Октябрь 2024

Прогноз развития рынка кибербезопасности в Российской Федерации на 2024-2028 годы

ЦСР
ЦЕНТР СТРАТЕГИЧЕСКИХ РАЗРАБОТОК

Оглавление

Введение

Центр стратегических разработок (далее также ЦСР) продолжает ежегодную серию исследований рынка кибербезопасности Российской Федерации с формированием его прогноза на ближайшие пять лет.

В прошлогоднем исследовании оценка объемы рынка кибербезопасности по итогам 2022 года составила 193,3 млрд рублей.

Целью настоящего исследования является формирование оценки рынка кибербезопасности в России в 2023 году и уточненного прогноза его развития на перспективу ближайших 5 лет, выявление тенденций развития рынка, а также оценка процессов замещения зарубежных продуктов.

Исследование проводилось с апреля по сентябрь 2024 года на основе анализа открытых источников о выручке основных вендоров продуктов информационной безопасности за 2023 год, непосредственного опроса вендоров и дистрибьюторов — представителей основных игроков российского рынка. 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 на средствах защиты информации (СЗИ), услуги рассматриваются укрупненно.

В рамках исследования рассматривались следующие категории средств защиты информации (подробная декомпозиция представлена в приложении А):

- средства защиты инфраструктуры (infrastructure security);
- средства защиты сетей (network security);
- средства защиты приложений (application security);
- средства защиты данных (data security);
- средства защиты пользователей (user security);
- средства защиты «конечных точек» (endpoint security).

Результаты исследования структурированы следующим образом:

- оценка рынка кибербезопасности по результатам 2023 года;
- прогноз развития рынка на 5 лет (2024–2028 гг.).

ЦСР выражает благодарность всем участникам опроса за предоставленные сведения.

Оценка рынка кибербезопасности по результатам 2023 года

Оценка общего объема рынка по результатам 2023 года

В 2023 году продолжилась интенсивная атака на информационную инфраструктуру российских организаций. За 2023 год число подозрений на инцидент в информационной безопасности (ИБ) увеличилось более чем на 60% до 1,5 млн событий ИБ, при этом доля подтвержденных инцидентов снизилась до 2%, но в абсолютных цифрах сопоставима с итогами 2022 года[1]. Количество DDoS-атак на российские организации в 2023 году по сравнению с 2022 годом снизилось почти в 3 раза[2], но их количество остается достаточно высоким. Кроме того, растет число инцидентов, связанных с утечкой персональных данных – более 80% утечек связано с кибератаками[3]. В отечественных компаниях продолжается процесс импортозамещения, подстегиваемый как нормами российского законодательства и требованиями регуляторов, так и ростом зрелости российских вендоров.

Рынок кибербезопасности Российской Федерации по результатам 2023 года оценивается в 248,5 млрд рублей[4], прирост общего объема рынка кибербезопасности (продукты и услуги) по сравнению с 2022 годом составил на 28,5%.

248,5 млрд рублей **28,5%**

Объем российского рынка кибербезопасности по итогам 2023 года и его прирост

Соотношение поставок СЗИ и услуг, как и в предыдущие годы, почти не изменилось.

В 2023 году совокупная доля услуг составила 27% (26% по итогам 2022 года) всего объема рынка, **а средств защиты информации – 73%** (74% по итогам 2022 года).

Диаграмма 1. Совокупная доля услуг и поставок средств защиты информации

[1] *https://rt-solar.ru/upload/iblock/1ea/i1809ydgf4yy1c1ncyau6l5oog2o6svf/Otchet-obshchiy-2023.pdf*
[2] *https://rt-solar.ru/upload/iblock/b26/19a69b1ur99t3ouey0iak7cflzziw6d1/Otchet-ob-atakakh-na-onlayn_resursy-rossiyskikh-kompaniy-v-2023-godu_new_.pdf*
[3] *https://www.infowatch.ru/analytics/analitika/issledovaniye-utechek-informatsii-v-mire-za-posledniye-dva-goda*
[4] *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.*

На российском рынке кибербезопасности в 2023 году сохраняется тенденция снижения доли присутствия зарубежных вендоров, продолжает усиливаться доминирующее положение российских компаний: они занимают уже 89% рынка продаж СЗИ (в 2022 году – 70%).

По итогам 2023 года иностранные решения в совокупных затратах все еще занимают весомую часть рынка – 11% (в 2022 году – 30%)[5].

