Прогноз развития рынка кибербезопасности в Российской Федерации на 2022–2026 годы

Август 2022

ЦСР

Содержание

Введение

Необходимость обеспечения информационной безопасности ИТ-ресурсов (ИБ, кибербезопасность) организаций Российской Федерации (РФ) сформировала за последние 25 лет отечественный рынок кибербезопасности, включающий в себя разработку и реализацию средств защиты информации и услуг в области обеспечения информационной безопасности.

В связи с существенно изменившейся в начале 2022 года геополитической обстановкой, повлекшей массовый уход западных производителей (вендоров) средств защиты информации и комплексных решений на их основе с отечественного рынка, предполагается значительное перераспределение долей рынка в перспективе ближайших пяти лет. Также на рынок кибербезопасности большое влияние оказывают инициативы регуляторов и правительства в части «импортозамещения» (обеспечения технологической независимости) технических решений, связанных с необходимостью обеспечения безопасного функционирования объектов критической информационной инфраструктуры (КИИ). Существенным фактором достижения целей технологической независимости является производство современной микроэлектроники, которое в контексте данного исследования не рассматривается.

Целью данного исследования является формирование прогноза развития рынка кибербезопасности (за исключением сегмента B2C, business-to-consumer) до 2026 года включительно, а также оценка перспектив его развития силами отечественных производителей средств защиты информации.

Перспективы развития рынка услуг в области обеспечения информационной безопасности, в силу сложности оценки и значительно меньшей по сравнению с сегментом средств защиты долей рынка кибербезопасности, детально в настоящем исследовании не рассматриваются.

Исследование проводилось в период с апреля по июль 2022 года в форме анализа сведений из открытых источников об официальной выручке компаний за 2021 год и данных с торговых площадок по продуктам анализируемых вендоров, а также данных от дистрибьюторов средств защиты информации.

В рамках исследования рассматривались следующие категории 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);
- защита рабочих станций/«конечных точек» (endpoint security).

Их декомпозиция в данном исследовании приведена в **Таблице 1**.

Аналитические результаты исследования структурированы следующим образом:
- оценка рынка кибербезопасности по результатам 2021 года;
- рыночные ожидания 2022 года и прогноз до 2026 года.

Таблица 1. Декомпозиция категорий средств защиты информации

Категории средств защиты	Англоязычный синоним (устойчивое сокращение)
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
Платформа реагирования на инциденты	Incident Response Platform (IRP)
Платформа 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	Vulnerability 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)
Защита рабочих 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)

Оценка рынка кибербезопасности по результатам 2021 года

Рынок кибербезопасности Российской Федерации по результатам 2021 года оценивается в **185,9 млрд руб**.[1] При этом совокупная доля услуг составляет **27 %** всего объема рынка, а поставки средств защиты информации, в том числе программных, — **73 %**.

Рисунок 1. Совокупная доля услуг и поставок средств защиты информации по результатам 2021 года

73 % **27 %**

Средства защиты информации Услуги

На отечественном рынке 2021 года доминируют российские вендоры средств защиты информации: они занимают **61 %** рынка, тогда как зарубежные — **39 %**.

Рисунок 2. Доля российских и зарубежных вендоров средств защиты по результатам 2021 года

