Ноябрь 2025

Прогноз развития рынка кибербезопасности в Российской Федерации на 2025-2030 годы

ЦСР
ЦЕНТР СТРАТЕГИЧЕСКИХ РАЗРАБОТОК

Ключевые выводы

Объем российского рынка кибербезопасности по итогам 2024 года составил **314 млрд рублей** при росте в **26,3%**. Темпы роста остаются высокими – выше мирового роста рынка ИБ (11,8%) и темпов роста отечественного ИТ-рынка, который по разным оценкам составлял 9,8-15% в 2024 году. Соотношение поставок СЗИ и услуг почти не изменилось. Совокупная доля услуг ИБ выросла на 0,4%, составив 26,9% рынка, а средств защиты информации (СЗИ) – 73,1%. Сохраняется тенденция снижения доли зарубежных вендоров, продолжает усиливаться доминирующее положение российских компаний. По итогам 2024 года доля иностранных решений в совокупных затратах компаний снизилась **до 7%** против 11% в 2023 году. Из десятки лидеров рынка полностью выбыли иностранные производители, официально покинувшие российский рынок.

Ведущие игроки рынка – **Лаборатория Касперского** (19,6%) и **Positive Technologies** (13,6%) сохранили свои прошлогодние позиции, так же, как и замыкающие лидирующую пятерку ИнфоТеКС (5,9%), Код Безопасности (5,1%) и UserGate (4,9%). При этом 3,8% рынка пришлось в 2024 году на новых отечественных игроков (включая стартапы), связанных с защитой сети, инфраструктуры и приложений, защитой облачной инфраструктуры и ИБ-услугами.

Объем рынка СЗИ по итогам в 2024 года составил **229,5 млрд рублей** с приростом в **25,6%**. Наибольший рост в абсолютных значениях к прошлому году показывают крупнейшие сегменты средств защиты сетей (доля 35,8%, прирост 25,9%) и конечных точек (доля 15,2%, прирост 24,3%). Сегмент средств защиты инфраструктуры испытывает небольшое снижение доли (доля 17,2%, прирост 14%), которое обусловлено как насыщением рынка, так и ситуативным перераспределением затрат в сторону импортозамещения сетевой защиты. В РФ формируется рынок облачных ИБ-сервисов и спрос на специализированные ИБ-решения (CNAPP, CSPM, CWPP, CASB и других категорий). Суммарно объем продаж данных решений уже превысил 1% от общей емкости рынка ИБ.

Объем рынка услуг по итогам 2024 года составил **84,5 млрд рублей** с ростом в **28,3%.** Отмечается тенденция существенного увеличения доли услуг аутсорсинга ИБ (MSSP/MDR) на 11,2%. Кроме того, на рынке заметно повышение интереса компаний к таким современным «краудсорсинговым» инструментам аудита безопасности как Bug-Bounty и формату «кибериспытаний» (в совокупности это 3% от объема всех услуг по анализу защищенности), что свидетельствует о повышении зрелости рынка в части практической безопасности.

С учетом экспертных оценок и текущего макроэкономического прогноза до 2028 года емкость российского рынка кибербезопасности **к 2030 может достичь 968 млрд рублей (21% CAGR).** До 2030 года рынок сохранит устойчивый рост, опираясь на внутренний спрос и политику технологического суверенитета. При сохранении темпов импортозамещения ожидается, что доля иностранных решений упадет к 2030 году до 4% от общего объема.

Ключевыми драйверами рынка будут активная государственная политика, направленная на обеспечение национальной безопасности и технологического суверенитета, сохранение налоговых льгот для российских разработчиков ПО, рост деструктивности кибератак, стимулирующих развитие практической кибербезопасности, усиление требований регуляторов и ответственности компаний за утечки данных, рост сервисных предложений (MSSP/MDR) в условиях дефицита квалифицированных ИБ-специалистов и рост применения технологий ИИ, порождающий новые ИБ-угрозы.

Ограничителями выступают экономические факторы (ключевая ставка, снижение инвестиционной активности в ИБ, повышение страховых взносов для IT-компаний и др.); усиление регулирования (новые правила регистрации в реестре отечественного ПО, повышающие порог входа для новых разработчиков СЗИ и сервисов, законопроект о реестре ФСБ для «белых хакеров» и др.) и внешние санкционные ограничения, вынуждающие российские компании ориентироваться в основном на внутренний рынок.

Введение

Фонд «Центр стратегических разработок» (далее также ЦСР) продолжает ежегодную серию исследования рынка кибербезопасности Российской Федерации с формированием его краткосрочного прогноза на ближайшие годы.

В прошлогоднем исследовании оценка объемы рынка кибербезопасности по итогам 2023 года составила 248,5 млрд рублей. В настоящем отчете ЦСР актуализировал оценку и прогноз рынка по результатам 2024 года. Целью исследования является формирование оценки рынка кибербезопасности в России в 2024 году и уточненного прогноза его развития до 2030 года, выявление тенденций развития рынка, а также оценка процессов замещения зарубежных продуктов.

Исследование проводилось с июня по октябрь 2025 года на основе анализа сведений из открытых источников о выручке основных вендоров продуктов информационной безопасности B2B рынка за 2024 год, опроса вендоров и дистрибьюторов — представителей основных игроков российского рынка. В данном исследовании объем рынка оценивался «в деньгах заказчика». При интерпретации результатов в спорных случаях мы исходили из принципа добросовестности игроков рынка и доверяли предоставленным сведениям.

Основной акцент в данном отчете, как и ранее, сделан именно на средствах защиты информации (СЗИ) и их поставщиках, услуги рассматриваются укрупненно.

В рамках исследования рассматривались следующие категории средств защиты информации:

- средства защиты сетей (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);

Детализированный перечень категорий приведен в Приложении А.

ЦСР выражает благодарность всем участникам проведенного в рамках исследования опроса за предоставленные сведения.

Тренды рынка кибербезопасности России

В рамках государственной политики в России в последние годы особое внимание уделяется **кибербезопасности как важной части национальной безопасности и технологического суверенитета**. Так в 2021 году кибербезопасность впервые вошла в стратегию национальной безопасности России[1], а в 2023 году была утверждена «Концепция технологического развития до 2030 года»[2], направленная на достижение «технологического суверенитета» и определяющая «нарушение безопасности инфраструктуры, продукции и производственных процессов, включая информационную безопасность» как угрозу для технологического развития Российской Федерации в период с 2023 по 2030 год.