Диаграмма 2. Доля российских и зарубежных вендоров средств защиты информации

Стоит отметить, что в прошлогоднем прогнозе ожидалось более существенное снижение доли закупки зарубежных продуктов на российском рынке - до 5%. Замедление темпов вытеснения зарубежных продуктов российскими обуславливается следующими причинами:

- Не все зарубежные вендоры покинули отечественный рынок (в частности, на российском рынке официально присутствует Check Point Software Technologies).
- На объем рынка влияет рост стоимости содержания зарубежных продуктов.
- В отдельных классах продуктов возникают проблемы подбора отечественных аналогов, в частности такую проблему озвучивают в сфере импортозамещения многофункциональных межсетевых экранов – 64% респондентов считают, что на рынке пока нет решений, способных полнофункционально заменить продукты ушедших зарубежных вендоров[6].

Кроме того, у компаний остаются сложности с импортозамещением установленных ранее решений. Несмотря на то, что на подавляющее большинство зарубежных продуктов уже имеются российские аналоги (более 84% зарубежных решений на объектах критической информационной инфраструктуры (КИИ) могут быть заменены отечественными аналогами), их значительный объем потребует больше времени на обновление. В частности, по данным «К2 Кибербезопасность» к 01 января 2025 года всего 41% [7] средних и крупных компаний, у которых имеются объекты критической информационной инфраструктуры, успеют перейти на российские разработки.

5 При определении доли зарубежных решений в общем объеме рынка учитывались, в том числе, поставки через «параллельный импорт».
[6] https://www.cnews.ru/news/line/2024-07-10_mts_red_svyshe_60_zakazchikov
[7] https://ict.moscow/news/k2-kiberbezopasnost-59-srednikh-i-krupnykh-kompanii-s-kii-ne-smogut-importozamestit-zarubezhnye-ib-resheniia/

По итогам 2023 года состав топ-30 лидеров рынка кибербезопасности из числа вендоров выглядит следующим образом:

1. **Лаборатория Касперского**
2. **Positive Technologies**
3. **BI.ZONE**
4. **ГК Солар**
5. **ИнфоТеКС**
6. **Код Безопасности**
7. **UserGate**
8. **Check Point Software Technologies**
9. **Крипто-Про**
10. **Fortinet**
11. **Search Inform**
12. **Гарда Технологии**
13. **Cisco**
14. **Актив-Софт**
15. **Фактор-ТС**
16. **Infowatch**
17. **IBM**
18. **Security Vision**
19. **F.A.C.C.T.**
20. **Киберпроект**
21. **Rvision**
22. **S-Terra**
23. **Амикон**
24. **Qrator Labs**
25. **Атлас-Карт**
26. **АйТи Бастион**
27. **DrWeb**
28. **Аладдин Р.Д**
29. **Palo Alto Networks**
30. **ЦБИ**

Лидерами рынка, с заметным отрывом от остальных участников, являются Лаборатория Касперского и Positive Technologies.

К крупным игрокам на российском рынке кибербезопасности следует отнести BI.ZONE, ГК Солар, ИнфоТеКС, Код Безопасности и UserGate. В совокупности, все обозначенные крупные игроки покрывают более половины отечественного рынка кибербезопасности.

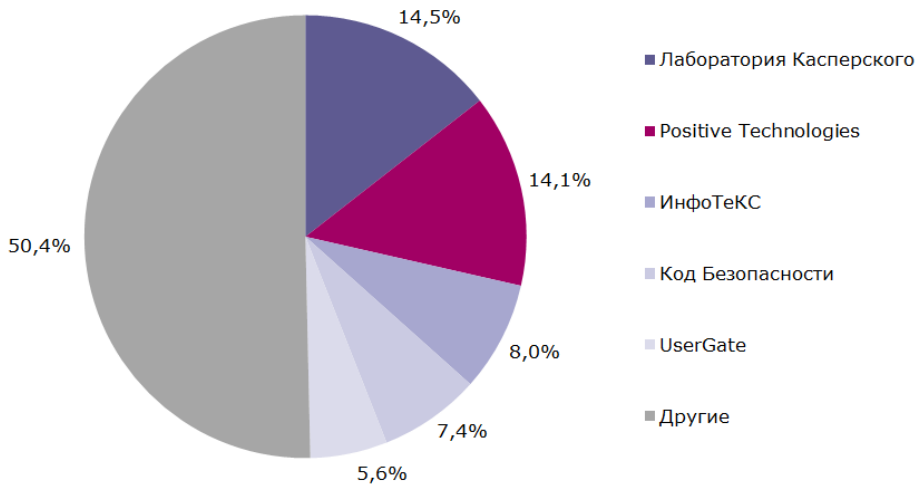
Оценка рынка СЗИ по результатам 2023 года

В топ-5 вендоров СЗИ по выручке в 2023 году вошли только российские компании.