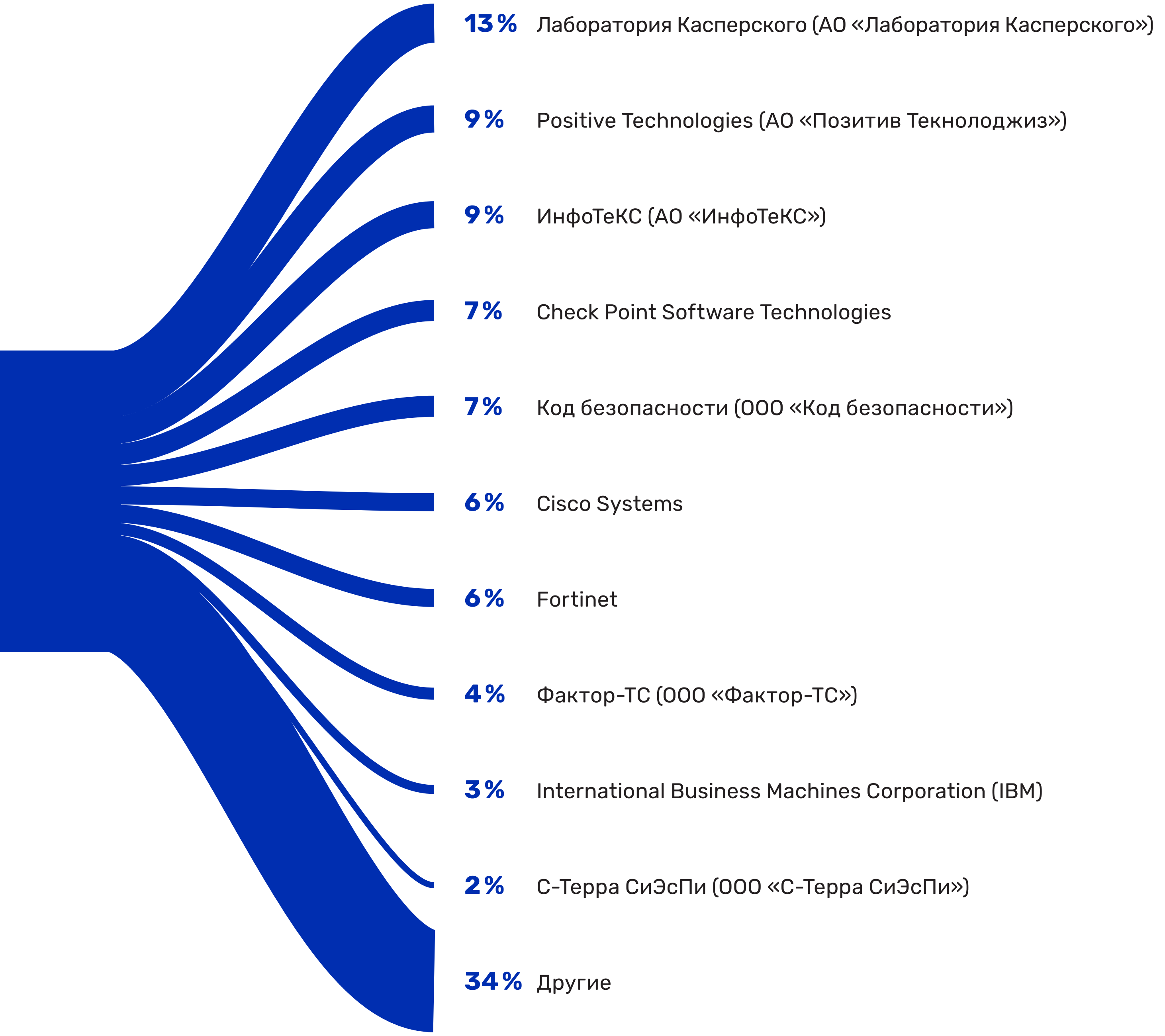
61 % **39 %**

Российские вендоры Зарубежные вендоры

1 Данные взяты 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 интеграторам, оказывающим услуги. Учитывалось, что выручка вендора не обязательно равна его присутствию на рынке в связи с партнерской скидкой дистрибьютора/интегратора

Процентное соотношение вендоров средств защиты информации на рынке в 2021 году представлено на графике ниже.

Рисунок 3. Доли вендоров средств защиты на рынке по результатам 2021 года



На следующем графике приведено долевое распределение следующих предлагаемых на рынке в 2021 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);
- защита рабочих станций/«конечных точек» (endpoint security).