Несмотря на непростую макроэкономическую ситуацию, в 2025 году было принято решение продлить ключевые **налоговые стимулы для ИТ- и ИБ-отрасли** в целях поддержания курса на технологический суверенитет. В частности, сохранена льгота[3] по налогу на добавленную стоимость (НДС) на продажи отечественного программного обеспечения. Таким образом, до конца 2025 года продажи программ, включенных в реестр отечественного ПО, освобождены от НДС, а с 2026 г. эта льгота, вероятно, будет продлена. Сохранение 0% НДС позволяет российским разработчикам средств защиты информации (СЗИ) и других ИБ-решений оставаться конкурентоспособными на внутреннем рынке и направлять сэкономленные средства на развитие отечественной продуктовой линейки.

Период 2024–2025 гг. в России характеризуется **ростом кибератак всё более деструктивного характера**. Если раньше злоумышленники чаще преследовали финансовую выгоду, то теперь их цель, наряду с организацией утечек данных, – максимальный ущерб бизнес-процессам организаций («паралич» ИТ-инфраструктуры). Показательны инциденты лета 2025 года, когда, например, в июле 2025 года крупнейший авиаперевозчик страны «Аэрофлот» подвергся хакерской атаке, которая привела к сбою ИТ-систем и отмене десятков рейсов. Хакерские группировки, взявшие на себя ответственность за атаку, заявили, что не только выкачали порядка 22 Тб данных, но и «*уничтожили 7000 физических и виртуальных серверов*» компании[4]. Одновременно в середине июля 2025 года сеть розничных магазинов «ВинЛаб» (Novabev Group) столкнулась с другой атакой, в результате которой *«была временно нарушена работоспособность части IT-инфраструктуры»*, а точки продаж и онлайн-сервисы перестали работать. Позднее компания подтвердила масштаб инцидента как «беспрецедентный»**.** Эти случаи показывают, что современные кибератаки всерьез нацелены на создание разрушительных последствий для бизнеса – остановку бизнес-процессов, подрыв доверия и репутации. Это стимулирует отечественные компании уделять повышенное внимание практической кибербезопасности.

Следует отметить, что общий **макроэкономический фон** в 2024–2025 годах привел к ограничению естественного роста рынка информационной безопасности, бизнес был вынужден сокращать или откладывать расходы, в том числе на дорогостоящие инфраструктурные ИТ- и ИБ-проекты.

Другой тенденцией периода 2024-2025 годов стало **ужесточение регулирования** в сфере защиты данных и ИБ в целом, которое привело к повышению ответственности бизнеса и менеджмента за инциденты кибербезопасности. Летом 2025 года вступили в силу поправки, значительно увеличивающие ответственность за утечки персональных данных. Так Федеральным законом №420-ФЗ от 30.11.2024 (вступил в силу 30 мая 2025 года) **введены оборотные штрафы**: повторные

---

[1] *Указ Президента РФ от 9 мая 2017 г. N 203 "О Стратегии развития информационного общества в РФ на 2017–2030гг".*

[2] *Распоряжение Правительства РФ от 20 мая 2023 г. № 1315-р*

[3] *Правительство отказалось от отмены льготы..., Ведомости, 2025*

[4] *«Аэрофлот» подвергся беспрецедентной хакерской атаке, Коммерсантъ, 2025*

утечки теперь грозят компании штрафом от 1 до 3% годового оборота (но не менее 25 млн руб. и не более 500 млн руб.).

Помимо финансовых санкций для бизнеса за недостаточное внимание к кибербезопасности, регуляторы подняли и **требования к продуктам и сервисам кибербезопасности**. В 2025 году ужесточены критерии включения ПО в Единый реестр российского программного обеспечения, что, с одной стороны, должно способствовать повышению качества и независимости отечественных решений от иностранных компонентов, но, с другой стороны, серьезно увеличивает порог входа на рынок для новых разработчиков и замедляет развитие решений в целом. Кроме того, предпринимаются попытки создания системы регулирования деятельности исследователей безопасности («белых хакеров»). Так предлагалось [5] ввести обязательную идентификацию исследователей, аккредитацию организаций, правила уведомления госорганов о найденных уязвимостях и даже уголовную ответственность за «неправомерную передачу уязвимости» третьим лицам. Рынок ИБ встретил эти идеи настороженно. Эксперты называют текущие формулировки достаточно жесткими, ставящими под угрозу не только работу квалифицированных ИБ-исследователей, но и желание компаний использовать для обеспечения своей информационной безопасности такие передовые «краудсорсинговые» практики, как, например, «баг-баунти» (bug bounty). Крупные игроки ИБ-рынка находятся в диалоге с регуляторами, призывая доработать законопроект, поскольку в текущем виде он «может вывести часть услуг за рамки правового поля».

При этом серьёзным вызовом для отрасли остаётся **кадровый голод** – нехватка квалифицированных специалистов по информационной безопасности. По некоторым данным[6], спрос на ИБ-экспертов в 2023–2025 гг. взлетел, особенно в промышленности и финансах, и многим предприятиям сложно привлечь и удержать таких сотрудников. В условиях дефицита компетенций и растущей сложности атак компании всё чаще обращаются к внешним сервисам и аутсорсингу ИБ. Это стимулирует активный **рост управляемых сервисов по кибербезопасности** (Managed Security Services, MSS) и услуг мониторинга и реагирование на угрозы (Managed Detection and Response, MDR). Параллельно набирает популярность практика привлечения сторонних специалистов через программы «баг баунти» и другие **формы «краудсорсинговой» кибербезопасности**. Многие компании начали открыто тестировать свою защиту силами сообщества «белых хакеров». Если ранее такие программы проводили в основном ИТ-гиганты, то теперь и госсектор, и бизнес всех уровней выходят на отечественные баг-баунти-платформы. Например, Минцифры России регулярно запускает этапы программ по поиску уязвимостей в важных госуслугах. Так, с июля 2025 по декабрь 2026 проводится открытая программа баг-баунти для девяти ключевых сервисов (портал «Госуслуги», ЕСИА, ЕБС и др.), где любой желающий исследователь может получить до 1 млн рублей за обнаружение критической уязвимости. К участию уже привлекли более 26 тысяч независимых исследователей, что значительно расширяет охват и глубину тестирования систем. В данном контексте отдельного упоминания заслуживает формат так называемых «кибериспытаний» – тестовых атак на компании по заранее заданным сценариям, ориентированным на достижение «недопустимых событий», которые формулирует бизнес (высшее руководство организации). Формат отличается от классического баг-баунти тем, что проверяется не одна уязвимость, а цепочка действий злоумышленника, способная привести к серьёзным последствиям для компании («недопустимым событиям»). Таким образом кибербезопасность становится стратегическим приоритетом уровня управления бизнесом. Подтверждением этому становится и увеличение количества программ киберстрахования для бизнеса, предлагаемых ведущими российскими страховщиками.