Таблица 1. Топ-5 вендоров средств защиты информации по выручке в 2023 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 2023 года

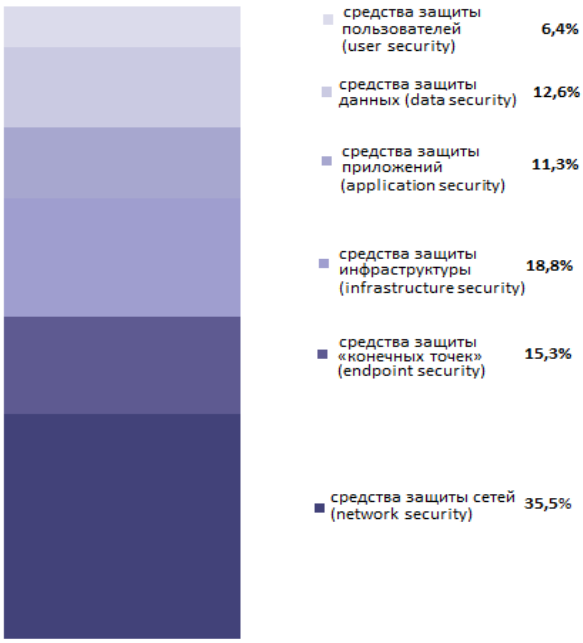


Необходимо отметить, что доля на рынке СЗИ вендора Лаборатория Касперского постепенно снижается (**-1,5%**), а доля Positive Technologies активно растет (**+1,7%**).

На следующем графике приведено долевое распределение следующих предлагаемых на рынке в 2023 году категорий средств защиты информации:

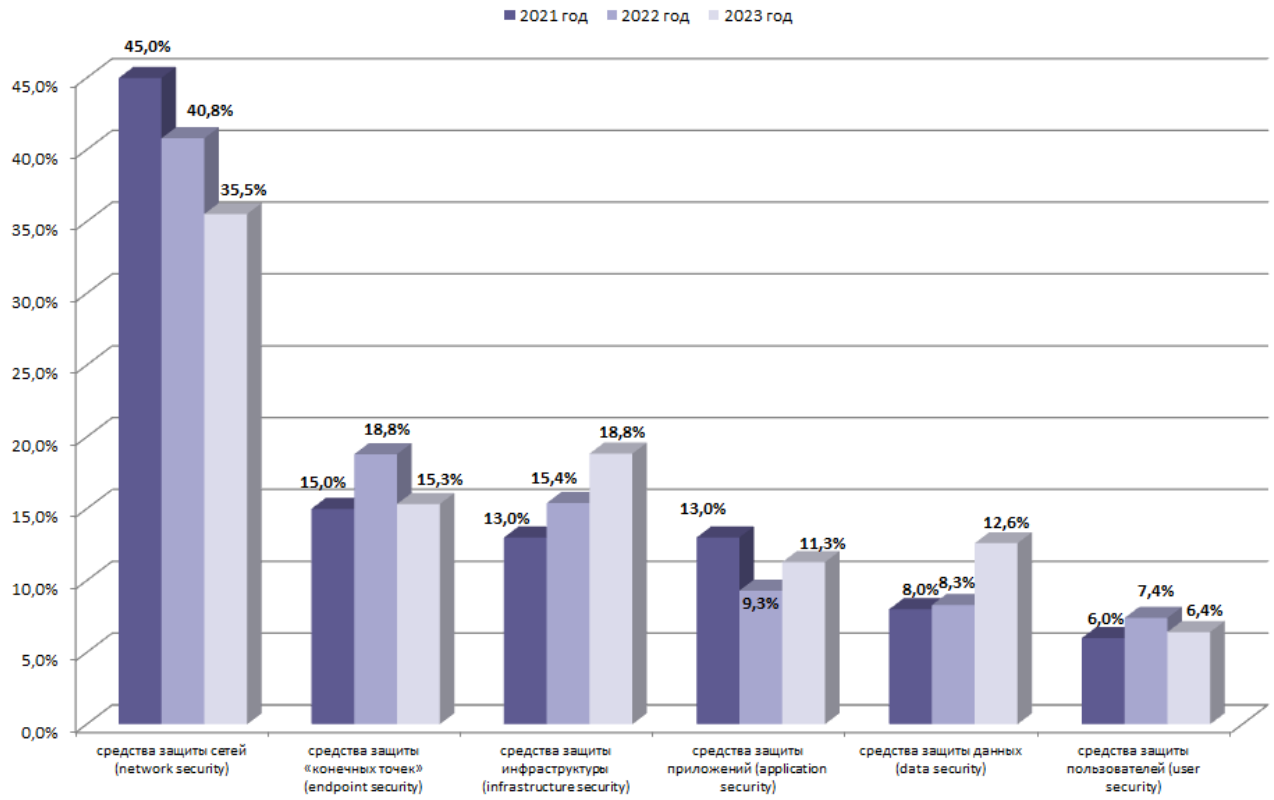
- средства защиты инфраструктуры (infrastructure security);
- средства защиты сетей (network security);
- средства защиты приложений (application security);
- средства защиты данных (data security);
- средства защиты пользователей (user security);
- средства защиты «конечных точек» (endpoint security).