Рисунок 4. Долевое распределение категорий средств защиты информации по результатам 2021 года

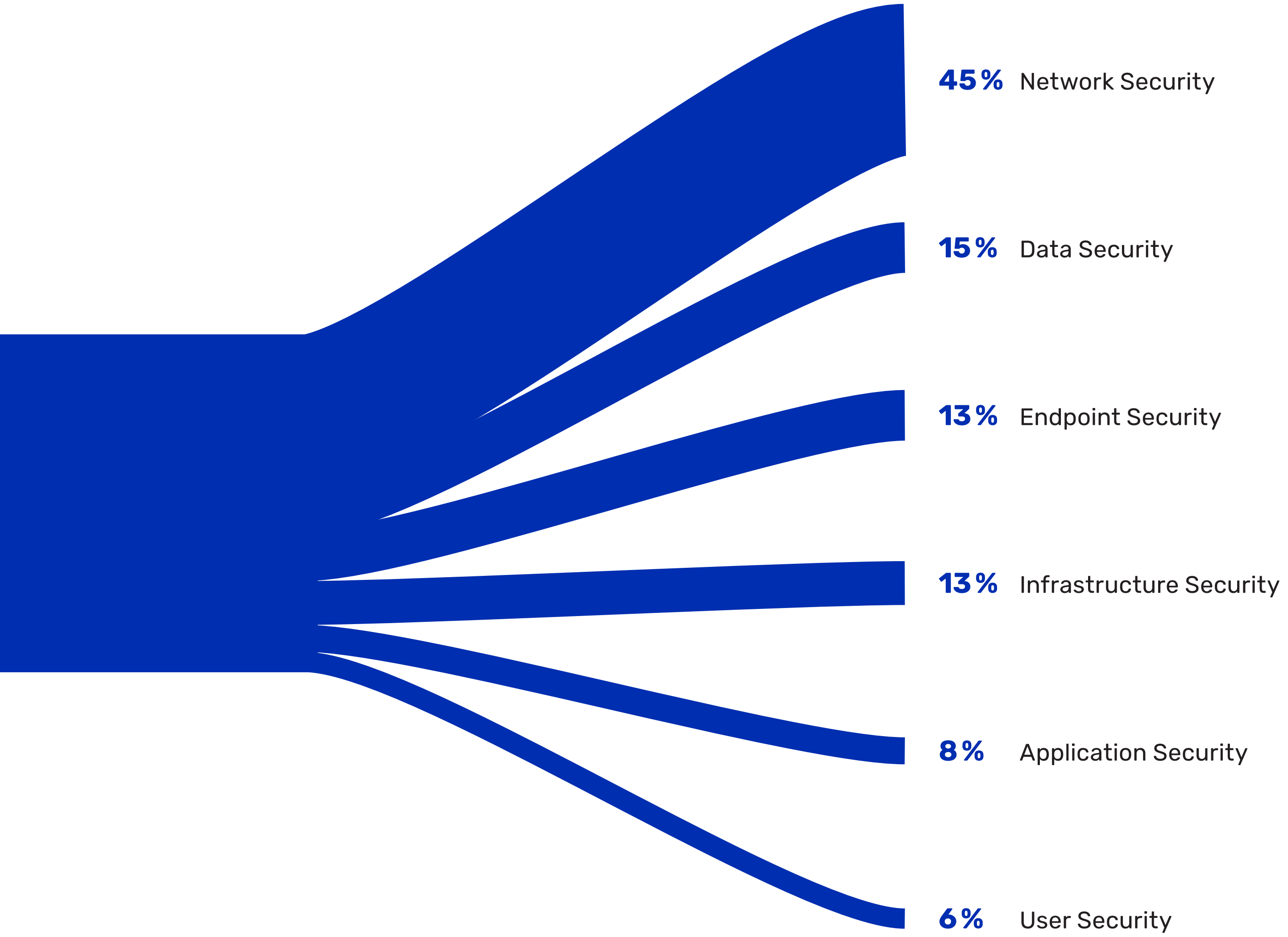


Таблица 2. Топ-10 вендоров средств защиты информации по выручке в 2021 году (т.е. без учета услуг)

