки участников рынка указывают на осторожный, но постепенно расширяющийся горизонт развития. Экспортный потенциал российских ИБ-решений в 2026–2028 годах оценивается респондентами на 3 балла из 10, однако в период 2029–2031 годов показатель повышается до 5 баллов. Это отражает сохранение ограничений для международного масштабирования российских продуктов в ближайшие годы, но также указывает на ожидание постепенного роста внешних возможностей по мере развития продуктовой зрелости и адаптации к дружественным рынкам.

Наиболее перспективными направлениями для экспорта, по мнению участников исследования, являются страны СНГ, которые отметили 92,3% респондентов. Это объясняется тесными историческими и экономическими связями, а также схожими стандартами и регуляторными требованиями в области ИБ. Второе место занимают страны БРИКС с показателем 69,2%, что отражает высокий потенциал сотрудничества в рамках развивающихся экономик.

Рис.10. Самые перспективные направления для экспорта российских ИБ-решений



Далее следуют страны Латинской Америки и Ближнего Востока, которые набрали по 53,8%. Эти регионы рассматриваются как новые, но динамично растущие рынки, заинтересованные в альтернативных источниках технологий и партнёрстве с Россией. Наименее перспективным направлением респонденты назвали страны Африки — лишь 15,4% считают этот регион привлекательным для экспорта ИБ-решений, что может быть связано с ограниченным спросом и недостаточно развитой цифровой инфраструктурой.

Взгляд ключевых игроков рынка[27]

О приоритетах потребителей решений в 2025 году

Павел Коростелев
Руководитель отдела продвижения продуктов, Код Безопасности

«Ключевые запросы заказчиков можно разделить на несколько направлений:
- *На эффективную интеграцию технологий ИБ в ИТ-инфраструктуру*
- *На повышение отдачи от уже сделанных инвестиций*
- *На системы защищенного удаленного доступа»*

Максим Филиппов
Заместитель генерального директора, Positive Technologies

«В 2025 году заказчики заметно сместили фокус с формального внедрения отдельных средств защиты на их практическую результативность. Для них стало важнее не наличие продукта как такового, а способность реально снижать риски, обеспечивать непрерывный мониторинг, быстрое выявление угроз и реагирование на инциденты в режиме 24/7. На этом фоне усилился спрос на комплексные решения и сервисные модели, в которых вендор может закрывать не точечную задачу, а весь контур защиты - от мониторинга и защиты периметра до реагирования и сопровождения. В условиях ограниченных ресурсов заказчики всё чаще выбирают интегрируемые, целостные подходы с понятной ответственностью за итоговый результат.»

Константин Левин
Заместитель директора, группа компаний BI.ZONE

«Сегодня ключевое требование заказчиков при построении защиты — это обеспечение киберустойчивости бизнеса по наиболее эффективной экономической модели. Защита стала отдельным измеряемым бизнес-процессом. Поскольку для организаций остро стоит вопрос оптимизации бюджетов, для обоснования соответствующих трат руководители служб кибербезопасности используют ущерб-ориентированный подход. Он позволяет оценить конкретные риски и реальные финансовые последствия, с которыми может столкнуться компания. Исходя из этого определяется набор организационных и технических мер, необходимых для обеспечения непрерывности бизнеса, — то есть формируются более детальные требования к кибербезопасности. Однако на предупреждении угроз работа по обеспечению киберустойчивости не заканчивается. Тренд — это быстрое восстановление после атаки, которое важно для снижения негативных последствий для бизнеса в случае киберинцидента. Кроме того, на фоне оптимизации затрат компании выбирают сервисную модель обеспечения кибербезопасности, которая направлена на экономию.»

[27] *Стилистика авторов сохранена*

О прогнозах на 2026 год

Павел Коростелев
Руководитель отдела продвижения продуктов, Код Безопасности

«На рынок будут разнонаправленно влиять несколько факторов. Положительно - требования в области защиты государственных информационных систем и безопасность работы с подрядчиками и иными взаимодействующими через СМЭВ организациями, а также уточнение требований в области отраслевого категорирования объектов КИИ и связанные с этим проекты по приведению безопасности значимых объектов КИИ в соответствие требованиям. Вместе с тем, некоторое замедление будет связано с общим охлаждением экономики и связанные с этим сокращение бюджетов и укорачивание горизонтов планирования.»