Диаграмма 4. Долевое распределение категорий средств защиты информации по результатам 2023 года



В ретроспективе, на протяжении трехлетнего периода наблюдения, отмечается тенденция снижения доли средств защиты сетей и роста доли средств защиты инфраструктуры, также можно отметить зарождающуюся тенденцию роста доли средств защиты данных.

Диаграмма 5. Долевое распределение категорий средств защиты информации в 2021-2023 годах



Снижение доли рынка в сегменте средств защиты сетей в 2023 году обуславливается возрастающими требованиями со стороны регулятора по переходу на отечественные продукты с одной стороны и, с другой стороны, ожиданиями заказчика появления на рынка зрелого отечественного продукта в области межсетевых экранов нового поколения (NGFW), обеспечивающего замену импортных аналогов как по функциональности, так и по скорости обработки трафика.

Снижение доли рынка в сегменте средств защиты «конечных точек» в 2023 году обусловлен общим насыщением рынка - снижением спроса со стороны заказчиков ввиду покрытия потребности.

Рост числа атак на российские организации, мотивированные не только финансовой составляющей, смещение фокуса атак с количественного аспекта на качественную подготовку, вынуждают заказчиков более внимательно относиться к защите информационной инфраструктуры, выстраиванию процесса обнаружения и реагирования на угрозы, что, в свою очередь, приводит к покрытию потребности в таких продуктах, как средства мониторинга и отражения кибератак (SIEM, SOAR, XDR и прочие). Фактически потребители на российском рынке постепенно перестраиваются и переходят к внедрению проактивной кибербезопасности. Высокий уровень зрелости российских продуктов на рынке в сегменте средств защиты инфраструктуры предопределил возможность заказчиков быстро и безболезненно осуществить миграцию с зарубежных продуктов, что и обуславливает активный рост доли сегмента на протяжении нескольких лет.

Также растет доля сегмента средств защиты приложений, что обусловлено следующими факторами:

- Активный рост зрелости команд разработчиков приложений приводит к активному вовлечению в методологию непрерывной разработки программного обеспечения аспектов информационной безопасности (DevSecOps), обеспечение защиты приложений. Также оказывает влияние и фактор роста числа атак на веб-приложения – ответственные заказчики, оценивая риски, переориентируются на безопасные приложения.
- Существенное влияние оказывают на сегмент и требования регуляторов по безопасной разработке (в частности, требования ФСТЭК для субъектов КИИ, требования Банка России к финансовым организациям и т.п.).
- Регуляторы уделяют все более значительное внимание процессу управления уязвимостями в информационных системах, мотивируя компании автоматизировать соответствующие процессы и процедуры, что стимулирует потребность в соответствующих продуктах.

Увеличение числа инцидентов по утечке персональных данных приводит к повышению внимания со стороны регулятора и организации качественного усиления защиты персональных данных, в частности, к повышению ответственности операторов персональных данных (введение оборотных штрафов, требования об обязательном уведомлении о любых инцидентах с персональными данными).

Доля сегмента средств защиты пользователей остается относительно стабильной и не подвержена значительным изменениям, существенной волатильности не наблюдается.