Позиция	Вендор	Юрисдикция	Доля рынка
1	Лаборатория Касперского (АО «Лаборатория Касперского»)	РФ	13 %
2	Positive Technologies (АО «Позитив Текнолоджиз»)	РФ	9 %
3	ИнфоТеКС (АО «ИнфоТеКС»)	РФ	9 %
4	Check Point Software Technologies	Иностранная	7 %
5	Код безопасности (ООО «Код безопасности»)	РФ	7 %
6	Fortinet	Иностранная	6 %
7	Cisco Systems	Иностранная	6 %
8	International Business Machines Corporation (IBM)	Иностранная	4 %
9	Фактор-ТС (ООО «Фактор-ТС»)	РФ	4 %
10	С-Терра СиЭсПи (ООО «С-Терра СиЭсПи»)	РФ	2 %

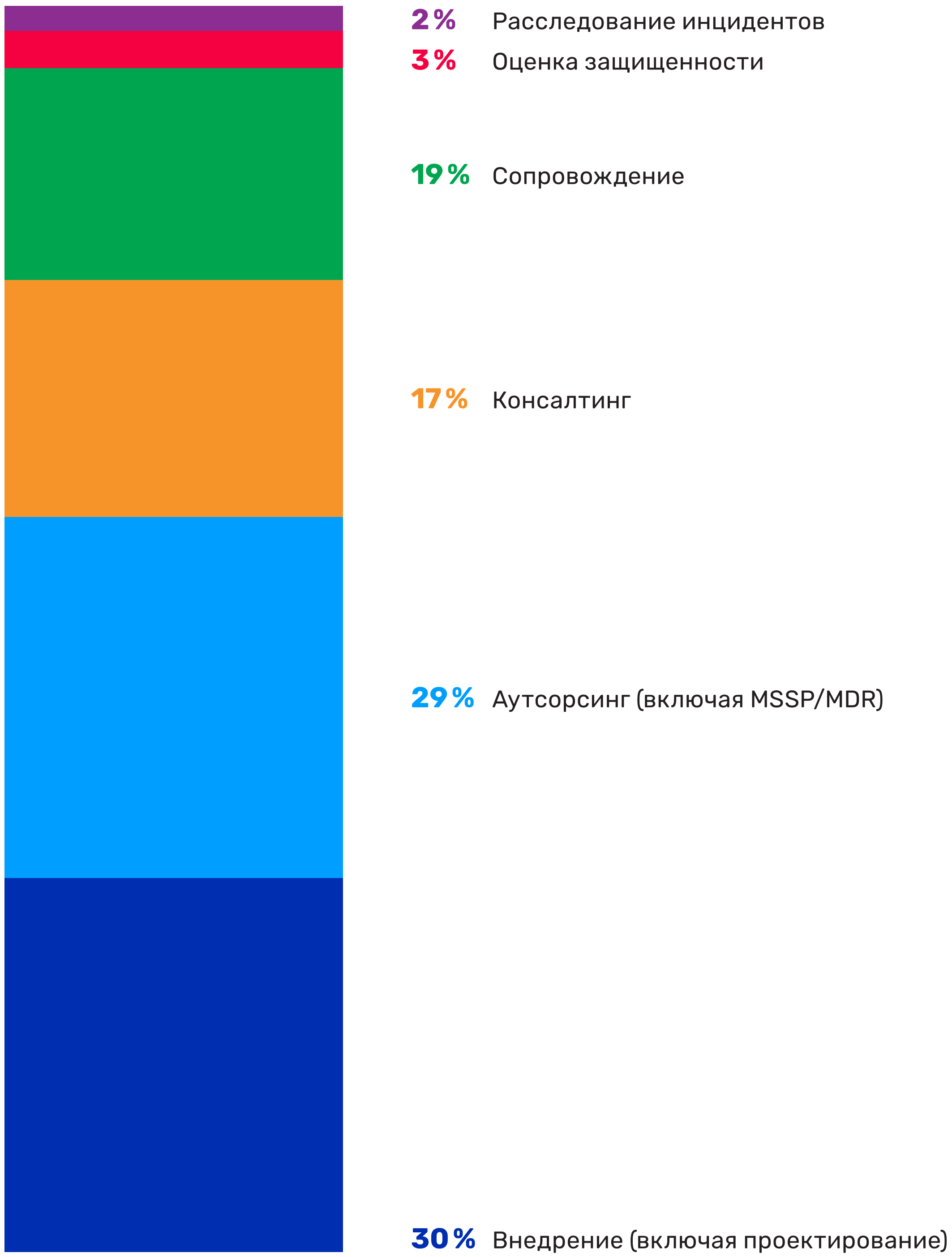
Таблица 3. Топ-5 вендоров в разрезе категорий средств защиты информации по состоянию на 2021 год