Максим Филиппов
Заместитель генерального директора, Positive Technologies

«Наш прогноз на 2026 год - сохранение умеренного роста рынка ИБ, ориентировочно в пределах 10–15%. Рынок останется растущим за счёт устойчивого спроса на защиту критичных процессов и общего понимания того, что киберриски напрямую влияют на ключевые бизнес-процессы. Определенным трендом станет распространение интегрального подхода к оценке защищенности и непрерывному ее улучшению. Показательным является Минэнерго России, которое планирует обязать 100 компаний ТЭК выходить на кибериспытания в ближайшие пять лет и сформировать рейтинг цифровой устойчивости. Это означает, что все больше компаний из энергетики начнут проекты по усилению ИБ, что позитивно отразится на его росте.
При этом в 2026 году, вероятнее всего, усилится консолидация рынка. В выигрыше окажутся те компании, которые сумели адаптировать свою бизнес-модель к новым условиям и сфокусироваться на реально востребованных сегментах. Основными факторами влияния на рынок останутся готовность заказчиков тратить деньги на ИБ, стоимость капитала, давление на бюджеты и общее требование к доказуемой эффективности вложений. Для дальнейшего развития отрасли важна более чёткая нормативная рамка в тех зонах, которые пока развиваются быстрее, чем база регулирования, включая кибериспытания, багбаунти и экспорт российских технологий. Появление более понятных правил здесь могло бы поддержать как внутренний рынок, так и международное развитие российских игроков.»

Юлия Косова
Руководитель отдела стратегической аналитики, UserGate

«В 2026 году рынок ИБ сохранит двузначный темп роста, но он будет ниже, чем в предыдущие годы. Основной сценарий - дальнейший переход рынка в фазу зрелости и консолидации. Конкуренция будет усиливаться, особенно в тех сегментах, где продуктовые различия между игроками постепенно сокращаются, расти будут не просто поставщики отдельных решений, а компании, способные предложить заказчику комплексный, технологически связанный и экономически обоснованный контур безопасности. Дополнительное влияние на рынок будут оказывать: продолжение импортозамещения на уровне архитектуры, развитие платформенных моделей, ужесточение регуляторных требований, а также рост спроса на сервисные форматы и автоматизацию функций ИБ. Отдельно стоит ожидать дальнейшего расширения продуктовых линеек со стороны крупных вендоров. При этом со стороны клиентов (особенно крупных федеральных органов власти) будет усиливаться тенденция к закупке нескольких решений у одного поставщика - не только по ценовым причинам, но и из-за требований к совместимости, поддержке и управляемости инфраструктуры.»

О прогнозах на 2026 год

Константин Левин
Заместитель директора, группа компаний BI.ZONE

«В 2026 году компании продолжат секвестирование расходов. Это значит, что оптимизация затрат на обеспечение защиты по-прежнему сохранится. В связи с этим рынок кибербезопасности, как и годом ранее, покажет, по нашим прогнозам, умеренный рост на уровне 10–15%. Среди других факторов, которые способны значительно повлиять на его динамику:

- *Ключевая ставка ЦБ РФ*
- *Усиление регуляторных требований в адрес компаний*
- *Налоговая нагрузка на IT-компании (возможный отказ от налоговых льгот на реализацию ПО может привести к подорожанию лицензий на 20–25%, что формально также приведет к росту рынка)*
- *Сокращение объемов бизнеса компаний (в связи с отсутствием достаточной рентабельности организации начнут отказываться от отдельных направлений бизнеса, что повлияет на инфраструктуру и требования к ее защите, а значит, приведет к сокращению затрат и замедлению роста рынка)*

Запрос бизнеса на разделение ответственности за безопасность между ее поставщиком и компанией (приведет к более комплексному подходу к построению кибербезопасности, что положительно скажется на динамике рынка).»