Таблица 2. Топ-5 вендоров в разрезе категорий средств защиты информации по итогам 2023 года

Позиция	Вендор	Юрисдикция
	Средства защиты сетей (network security)	
1	UserGate	РФ
2	Check Point Software Technologies	Иностранная
3	Positive Technologies	РФ
4	Код Безопасности	РФ
5	ИнфоТеКС	РФ
	Средства защиты «конечных точек» (endpoint security)	
1	Лаборатория Касперского	РФ
2	DrWeb	РФ
3	Positive Technologies	РФ
4	ESET	Иностранная
5	Крипто-Про	РФ
	Средства защиты инфраструктуры (infrastructure security)	
1	Positive Technologies	РФ
2	Лаборатория Касперского	РФ
3	Security Vision	РФ
4	IBM	Иностранная
5	Rvision	РФ

	Средства защиты приложений (application security)	
1	**Positive Technologies**	**РФ**
2	**ГК Солар**	**РФ**
3	**BI.ZONE**	**РФ**
4	**Гарда Технологии**	**РФ**
5	**СолидСофт**	**РФ**
	Средства защиты данных (data security)	
1	**Infowatch**	**РФ**
2	**Гарда Технологии**	**РФ**
3	**ИнфоТеКС**	**РФ**
4	**Киберпроект**	**РФ**
5	**ГК Солар**	**РФ**
	Средства защиты пользователей (user security)	
1	**Актив-Софт**	**РФ**
2	**Аладдин Р.Д.**	**РФ**
3	**Крипто-Про**	**РФ**
4	**АйТи Бастион**	**РФ**
5	**Конфидент**	**РФ**

Рынок СЗИ Российской Федерации в 2023 году продолжил расти и составил 182,6 млрд рублей с совокупным приростом к значениям 2022 года на 27,6%. Данные показатели значительно превышают рост мирового рынка, который составляет 15,6%[8].

Можно сделать вывод, что российский рынок продуктов кибербезопасности продолжает активно развиваться, при этом наблюдаются существенные темпы замещения зарубежных продуктов.

182,6 млрд рублей **27,6%**

Объем российского рынка СЗИ по итогам 2023 года и его прирост относительно 2022 года

[8] *https://www.itbestsellers.ru/companies-analytics/detail.php?ID=56368*

Декомпозиция объемов долей рынка и расчетных значений прироста за 2023 год по категориям рассмотренных ранее средств защиты приведена в Таблице 3.

Таблица 3. Декомпозиция объемов долей рынка и расчетных значений прироста за 2023 год по категориям рассмотренных ранее средств защиты

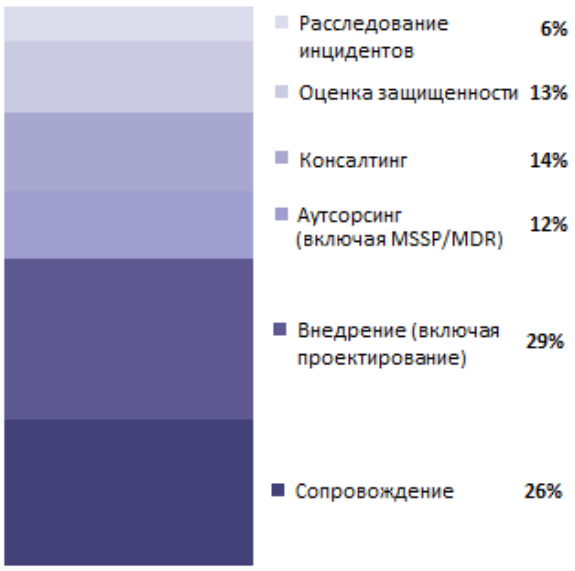
Категории средств защиты	Доля рынка (%)	Объем доли рынка (млрд. руб.)	Прирост (%)
Средства защиты сетей (network security)	35,5 %	64,9	11,1 %
Средства защиты «конечных точек» (endpoint security)	15,3 %	28,0	4,1 %
Средства защиты инфраструктуры (infrastructure security)	18,8 %	34,4	56,1 %
Средства защиты приложений (application security)	11,3 %	20,6	54,8 %
Средства защиты данных (data security)	12,6 %	23,0	93,8 %
Средства защиты пользователей (user security)	6,4 %	11,7	10,7 %
Итого		**182,6**	**27,6%**