Позиция	Вендор	Юрисдикция
	Средства защиты сетей (network security)	
1	Cisco Systems	Иностранная
2	Check Point Software Technologies	Иностранная
3	Код безопасности (ООО «Код безопасности»)	РФ
4	Fortinet	Иностранная
5	ИнфоТеКС (АО «ИнфоТеКС»)	РФ
	Защита рабочих станций/«конечных точек» (endpoint security)	
1	Лаборатория Касперского (АО «Лаборатория Касперского»)	РФ
2	ESET	Иностранная
3	Доктор Веб (ООО «Доктор Веб»)	РФ
4	Trend Micro	Иностранная
5	Check Point Software Technologies	Иностранная
	Средства защиты инфраструктуры (infrastructure security)	
1	Positive Technologies (АО «Позитив Текнолоджиз»)	РФ
2	International Business Machines Corporation (IBM)	Иностранная
3	Micro Focus International	Иностранная
4	R-Vision (ООО «Р-Вижн»)	РФ
5	Лаборатория Касперского (АО «Лаборатория Касперского»)	РФ
	Средства защиты приложений (application security)	
1	Positive Technologies (АО «Позитив Текнолоджиз»)	РФ
2	International Business Machines Corporation (IBM)	Иностранная
3	Qrator (ООО «Эйч-Эль-Эль»)	РФ
4	Micro Focus International PLC	Иностранная
5	F5	Иностранная
	Средства защиты данных (data security)	
1	Infowatch (АО «Инфовотч»)	РФ
2	SearchInform (ООО «Серчинформ»)	РФ
3	КриптоПро (ООО «КриптоПро»)	РФ
4	ИнфоТеКС (АО «ИнфоТеКС»)	РФ
5	Фактор-ТС (ООО «Фактор-ТС»)	РФ
	Средства защиты пользователей (user security)	
1	CyberArk Software	Иностранная
2	Аладдин Р.Д. (АО «Аладдин Р.Д.»)	РФ
3	SearchInform (ООО «Серчинформ»)	РФ
4	КриптоПро (ООО «КриптоПро»)	РФ

Долевое распределение предлагаемых на рынке в 2021 году категорий услуг в области обеспечения информационной безопасности, а именно:

- 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.

Рисунок 5. Долевое распределение услуг ИБ по результатам 2021 года



Рынок кибербезопасности Российской Федерации в 2021 году показывает совокупный среднегодовой темп роста (CAGR — Compound annual growth rate) не менее **15%**. Это больше, чем рост мирового рынка, который за счет стран Северной Америки и Западной Европы исторически развит сильнее российского, и растет по причине своей зрелости в среднем только на **11%** в год.

Декомпозиция объемов долей рынка и расчетных значений CAGR за 2021 год по категориям рассмотренных ранее средств защиты приведена в **Таблице 4**.