Наряду с внутренними драйверами, на российский рынок кибербезопасности оказывают влияние и внешние санкционные ограничения. После 2022 года западные государства ввели против Российской Федерации санкции, затронувшие ИТ- и телеком-сектор. Многие зарубежные производители ИБ-продуктов (антивирусы, межсетевые экраны, системы мониторинга) прекратили продажи и поддержку

---

[5] *Законопроект № 509708-8, 2025*

[6] *Российская промышленность массово ищет специалистов..., Известия, 2025*

в России. В этих условиях отечественным компаниям приходится опираться почти исключительно на внутренний рынок – как в плане спроса, так и предложения технологий. Российские разработчики форсированно заменяют недоступные западные аналоги собственными решениями. Для российских ИБ-вендоров сейчас основным полем сбыта остается домашний рынок – корпоративные и государственные заказчики внутри страны, где из-за санкций резко возрос спрос на отечественные продукты. Выход же на крупнейшие мировые рынки затруднен: во-первых, из-за экспортных ограничений (некоторые российские ИБ-компании сами попали под санкции); во-вторых, из-за геополитической обстановки, снижающей доверие к импортным поставщикам в ряде стран. Тем не менее, в рамках Евразийского союза и других дружественных объединений наметилось формирование автономного киберпространства. Российские решения по безопасности начинают занимать ниши в соседних странах – в частности, осваивается рынок Беларуси и Центральной Азии.

В настоящее время можно констатировать, что отечественный рынок ИБ продолжает активно развиваться, в частности, это подтверждается количеством зарегистрированных в 2024 году организаций, занимающихся разработкой продуктов в сфере кибербезопасности, как одним из основных видов деятельности – по оценкам ЦСР за 2024 год таких организаций зарегистрировано более 300. Общее количество компаний, занимающихся кибербезопасностью по состоянию на 01.01.2025, превысило 11,2 тыс.[7], а количество российских ИБ стартапов по некоторым оценкам выросло на 8% за 2024 год[8].

[7] *В РФ число компаний в сфере кибербезопасности выросло на 41%, ТАСС, 2025*
[8] *Доля ИБ-стартапов в России за два года выросла в 1,5 раза, CyberStage, 2025*

Оценка рынка кибербезопасности по результатам 2024 года в России

Рынок кибербезопасности Российской Федерации по результатам 2024 года оценивается в 314 млрд рублей[9], прирост общего объема рынка кибербезопасности (продукты и услуги) составил 26,3% к показателю 2023 года (248,5 млрд руб.).

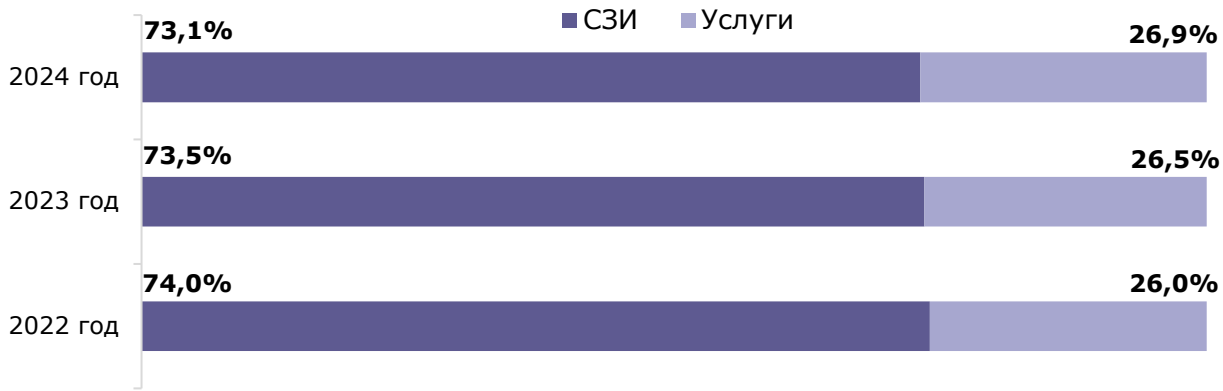
314 млрд руб. **+26,3%**

Объем российского рынка кибербезопасности по итогам 2024 года и его прирост

Темпы роста остаются высокими – выше роста отечественного ИТ-рынка, который по разным оценкам[10] составил 9,8-15% в 2024 году. Данные показатели также значительно превышают рост мирового рынка ИБ, прогноз роста которого до 2028 года оценивался в 11,8%[11].

Соотношение поставок СЗИ и услуг почти не изменилось. Тем не менее, в 2024 году совокупная доля услуг немного выросла, составив 26,9% (26,5% по итогам 2023 года) всего объема рынка, а средств защиты информации – 73,1% (73,5% по итогам 2023 года).

Диаграмма 1. Совокупная доля услуг и поставок средств защиты информации



[9] Расчет осуществлен на основе данных из различных источников, в том числе из официальной отчетности компаний, данных закупочных площадок и других источников на правах анонимности. При оценке рассматривались данные как по вендорам, так и по интеграторам, оказывающим услуги. Учитывалось, что выручка вендора не обязательно равна его присутствию на рынке в связи с партнерской скидкой дистрибьютора/интегратора.

[10] «Рынок ИТ России 2024», СТРИМ Консалтинг, 2024, «Рынок инфраструктурного ПО в России», Strategy Partners 2024

[11] «Forecast: Information Security, Worldwide, 2022-2028, 4Q24 Update», Gartner, 2024

Диаграмма 2. Доля российских и зарубежных вендоров средств защиты информации

На российском рынке кибербезопасности в 2024 году сохраняется тенденция снижения доли зарубежных вендоров, продолжает усиливаться доминирующее положение российских компаний: они занимают уже 93% рынка СЗИ (в 2023 году – 89%). По итогам 2024 года иностранные решения в совокупных затратах занимают 7% (в 2023 году – 11%). Стоит отметить, что в прошлогоднем прогнозе ожидалось снижение доли закупки зарубежных продуктов на российском рынке до 5,7%. В целом небольшое замедление темпов вытеснения зарубежных продуктов обуславливается сохранением официального присутствия некоторыми иностранными вендорами (например, израильской Check Point) на рынке, поставками по каналам параллельного импорта тех иностранных решений, которые пока нет возможности полноценно и оперативно заменить на отечественные аналоги (например, некоторое сетевое оборудование - многофункциональные межсетевые экраны, МСЭ) и общим ростом стоимости приобретения необходимых иностранных СЗИ в настоящих условиях.