Оценка рынка услуг по результатам 2023 года

Долевое распределение предлагаемых на рынке в 2023 году категорий услуг в области обеспечения кибербезопасности:

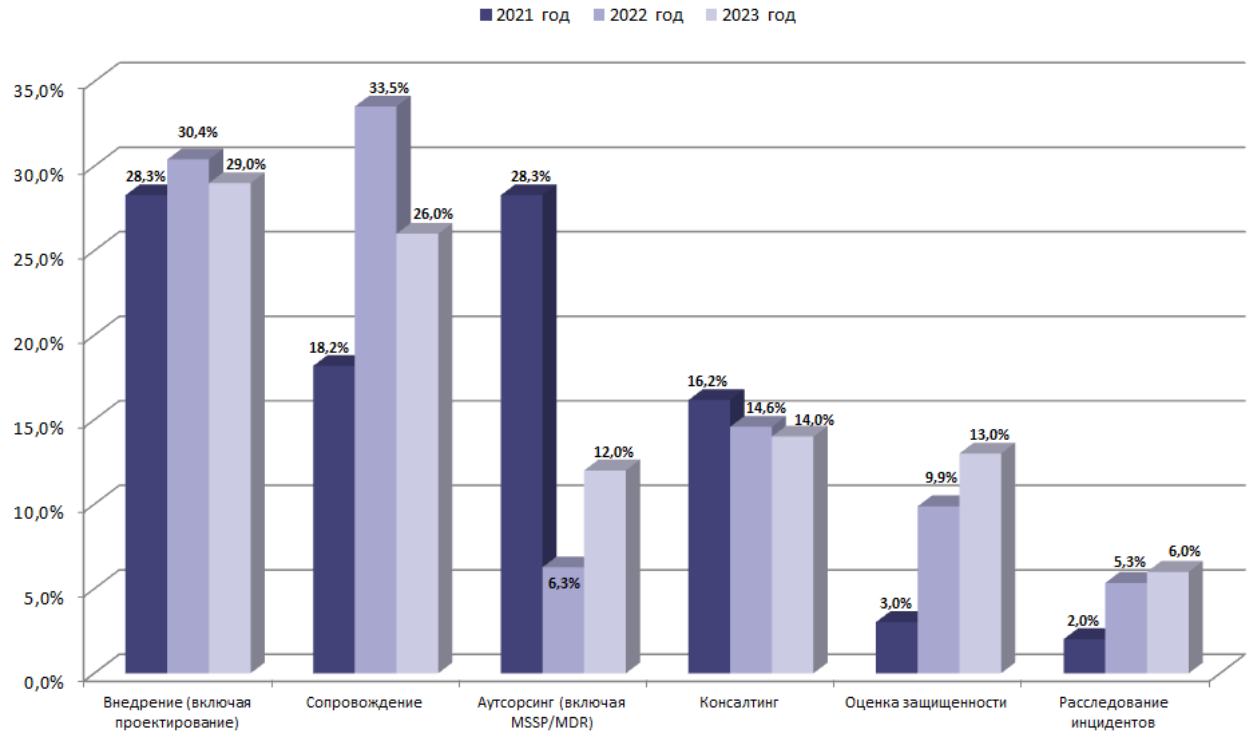
- внедрение, включая подготовительные этапы, проектирование и сопровождение (обеспечение жизненного цикла средств защиты);
- консалтинг, включая оценку защищенности информационных ресурсов и расследование инцидентов информационной безопасности;
- аутсорсинг, включая управление средствами защиты, выявление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

Диаграмма 6. Долевое распределение услуг ИБ по результатам 2023 года



В ретроспективе, на протяжении трехлетнего периода наблюдения, отмечается тенденция существенного роста доли услуг по оценке защищенности, расследования инцидентов и постепенного снижения доли услуг консалтинга.

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



Топ-5 вендоров на рынке услуг информационной безопасности в 2023 году:

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

При этом на рынке услуг сильные позиции у интеграторов решений. Учитывая это, к лидерам рынка оказания услуг информационной безопасности в 2023 году можно отнести:

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

Объем рынка услуг по итогам 2023 года составил 65,9 млрд руб. с приростом в 31,1%. Рынок услуг в области кибербезопасности также растет значительными темпами.

65,9 млрд рублей **31,1%**

Объем российского рынка СЗИ по итогам 2023 года и его прирост

Рыночные ожидания и прогноз до 2028 года

Основные тенденции рынка кибербезопасности

В текущем 2024 году интенсивность кибератак по сравнению с 2023 годом нарастает[9], при этом кибератаки смещаются с массовых атак на точечные, подготовленные, т.е. кибератаки качественно меняются.