Таблица 4. Декомпозиция объемов долей рынка и расчетных значений CAGR за 2021 год по категориям рассмотренных ранее средств защиты

Категория средства защиты информации	Объем доли рынка (%)	Объем доли рынка (млрд руб.)	CAGR (%)
Сетевая безопасность (network security)	45%	61	20%
Защита рабочих мест (endpoint security)	13%	18	17%
Защита инфраструктуры (infrastructure security)	12%	17	32%
Защита приложений (application security)	8%	11	34%
Защита данных (data security)	15%	20	13%
Защита пользователей (user security)	7%	9	10%
ИТОГО		136	

Объем рынка услуг составил **49,5 млрд руб.** с CARG **17%**.

Рыночные ожидания 2022 года и прогноз до 2026 года

Рыночные ожидания 2022 года формируются на фоне массового ухода зарубежных вендоров с отечественного рынка[2] (у них было **39 %** общего объема рынка по состоянию на 2021 год). Сложившаяся ситуация для российских вендоров выгодна, так как спрос на решения, обеспечивающие кибербезопасность, уверенно растет. Рост спроса обусловлен следующими факторами, связанными с изменившейся геополитической обстановкой и мерами, предпринимаемыми правительством (регуляторами) и бизнесом для укрепления кибербезопасности:

1 Наблюдается значительный рост числа кибератак на органы власти, бизнес и промышленные объекты экономики РФ;

2 Вводится ответственность первых лиц организаций за обеспечение их информационной безопасности (см. Указ Президента от 01.05.2022 № 250 «О дополнительных мерах по обеспечению информационной безопасности РФ»);

3 С 31 марта текущего года запрещается закупка зарубежного программного обеспечения для использования на значимых объектах КИИ, а с 1 января 2025 года запрещается использование зарубежного программного обеспечения на таких объектах (см. Указ Президента от 30.03.2022 № 166 «О мерах по обеспечению технологической независимости и безопасности критической информационной инфраструктуры РФ»);

4 Вводится поддержка отрасли со стороны государства (льготы, дополнительные учебные программы, снижение регуляторной нагрузки);

5 Ужесточаются требования отраслевых регуляторов, предъявляемые к заказчикам решений ИБ, что будет дополнительно стимулировать спрос.

---

2 При формировании модели рынка информационной безопасности до 2026 года:

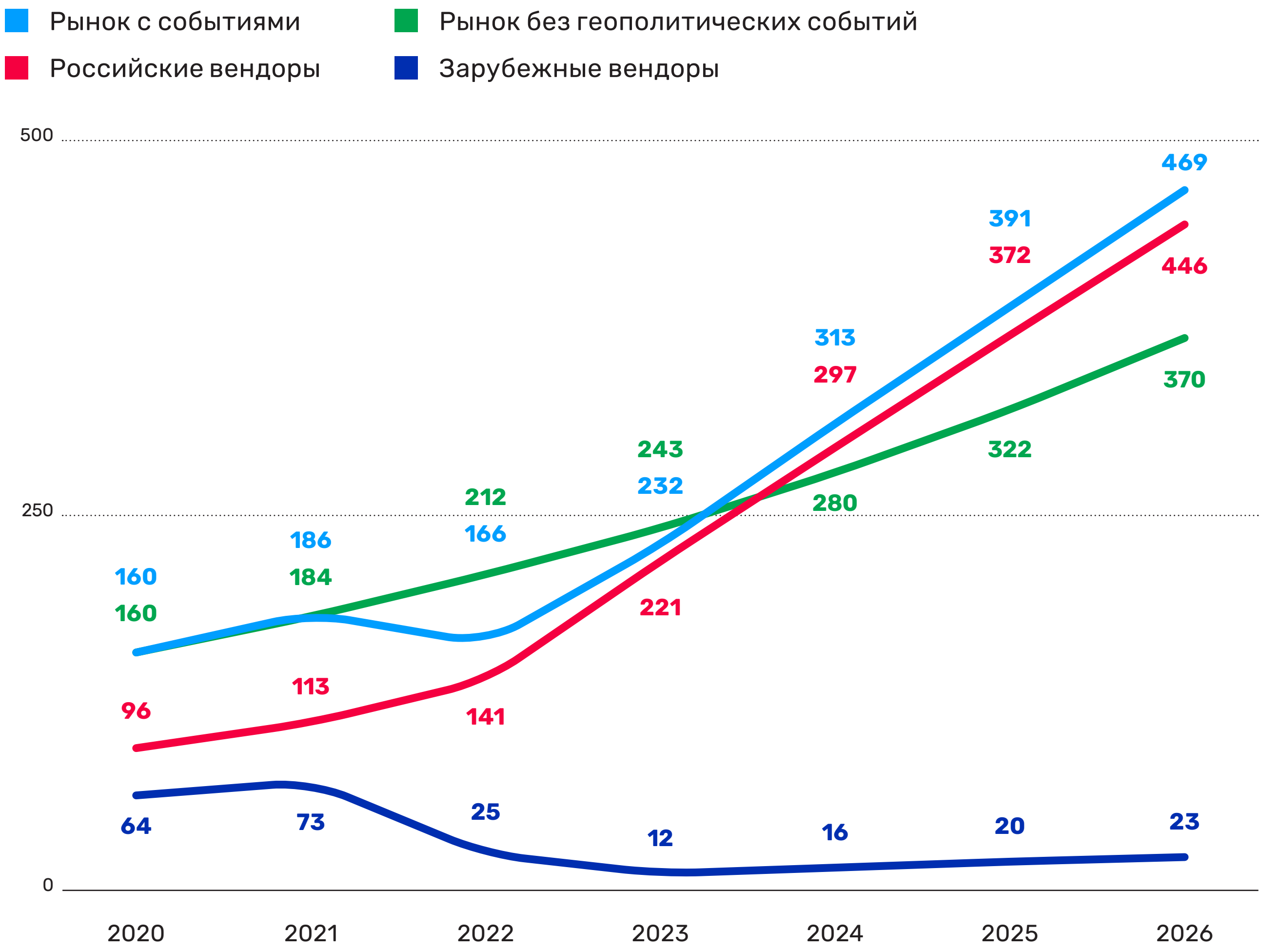
- за основу брался рост рынка в предыдущие годы (CARG 15 %)
- оценивалось влияние указанных факторов на рост рынка по отдельным категориям средств защиты информации и услугам
- влияние факторов оценивалась по годам исходя из постепенной стабилизации рынка в изменившихся условиях к 2026 году
- оценка влияния факторов сформирована из оценки первой половины 2022 года и экспертных оценок

Стремительный уход зарубежных вендоров в 2022 году ожидаемо приводит к сокращению общего объема рынка на **11 %** (под объемом рынка подразумевается объем денег, выплаченных заказчиком, а не актуальная потребность) — это тот объем денежных средств, которые не смогут быть выплачены зарубежным вендорам по причине либо их невозможности поставить решения / оказать услуги, либо невозможности получить оплату. Это связано с тем, что ожидается падение выручки зарубежных вендоров на более чем **66 %** в 2022 году, в итоге по результатам года их доля на рынке сократится до **12 %**.

Уход зарубежных вендоров произойдет не одномоментно, но большая часть их доли рынка освободится в 2022 и 2023 годах. Постепенный характер ухода зарубежных вендоров связан с большим объемом контрактов, которые попали в «серую зону»: проведен конкурс, но нет возможности реализации проекта или этап реализации проекта, который не может быть продолжен. Также возможно разное поведение вендоров по 2–3-летним контрактам. Кроме этого, возможен серый (параллельный импорт).

Ситуация для российских вендоров выглядит в целом позитивно. Они широко представлены на нашем рынке и кооперативно имеют солидный портфель продуктов и сервисов. В связи с этим они быстро смогут заменить широкий ряд зарубежных решений и в течение ближайших лет забрать практически весь рынок. Основная часть освобождаемой доли рынка будет освоена в течение ближайших 2–3 лет на существующих наработках и решениях российских вендоров. Разработка недостающих решений может занять 2–5 лет, прежде чем продукты выйдут на должный уровень качества.