По итогам 2024 года состав топ-30 лидеров рынка кибербезопасности из числа вендоров СЗИ выглядит следующим образом:

1. **Лаборатория Касперского**
2. **Positive Technologies**
3. **ГК Солар**
4. **BI.ZONE**
5. **ИнфоТеКС**
6. **Код Безопасности**
7. **UserGate**
8. **Крипто-Про**
9. **Check Point**
10. **Search Inform**
11. **Киберпротект**
12. **InfoWatch**
13. **ГК Гарда**
14. **Фактор-ТС**
15. **Актив-Софт**
16. **F6**
17. **Security Vision**
18. **Fortinet**
19. **R-Vision**
20. **S-Terra**
21. **Амикон**
22. **Cisco**
23. **Palo Alto Networks**
24. **Qrator Labs**
25. **Атлас-Карт**
26. **Dr.Web**
27. **Ай-Ти Бастион**
28. **Ideco**
29. **Индид**
30. **Аладдин Р.Д.**

Лидерами рынка, с заметным отрывом от остальных участников, являются Лаборатория Касперского и Positive Technologies. К крупнейшим игрокам на российском рынке кибербезопасности следует отнести ГК Солар, BI.ZONE, ИнфоТеКС, Код Безопасности и UserGate.

В 2024 году из десятки лидеров полностью выбыли иностранные производители, ушедшие с российского рынка. Исключение – израильская Check Point, которая не только сохраняет

официальное присутствие в РФ, но и, по некоторым сведениям, планирует развивать бизнес[12]. В совокупности, первые десять перечисленных компаний занимают 60% отечественного рынка кибербезопасности.

В 2024 году 3,8% рынка пришлось на рост относительно новых отечественных игроков и стартапы, связанные с защитой сети, инфраструктуры и приложений (например, Xello, Вебмониторэкс, Metascan и Codemaster, преодолевших в прошлом году отметку в 500 млн руб. выручки), защитой облачной инфраструктуры (например, вышедший на рынок безопасности Yandex Cloud (входит в Yandex B2B Tech), Luntry (Клаудран) и другие) и ИБ-услугами (например, RED Security и другие).

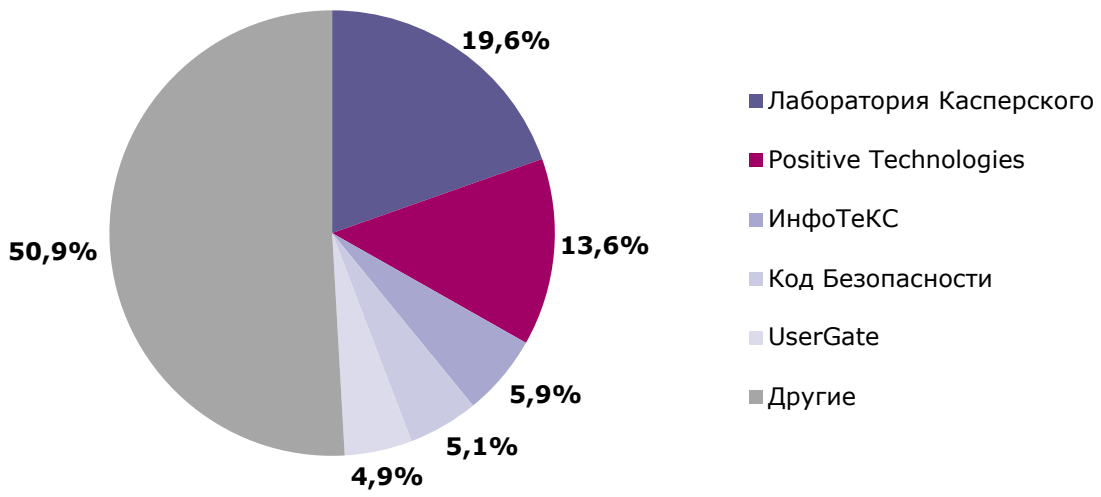
Оценка рынка СЗИ по результатам 2024 года

Лидирующая пятерка вендоров СЗИ в 2024 году не изменилась – все игроки сумели сохранить свои позиции.

Таблица 1. Топ-5 вендоров средств защиты информации по выручке в 2024 году (без учета услуг)

Позиция	Вендор	Юрисдикция
1	**Лаборатория Касперского**	**РФ**
2	**Positive Technologies**	**РФ**
3	**ИнфоТеКС**	**РФ**
4	**Код Безопасности**	**РФ**
5	**UserGate**	**РФ**

Диаграмма 3. Доля топ-5 вендоров средств защиты информации на рынке по результатам 2024 года



[12] *«Check Point может создать СП с российским партнером для выпуска NGFW»*, *SecPost, 2025*

На следующей диаграмме приведено долевое распределение ключевых категорий средств защиты информации в 2024 году:

- средства защиты сетей (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);

Диаграмма 4. Долевое распределение категорий средств защиты информации по результатам 2024 года