Также в 2024 году продолжается развитие тенденций на нормативное регулирование требований к информационной безопасности и повышению ответственности, в том числе и требований по импортозамещению. Так, согласно Постановления Правительства Российской Федерации №1912 от 14 ноября 2023 года ужесточаются требования по импортозамещению в части перехода на доверенные программно-аппаратные комплексы (ПАК). Требования по переходу на отечественное программное обеспечение касаются не только субъектов КИИ, но и распространяются на госкорпорации и компании с государственным участием[10].

Государство продолжает активное стимулирование развития отрасли. Как итог, на рынке кибербезопасности появляются компании-новички (ИБ-стартапы), которые по различным оценкам занимают до 30% отечественного рынка ИБ[11].

Кроме того, стоит отметить активно зарождающиеся тренды российского рынка информационной безопасности, которые на текущем этапе еще не переросли в факторы, влияющие на рынок ИБ, но могут повлиять на него в будущем:

1. Рост применения рынком методик Bug Bounty - поиска уязвимостей за вознаграждение.
2. Применение квантовых технологий и технологий искусственного интеллекта в кибербезопасности.
3. Усиление запроса со стороны компаний-потребителей решений на понятный и измеримый результат работы решений кибербезопасности.

Вместе с тем, в 2024 году наблюдается снижение темпов роста рынка (отсутствует ожидаемый пик), наблюдается их органическое перераспределение на будущие периоды - в 2025 году и далее. Такое поведение рынка связано с рядом факторов, а именно:

- ожиданием смягчения требований по резкому переходу на применение отечественных решений и предоставлением дополнительного времени на такой переход;
- ростом ключевой ставки и, как следствие, вынужденной приоритезацией затрат компаниями-потребителями решений;
- попыткой компаний-потребителей решений обеспечивать свои потребности путем организации внутренней разработки (доработки и адаптации) для сохранения выручки и сокращения издержек.

---

[9] *https://rt-solar.ru/upload/iblock/ea1/c5cpl3rj2d3vzbvw8hsxbxf3644q374d/Kiberataki_na_rossiyskie_kompanii_vo_IIkvartale_iIpolugodii2024-_1_.pdf*
[10] *https://digital.gov.ru/ru/documents/7342/*
[11] *https://tass.ru/ekonomika/21276683*

В текущем году при формировании прогноза рынка кибербезопасности учитывались следующие укрупненные факторы:

1. Киберугрозы: продолжающийся рост числа кибератак на органы власти, бизнес, финансовые организации и промышленные объекты экономики России, а также их качественные изменения.
2. Ограничение и сложности поставок продуктов зарубежных вендоров.
3. Ужесточение ответственности первых лиц организаций за обеспечение информационной безопасности.
4. Ограничение применения зарубежного ПО на объектах КИИ, в госкорпорациях и компаниях с государственным участием.
5. Активное стимулирование государством развития отрасли (выделение субсидий, грантов, налоговые и прочие льготы, дополнительные программы обучения и т.п.).
6. Ужесточение требований регуляторов, предъявляемых к заказчикам ИБ.

На основе опроса участников рынка была проведена оценка влияния указанных факторов на рынок по годам.

Таблица 4. Оценка влияния факторов на рост рынка кибербезопасности

Фактор	2024	2025	2026	2027	2028
Рост числа кибератак	**3,0 %**	**3,0 %**	**3,0 %**	**3,0 %**	**3,0 %**
Уход зарубежных вендоров	**3,0 %**	**3,0 %**	**3,5 %**	**3,1 %**	**3,0 %**
Санкции и связанные с ними ограничения	**0,0 %**	**0,0 %**	**0,0 %**	**0,0 %**	**0,0 %**
Ответственность первых лиц организаций за обеспечение ИБ	**3,0 %**	**4,0%**	**4,0 %**	**4,0 %**	**4,0 %**
Запрет зарубежного ПО на объектах КИИ	**3,0 %**	**3,0 %**	**4,0 %**	**5,0 %**	**5,0 %**
Финансовые меры поддержки	**3,7 %**	**3,6 %**	**3,8 %**	**3,7 %**	**4,1 %**
Нефинансовые меры поддержки	**2,3 %**	**2,4 %**	**2,5 %**	**2,6 %**	**2,8 %**
Ужесточение требований к ИБ	**3,4 %**	**3,2 %**	**3,5 %**	**3,6 %**	**3,7%**
Итоговый рост рынка (год к году)	**21,4 %**	**22,3 %**	**24,3 %**	**25,0 %**	**24,8 %**