Рисунок 6. Прогноз развития рынка кибербезопасности России, млрд руб.



На графике можно видеть прогнозируемое снижение объема рынка в 2022–2023 годах в связи со сложившейся геополитической ситуацией, однако она не затронет отечественных вендоров. В целом рынок кибербезопасности России преодолеет тренд на снижение, связанное с сокращением доли зарубежных вендоров, и выйдет на прогнозируемые объемы (голубая линия на графике **Рисунок 6**) в 2023 году, после чего продолжит стремительный рост.

Повышение скорости роста рынка связана с указанными выше факторами. Наибольший эффект они будут давать в 2022 и 2023 году, затем постепенно будут снижаться и ожидается их стабилизация на уровне **20%** к 2026 году. CAGR для российских вендоров предположительно составит: 2022 год – **25%**, 2023 год – **56%**, 2024 год – **35%**, 2025 год – **25%**, 2026 год – **20%**; за 5 лет CAGR **32%** (красная линия на графике **Рисунок 6**)

При этом доля рынка зарубежных вендоров продолжит сокращаться и достигнет своего минимума в **5%** доли рынка в 2023 году (синяя линия на графике **Рисунок 6**) в связи с окончательным уходом традиционных для нашего рынка зарубежных вендоров (Cisco, IBM, Fortinet, ESET и др.). Далее доминантное положение отечественных вендоров может изменяться в связи с вероятным серым импортом. Ожидается что доля зарубежных вендоров на отечественном рынке стабилизируется на уровне **5%**, однако может вырасти до **8%** в 2026 году.

Таблица 5. Декомпозиция объемов долей рынка и расчетных значений CAGR за 2021 год и предполагаемый объем доли рынка в 2026 году по категориям рассмотренных ранее средств защиты

Категория средства защиты информации	Объем доли рынка в 2021 году (%)	Объем доли рынка в 2021 году (млрд руб.)	Объем доли рынка в 2026 году (%)	Предполагаемый объем доли рынка в 2026 году (млрд руб.)
Сетевая безопасность (network security)	**45%**	**60**	**42%**	**153**
Защита рабочих мест (endpoint security)	**13%**	**18**	**11%**	**40**
Защита инфраструктуры (infrastructure security)	**12%**	**17**	**19%**	**68**
Защита приложений (application security)	**8%**	**11**	**14%**	**49**
Защита данных (data security)	**15%**	**20**	**10%**	**38**
Защита пользователей (user security)	**7%**	**9**	**4%**	**14**
ИТОГО		**136**		**362**

Рост объема рынка в части средств защиты информации за период 2021–2026 года составит **22%**, для отечественных вендоров – **33%**, а для зарубежных – падение в **19%**. На долю российских вендоров придется **343,6 млрд руб.** или **95%** всего объема этой части рынка. Объем рынка услуг в 2026 году оценочно составит **107,3 млрд руб.** против **49,5 млрд руб.** в 2021 году, из которых на долю российских вендоров придется 102 млрд руб. Рост за период 2021–2026 года составит **17%**, для отечественных вендоров – **28%**, а для зарубежных – падение в **23%**.

Выводы

В ближайшие 5 лет отечественный рынок кибербезопасности предположительно вырастет с **185,9 млрд руб.** до **469 млрд руб.** (**в 2.5 раза**), CAGR рынка в 2026 году составит **20 %**.

Начиная с 2023 года практически весь бюджет заказчиков на средства защиты информации в секторах B2G и B2B будет потрачен на продукцию российских вендоров, что дает возможность роста этой части рынка с **113 млрд руб.** в 2021 году до **446 млрд руб.** в 2026 году (**в 4 раза**). CAGR для российских вендоров предположительно составит: 2022 год — **25 %**, 2023 год — **56 %**, 2024 год — **35 %**, 2025 год — **25 %**, 2026 год — **20 %**; за 5 лет CAGR **32 %**.

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