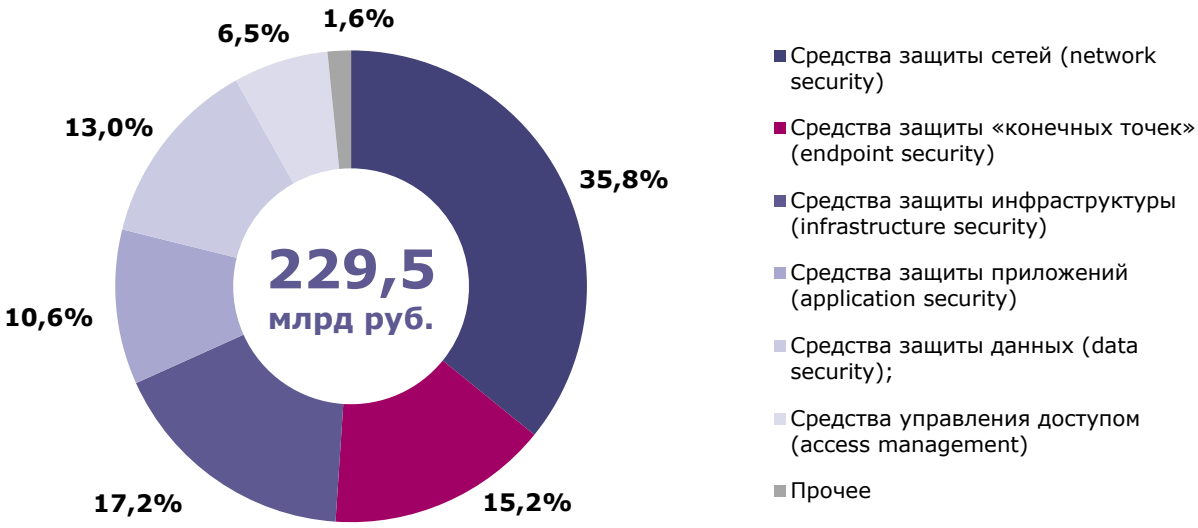
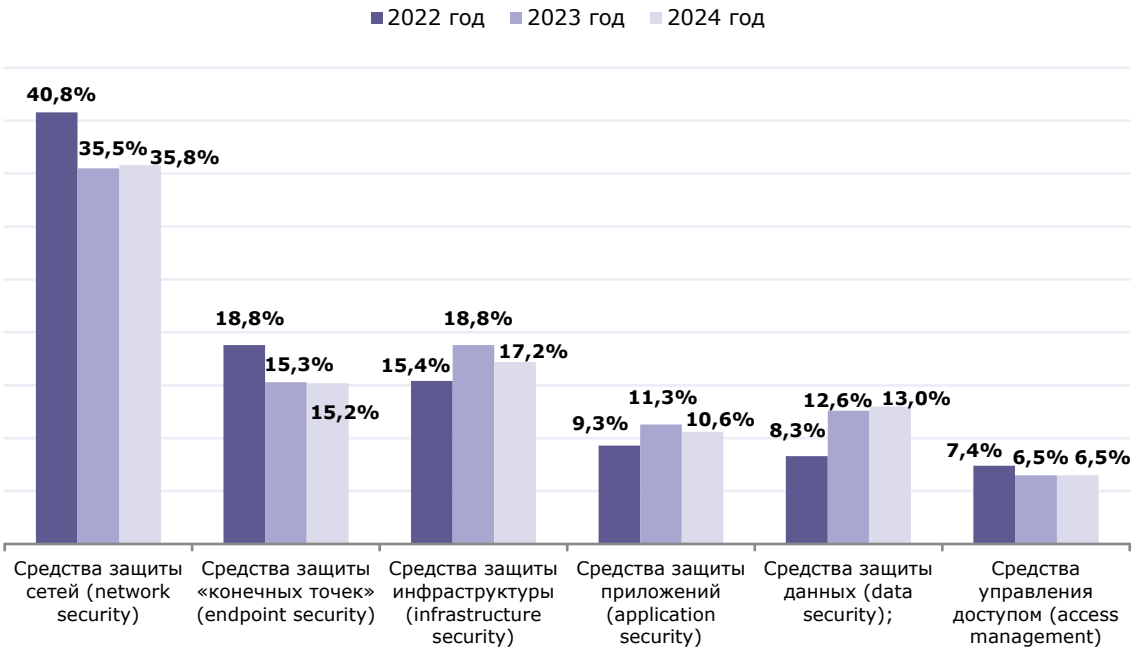


Диаграмма 5. Долевое распределение продаж в категориях средств защиты информации в 2022-2024 годах



В ретроспективе, на протяжении трехлетнего периода наблюдения, отмечается стабилизация структуры спроса. Наибольший рост в абсолютном объеме рынка к прошлому году показывают крупнейшие сегменты средств защиты сетей и конечных точек (с темпом +26% и +24% к 2023 году соответственно), при этом сегмент средств защиты инфраструктуры испытывает небольшое снижение в доле продаж (на 1,5%), которое обусловлено насыщением рынка, длительностью внедрения данного класса средств защиты и ситуативным перераспределением затрат в сторону импортозамещения сетевой защиты.

В РФ быстро растет рынок облачной инфраструктуры и сервисов (+30-40% в год по разным оценкам)[13] и формируется спрос на специализированные ИБ-решения (CNAPP, CSPM, CWPP, CASB и других категорий). Суммарно объем продаж данных решений превысил 1% от общей емкости рынка ИБ, включая в себя решения от таких отечественных производителей, как Лаборатория Касперского, Yandex Cloud, Luntry (Клаудран), Cloud Advisor (Клаудэдвайзор) и других.

Также стоит отметить, что сформировавшийся в России еще до 2022 года сегмент кибербезопасности промышленных систем составляет на сегодня немногим более 1% от всей емкости рынка ИБ, что, учитывая большую базу промышленных предприятий в России, может свидетельствовать о нереализованном потенциале роста в данной нише.

Таблица 2. Топ-5 вендоров в разрезе категорий средств защиты информации по итогам 2024 года

Позиция	Вендор/Сегмент	Юрисдикция
	Средства защиты сетей (network security)	
1	**UserGate**	**РФ**
2	**Код Безопасности**	**РФ**
3	**Positive Technologies**	**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	**Search Inform**	**РФ**
	Средства защиты приложений (application security)	
1	**Positive Technologies**	**РФ**
2	**ГК Солар**	**РФ**
3	**BI.ZONE**	**РФ**
4	**SolidSoft**[14]	**РФ**
5	**Вебмониторэкс**	**РФ**
	Средства защиты данных (data security)	
1	**Infowatch**	**РФ**
2	**ГК Солар**	**РФ**

[13] *Рынок облачных услуг в России вырастет на 30% в 2025 году, CNews, 2025*
[14] *В 2025 году 50% компании SolidSoft было приобретено Yandex B2B Tech*

Позиция	Вендор/Сегмент	Юрисдикция
3	Гарда Технологии	РФ
4	ИнфоТеКС	РФ
5	SearchInform	РФ
	Средства управления доступом (access management)	РФ
1	Актив-Софт	РФ
2	Крипто-Про	РФ
3	АЙ-ТИ БАСТИОН	РФ
4	Аладдин Р.Д.	РФ
5	Индид	РФ

Таким образом, рынок СЗИ в Российской Федерации в 2024 году продолжил расти и составил 229,5 млрд рублей с совокупным приростом к 2023 году в 25,6%. Можно сделать вывод, что российский рынок продуктов кибербезопасности продолжает активно развиваться, при этом наблюдается существенное замещение доли зарубежных решений.

229,5 млрд руб. **+25,6%**

Объем российского рынка СЗИ по итогам 2024 года и его рост относительно 2023 года

Декомпозиция объемов долей рынка и расчетных значений прироста за 2024 год по категориям рассмотренных ранее средств защиты приведена в Таблице 3.