Стоит отметить, что по текущим средневзвешенным оценкам экспертного сообщества ни один фактор не был отмечен как отрицательно влияющий на рынок, в прошлом исследовании к таким факторам были отнесены «санкции и связанные с ними ограничения» и «ужесточение требований к ИБ». При этом по фактору «санкции и связанные с ними ограничения» мнения экспертов по отнесению вектора влияния фактора на рынок разделились поровну среди респондентов, средневзвешенная оценка близка к балансу, поэтому влияние этого фактора оценено как 0.

Прогноз объема рынка на 2024-2028 годы

По результатам оценок объема рынка по итогам 2023 года, а также экспертной оценки влияния факторов сформирован прогноз развития рынка на 2024–2028 годы.

Диаграмма 8. Прогноз развития рынка кибербезопасности России, млрд руб.

На графике представлен обновленный прогноз на 2024-2028 годы рынка кибербезопасности России и ранее подготовленный прогноз развития рынка на 2023-2027 годы.

Можно видеть снижение темпов импортозамещения продуктов информационной безопасности по сравнению с прошлогодними оценками (бордовая линия на графике), однако в долевом соотношении сценарий импортозамещения продолжает активно реализовываться. По итогам 2023 года доля зарубежных продуктов в совокупном объеме рынка кибербезопасности составляет 11% и к 2028 году прогнозируется ее снижение до 4,2%. Ожидается, что доля зарубежных вендоров на отечественном рынке стабилизируется в районе 4-5% за счет продуктов вендоров, которые предпочли остаться на российском рынке (в частности, Check Point Software Technologies) и вендоров из «дружественных» стран, планирующих вывод своих продуктов на российский рынок (в частности, из Китая, Индии, Ирана и т.д.).

Стремительный рост рынка продолжится на протяжении всего прогнозного периода с ежегодным приростом 20-25%.

Выводы

Российский рынок кибербезопасности продолжает активно расти, причем темпами, значительно опережающими рост мирового рынка ИБ.

Рост объема рынка кибербезопасности в России в следующие 5 лет ожидается со среднегодовым темпом прироста в 23,6%.

К 2028 году рынок достигнет 715 млрд рублей, на долю российских вендоров будет приходиться более 95% всего объема рынка.

715 млрд рублей **23,6%**

Прогнозный объем российского рынка ИБ в 2028 году и его темп прироста

По итогам 2023 обозначились два лидера рынка СЗИ, которые занимают схожие доли рынка и идут с заметным отрывом от остальных участников, Лаборатория Касперского и Positive Technologies.

На рынке не выявлено ни одной группы средств защиты информации, где бы лидерство фиксировалось за зарубежными вендорами.

Авторы

Екатерина Кваша
Заместитель генерального директора

Владимир Тютрин
Заместитель директора
центра цифрового развития

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 (ICS) security
Платформы реагирования на инциденты	Incident Response Platform (IRP)
Платформы управления рисками	Governance, Risk and Compliance (GRC)
Средства защиты сетей	**network security**
Межсетевые экраны (в т.ч. «нового поколения»)	(Next Generation) Firewall (FW, NGFW)
Многофункциональные решения	Unified Threat Management (UTM)
Системы обнаружения/предотвращения вторжений	Intrusion Detection/Prevention System (IDS/IPS)
Системы анализа трафика	Network Traffic Analysis (NTA)
Средства контроля доступа к сети	Network Access Control (NAC)
Средства защиты от сложных и неизвестных киберугроз	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 защиты пользователей	**user security**
Средства управления идентификацией, аутентификацией и контролем доступа	Identity & Access Management/Governance & Administration (IAM/IGA)
Средства контроля привилегированных пользователей	Privileged Access Management (PAM)
Средства криптографической защиты информации пользователей (в т.ч. средства электронной подписи)	Public Key Infrastructure (PKI)
Средства защиты станций / «конечных точек»	**endpoint security**
Антивирусная защита	Antivirus Protection (AVP)
Системы обнаружения и реагирования на угрозы на рабочих станциях пользователей («конечных точках»)	Endpoint Detection and Response (EDR)

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