Взгляд на развитие технологий в перспективе 5 лет и 10 лет

Павел Коростелев

Руководитель отдела продвижения продуктов, Код Безопасности

«Среднесрочно на рынок будут влиять следующие факторы:

- *Импортозамещение ИТ-инфраструктуры, в частности сред виртуализации и контейнеризации. Можно ожидать значительной синергии между разработчиками инфраструктурного ПО и разработчиками СЗИ*
- *Внедрение ИИ для обнаружения угроз, обогащения информации о них, а также для автоматизации рутинных операций. Сюда же можно добавить расширение возможностей создания «домашних» средств аналитики и консолидации и очистки данных за счет использования «Вайб-кодинга»*
- *Уход заказчиков в публичные облака из-за высоких цен и низкой доступности аппаратных компонентов, а также высоких требований LLM к инфраструктуре.*
- *Технологическая фрагментация мирового ИТ-рынка и изоляция российского сегмента Интернет*
- *Конвергенция системного ПО и средств защиты на конечных точках. Механизмы защиты (разграничение доступа, контроль целостности, изоляция ПО перераспределяются на уровень системного ПО. Обнаружение угроз, управление потоками сетевого трафика, в т.ч. VPN, а также анализ соответствия политике безопасности – на наложенные СЗИ»*

Алексей Андреев

Управляющий директор Positive Technologies

«В ближайшие 5 лет ключевым драйвером развития рынка ИБ станет повсеместное внедрение технологий искусственного интеллекта и AI-агентов — как у атакующих, так и у защитников. Значительная часть задач, которые сегодня требуют участия человека, в среднесрочной перспективе будет автоматизироваться и выполняться существенно быстрее.

Второй крупный тренд — платформизация. Рынок будет уходить от набора разрозненных продуктов к более сложным платформам, где ключевую роль играет единая среда данных, общая логика аналитики и возможность работать с большим количеством источников в реальном времени.

Третий важный вектор — развитие облачных и гибридных моделей в построении киберзащиты. Это связано с тем, что именно через такие модели заказчики смогут получать доступ к вычислительным мощностям, большим моделям и сложной аналитике, которые в одиночку разворачивать и поддерживать будет слишком дорого или сложно.

В долгосрочной перспективе конкурентоспособность игроков рынка будет определяться способностью строить AI-first-платформы, работать с большими данными, обеспечивать высокую скорость аналитики и предлагать заказчику максимально автоматизированную, интеллектуальную и адаптивную защиту. Те компании, которые не смогут пройти эту технологическую трансформацию, скорее всего либо останутся в очень узких нишах, либо станут частью более крупных платформенных игроков.»

Взгляд на развитие технологий в перспективе 5 лет и 10 лет

Юлия Косова

Руководитель отдела стратегической аналитики, UserGate

«В ближайшие 5 лет увеличится спрос на комплексные решения в ИБ, продукты, которые одновременно объединяют защиту данных, контроль коммуникаций, управление доступом, применение поведенческой аналитики, мониторинг инфраструктуры и автоматическое реагирование на инциденты. Постепенный переход в Cloud-native security. По мере развития гибридных и облачных сред будет расти спрос на решения, изначально рассчитанные на защиту распределенной инфраструктуры, контейнеров, облачных рабочих нагрузок и API. Рост security-as-a-service (MSSP, SOC-as-a-service, cloud security). Активная интеграция ИИ в кибербезопасность (автоматизация процессов путем перераспределения задач на ИИ). Рынок уже перешел от стадии интереса к стадии практического внедрения, по нашим данные около 90% компаний используют, планируют или пилотируют решения на основе ИИ. На горизонте 10 лет нас ожидает:

- *Переход от набора отдельных ИБ-решений к единым платформам управления безопасностью*
- *Встраивание ИБ в базовую архитектуру ИТ, данных и бизнес-процессов*
- *Переход от автоматизации отдельных операций к полуавтономным и автономным функциям ИБ на основе ИИ*
- *Рост роли ИИ одновременно как инструмента защиты и как источника новых классов угроз*
- *Дальнейшее развитие security-as-a-service и адаптация рынка к новым технологическим рискам, включая автономные системы и постквантовые угрозы.»*

Теймур Хеирхабаров

Директор по продуктам, группа компаний BI.ZONE

«Технологические тенденции, которые будут определять развитие рынка кибербезопасности в ближайшие 5–10 лет:

- *Применение искусственного интеллекта в атаках и защите. Благодаря ИИ скорость атак продолжит повышаться, а барьеры для входа в киберпреступность — снижаться. В ответ на это на стороне защиты в ближайшие годы будут активно развиваться автономные системы кибербезопасности на базе ИИ-агентов, которые будут существенно автоматизировать отдельные процессы. Появятся новые классы средств защиты, а многие специализации в кибербезопасности существенно трансформируются или вовсе исчезнут.*
- *Балканизация интернета и технологический суверенитет. Геополитика постепенно приводит к разделению интернета на независимые сегменты. Страны продолжат развивать собственные технологии для снижения зависимости от зарубежных решений.*
- *Смещение фокуса с предотвращения атак в сторону повышения киберустойчивости и скорости восстановления. С ростом зрелости отрасли приходит понимание, что обеспечить защиту от 100% атак невозможно, важно уметь быстро эти атаки обнаруживать и иметь возможность быстрого восстановления бизнеса в случае, если атака все же произошла.*
- *Развитие направления облачной безопасности. Увеличение проникновения облаков будет стимулировать развитие специализированных решений (CSPM, CNAPP и др.), так как классические подходы инфраструктурной безопасности зачастую не работают в облачных инфраструктурах.*
- *Безопасность identity. Массовое использование ИИ-агентов сделает устаревшей модель «identity = человек». Все решения управления доступом потребуют существенной перестройки в части умения идентифицировать не только людей, но и ИИ-агентов.*

Развитие квантовых вычислений. Это поставит под угрозу современную криптографию и ускорит переход на постквантовые алгоритмы.»

Авторы

Екатерина Кваша
Заместитель генерального директора

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

Приложение 1. Декомпозиция категорий средств защиты

Категории средств защиты	Англоязычный синоним
Средства защиты инфраструктуры	**Infrastructure security**
Средства управления событиями ИБ	Security information and event management (SIEM)
Средства анализа киберугроз	Threat Intelligence (TI)
Средства оркестровки (управления) систем безопасности	Security Orchestration, Automation and Response (SOAR)
Средства защиты промышленных систем управления (систем управления технологическими процессами)	Industrial Control System security (ICS)
Платформы реагирования на инциденты	Incident Response Platform (IRP)
Платформы управления рисками	Governance, Risk and Compliance (GRC)
Средства защиты конечных точек	**Endpoint security**
Антивирусная защита	Antivirus Protection (AVP)
Платформы для защиты конечных точек	Endpoint Protection Platform (EPP)
Системы обнаружения и реагирования на угрозы на серверах и рабочих станциях пользователей	Endpoint Detection and Response (EDR)
Средства защиты сетей	**Network security**
Межсетевые экраны (в т.ч. «нового поколения»)	(Next Generation) Firewall (FW, NGFW)
Многофункциональные решения сетевой безопасности	Unified Threat Management (UTM)
Системы обнаружения/предотвращения вторжений	Intrusion Detection/Prevention System (IDS/IPS)
Системы анализа сетевого трафика	Network Traffic Analysis (NTA)
Средства контроля доступа к сети	Network Access Control (NAC)
Средства обнаружения и реагирования на сложные, неизвестные киберугрозы	Network Detection & Response (NDR)
Шлюзы информационной безопасности	Security Web/Mail Gateway (SWG/SMG)
Сетевые «песочницы»	Network Sandbox
Виртуальные частные сети	Virtual Private Network (VPN)
Средства защиты приложений	**Application security**
Средства контроля и оценки уязвимостей	Vulnerability Assessment (VA)
Средства управления уязвимостями	Vulnarability Management (VM)
Средства поиска уязвимостей в исходном коде ПО	Application Security Testing (AST)
Межсетевой экран для веб-приложений	Web Application Firewall (WAF)
Защита от DDoS-атак	DDoS Protection
Средства защиты данных	**Data security**
Средства защиты от несанкционированного доступа	Unauthorized Access Protection (UAP)
Средства защиты от утечек информации	Data Loss Prevention (DLP)
Средства шифрования	Encryption
Средства управления доступом	**Access management**
Средства управления идентификацией, аутентификацией и контролем доступа	Identity & Access Management/Governance & Administration (IAM/IGA)
Средства контроля привилегированных пользователей	Privileged Access Management (PAM)
Средства управления криптографической инфраструктурой (в т.ч. средства электронной подписи)	Public Key Infrastructure (PKI)

Москва, 125009, Газетный пер., 3–5 стр. 1, 3 этаж
Тел.: +7 (495) 410-15-53
E-mail: info@csr.ru

csr.ru