Таблица 3. Декомпозиция объемов долей рынка и расчетных значений прироста за 2024 год по категориям рассмотренных ранее средств защиты

Категория СЗИ	Доля рынка (%)	Объем доли рынка (млрд руб.)	Прирост за 2024 год (%)
Средства защиты сетей (network security)	35,8 %	82,0	25,9 %
Средства защиты «конечных точек» (endpoint security)	15,2 %	34,9	24,3 %
Средства защиты инфраструктуры (infrastructure security)	17,2 %	39,4	14,0 %
Средства защиты приложений (application security)	10,6 %	24,3	17,6 %
Средства защиты данных (data security)	13,0 %	29,8	28,8 %
Средства управления доступом (access management)	6,5 %	14,9	27,3 %

Оценка рынка услуг по результатам 2024 года

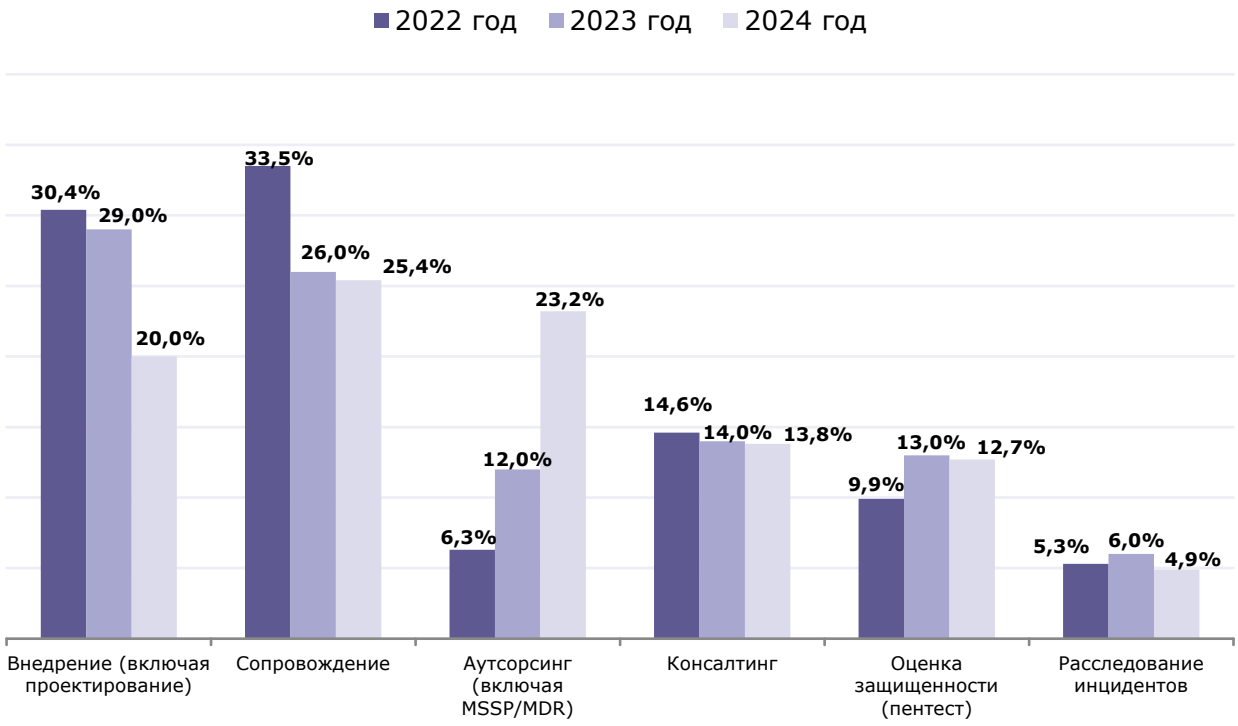
Распределение предлагаемых на рынке в 2024 году категорий услуг в области обеспечения кибербезопасности:

- внедрение, включая подготовительные этапы, проектирование и сопровождение (обеспечение жизненного цикла средств защиты);
- консалтинг, включая оценку защищенности информационных ресурсов и расследование инцидентов информационной безопасности;
- аутсорсинг, включая управление средствами защиты, выявление и реагирование на инциденты (MSSP, MDR и т.п.).

Диаграмма 6. Долевое распределение услуг ИБ по результатам 2024 года

В ретроспективе трехлетнего периода наблюдается выраженная тенденция роста доли услуг по аутсорсингу информационной безопасности (MSSP/MDR) — на 11,2%, при одновременном снижении объема услуг по внедрению решений на 9% по сравнению с 2023 годом. Объем услуг анализа защищенности остался практически на прежнем уровне, однако внутри этого сегмента отмечается рост популярности программ баг-баунти и «кибер-испытаний», которые в совокупности заняли около 3% рынка услуг по оценке защищенности в 2024 году. На этом фоне прослеживается усиливающийся интерес к киберстрахованию и появление специализированных программ страхования кибер-рисков от ведущих страховых компаний. Эти тенденции свидетельствуют о повышении зрелости отрасли в сфере практической кибербезопасности.

Диаграмма 7. Долевое распределение услуг ИБ в 2021-2023 годах



Топ-5 вендоров на рынке услуг информационной безопасности в 2024 году

1. **ГК Солар**
2. **BI.ZONE**
3. **ИнфоТеКС**
4. **Код Безопасности**
5. **Positive Technologies**

При этом на рынке услуг сильные позиции у интеграторов решений. Учитывая это, к лидерам рынка оказания услуг информационной безопасности в 2024 году можно отнести:

1. **ГК Солар**
2. **BI.ZONE**
3. **ГК Innostage**
4. **Jet Infosystems**
5. **Информзащита**

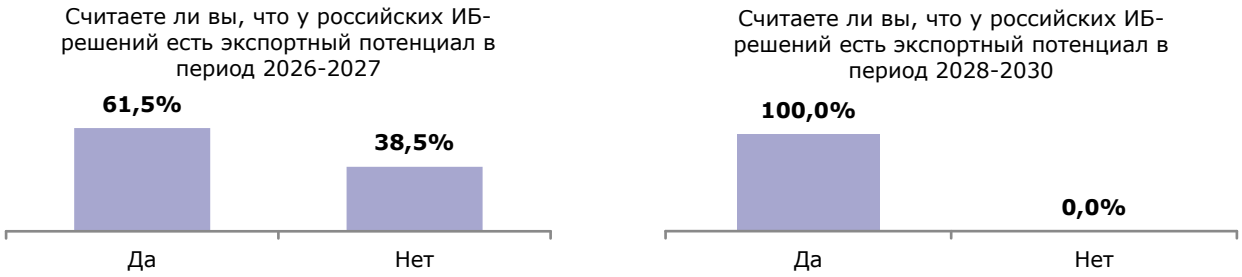
Объем рынка услуг по итогам 2024 года составил 84,5 млрд руб. с приростом в 28,3%. Рынок услуг в области кибербезопасности также растет значительными темпами.

84,5 млрд руб. **+28,3%**

Объем российского рынка ИБ услуг по итогам 2024 года и его годовой прирост

Экспортный потенциал российских ИБ-решений

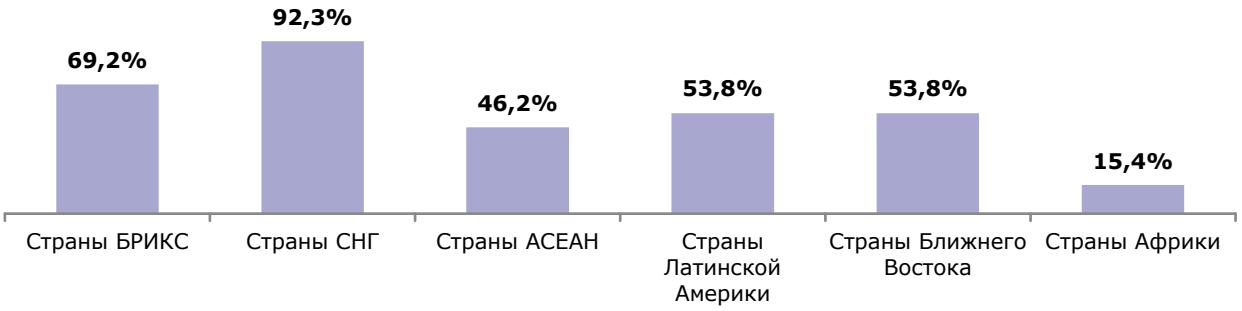
Диаграмма 8. Экспортный потенциал российских ИБ-решений



Согласно приведенному опросу, можно отметить устойчивый рост уверенности в экспортном потенциале российских ИБ-решений. Если в период 2026–2027 годов 61,5% респондентов считают, что отечественные решения обладают экспортным потенциалом, а 38,5% придерживаются противоположного мнения, то уже на период 2028–2030 годов сто процентов опрошенных уверены в том, что российские ИБ-решения смогут претендовать на востребованность за рубежом.

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.

Диаграмма 9. Перспективные направления для экспорта российских ИБ-решений



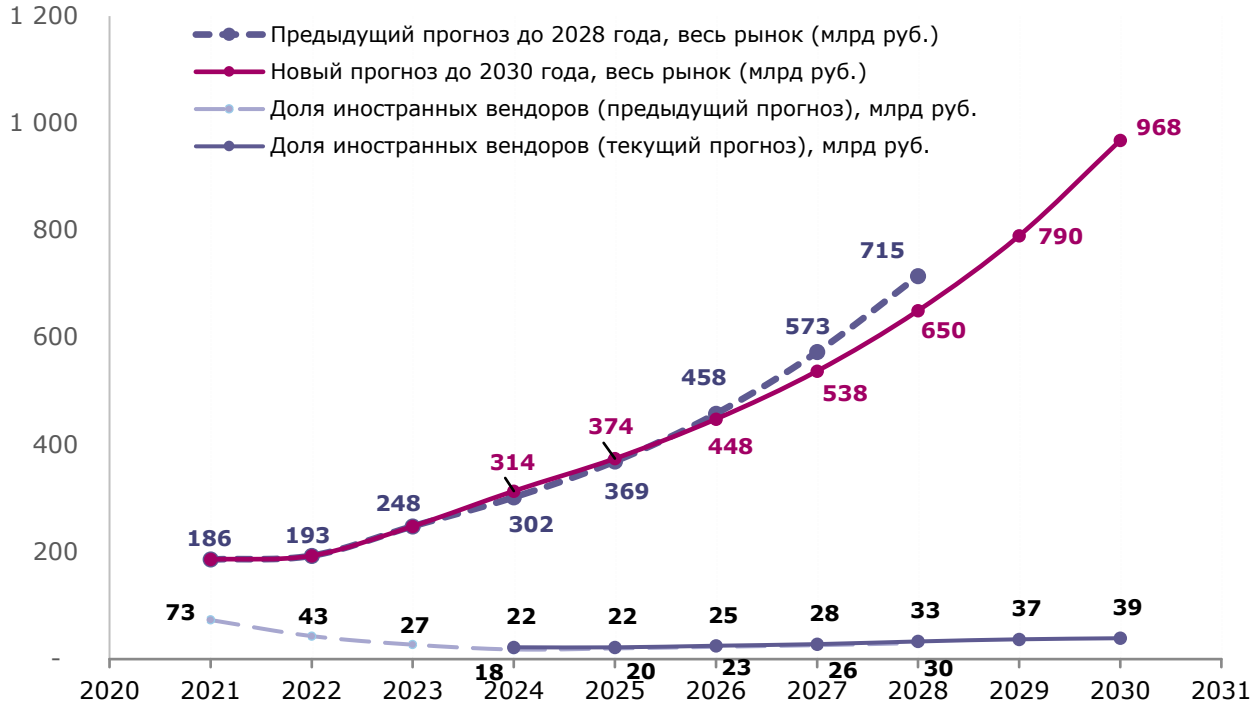
Далее следуют страны Латинской Америки и Ближнего Востока, которые набрали по 53,8%. Эти регионы рассматриваются как новые, но динамично растущие рынки, заинтересованные в альтернативных источниках технологий и партнёрстве с Россией. Наименее перспективным направлением респонденты назвали страны Африки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

В целом опрос показывает, что участники ожидают существенного расширение экспорта российских ИБ-решений после 2027 года. Основные усилия, по их мнению, должны быть сосредоточены на укреплении сотрудничества со странами СНГ, БРИКС, а также на развитии новых рынков в Латинской Америке и на Ближнем Востоке. Всё это отражает тенденцию к диверсификации экспортных направлений и переориентации на дружественные и развивающиеся страны.

Рыночные ожидания и прогноз до 2030

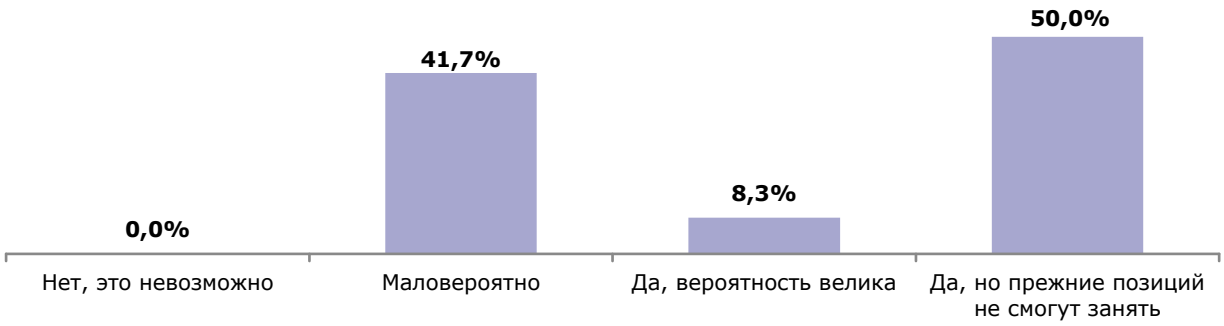
По результатам оценок объема рынка по итогам 2024 года, а также экспертной оценки влияния факторов был сформирован прогноз развития рынка на 2025–2030 годы. Данная оценка учитывает, в том числе, прогнозные темпы роста ВВП РФ (согласно текущему прогнозу Минэкономразвития России до 2028 года) с последующим восстановлением темпов роста сектора ИБ к 2030 году до 23%.

Диаграмма 10. Прогноз развития рынка ИБ до 2030 года



Согласно прогнозу с учетом экспертных оценок **к 2030 рынок может достичь 968 млрд рублей (CAGR 21%**). До 2030 года рынок информационной безопасности России сохранит устойчивый рост, опираясь на внутренний спрос и государственную политику технологического суверенитета. Согласно проведенному опросу 33,8% - такова доля уже установленных зарубежных решений в организациях к 2025 году. Импортозамещение не только в новых продажах, но и в инсталляционной базе остается одним из драйверов рынка в контексте обеспечения технологического суверенитета.

Диаграмма 11. Перспективы возвращения зарубежных вендоров на рынок РФ до 2030 года



В целом, перспективы возвращения иностранных игроков на российский рынок оцениваются либо как маловероятные (41,7% опрошенных), либо не вызывают опасений за лидирующие позиции отечественных вендоров (50% опрошенных). Таким образом, при сохранении курса на

технологический суверенитет, согласно прогнозу, ожидается, что доля продаж иностранных решений упадет до 4% от общего объема рынка к 2030 году.

Драйверы развития рынка кибербезопасности России

1. Главным драйвером продолжит выступать активная государственная политика, направленная на укрепление национальной безопасности и обеспечение технологического суверенитета. Кибербезопасность закреплена в стратегических документах России как ключевой элемент национальной устойчивости. Принятие «Концепции технологического развития до 2030 года» и включение ИБ в стратегию национальной безопасности способствовали формированию комплексной системы поддержки отечественных разработчиков, усилению программ импортозамещения и развитию суверенных ИТ-инфраструктур. Государство фактически определило кибербезопасность как приоритетную отрасль, обеспечивая ей институциональную и регуляторную поддержку.

2. Существенную поддержку отрасли обеспечивает сохранение налоговых льгот для российских ИТ- и ИБ-компаний. Продление нулевой ставки НДС на реализацию отечественного программного обеспечения, включенного в реестр Минцифры России, позволяет разработчикам сохранять конкурентоспособность на внутреннем рынке, направлять высвобожденные средства на развитие и удерживать квалифицированные кадры. Отказ от введения НДС с 2026 года подтвердил стратегическую значимость отрасли для государства и укрепил доверие бизнеса к долгосрочной политике в сфере технологического суверенитета.

3. Рост деструктивности кибератак в 2024–2025 годах стал еще одним мощным стимулом для развития рынка. Атаки на «Аэрофлот» и сеть «ВинЛаб» показали, что злоумышленники все чаще нацелены не на кражу данных, а на физическое разрушение ИТ-инфраструктуры и парализацию бизнес-процессов. Компании начали воспринимать кибербезопасность не как техническую функцию, а как стратегическую задачу, напрямую влияющую на устойчивость бизнеса. В результате растет спрос на решения по мониторингу и реагированию на инциденты, а также на услуги по киберстрахованию.

4. Важным фактором, стимулирующим рост рынка, является усиление требований регуляторов и повышение ответственности компаний за утечки данных. Введение в 2025 году оборотных штрафов в размере до 3% годового оборота за повторные инциденты заставляет бизнес пересматривать подходы к защите информации. Это активизировало спрос на современные системы защиты персональных данных, аудит безопасности и консалтинговые услуги. Таким образом, регуляторные меры становятся фактором повышения зрелости рынка, стимулируя внедрение более совершенных технологий и процессов.

5. Драйвером на рынке услуг продолжит выступать кадровый дефицит в сфере ИБ. Нехватка квалифицированных специалистов вынуждает компании все чаще обращаться к аутсорсинговым и сервисным моделям (MSSP и MDR). Рынок управляемых сервисов кибербезопасности растет особенно быстро: бизнес стремится делегировать функции мониторинга, реагирования и анализа угроз профессиональным поставщикам. Параллельно развивается практика краудсорсинговых услуг, таких как программы баг-баунти, которые получают поддержку со стороны государства и привлекают десятки тысяч независимых исследователей. Это расширяет охват тестирования и способствует повышению общей устойчивости цифровых сервисов.

6. Рост применения технологий искусственного интеллекта также стимулирует рынок кибербезопасности. С одной стороны, ИИ создает новые угрозы — от подмены обучающих данных до автоматизированных фишинговых атак. С другой — становится инструментом защиты, лежащим в основе новых интеллектуальных систем детектирования и реагирования.

Ограничители развития рынка

1. Основным ограничителем в 2024–2025 годах выступают экономические факторы, в том числе, ключевая ставка. Компании вынуждены оптимизировать бюджеты, сокращая расходы на ИБ-проекты, особенно капиталоемкие инфраструктурные инициативы. Рост страховых взносов для ИТ и общая макроэкономическая нестабильность также негативно влияют на темпы инвестиций, заставляя бизнес фокусироваться на выполнении обязательных требований, а не на проактивном развитии систем защиты.

2. Ограничивающим фактором становится усиление регулирования. Ужесточение критериев включения программного обеспечения в реестр отечественного ПО повысило требования к локализации, уровню технологий и независимости от иностранных компонентов. Хотя это способствует повышению качества решений, одновременно создает высокие барьеры входа для новых разработчиков и замедляет развитие инновационного бизнеса. Дополнительную озабоченность у отрасли вызвал законопроект о реестре ФСБ для «белых хакеров», предусматривающий явную аккредитацию специалистов и уголовную ответственность за нарушения при исследовании защищенности систем. По мнению экспертного сообщества, требуется доработать эту инициативу, чтобы избежать риска замедления развития исследовательской деятельности и практик краудсорсинговой кибербезопасности.

3. Одним из ограничителей остаются внешние санкции. Отечественные компании вынуждены концентрироваться на импортозамещении более недоступных зарубежных продуктов ИБ во внутреннем контуре страны, а возможности выхода российских вендоров на международные рынки ограничены внешней санкционной политикой и рисками. Это сужает экспортный потенциал отрасли, хотя в то же время стимулирует развитие сотрудничества с партнерами по ЕАЭС и дружественными государствами, где наблюдается постепенное формирование автономного киберпространства.

Приложение А. 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)

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

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