Аналитический обзор рынка кибербезопасности (ИБ) 2025: в поисках новых точек роста

Май 2025

Главное кратко

Российский рынок кибербезопасности (информационной безопасности, ИБ) на фоне успехов импортозамещения за прошедшие два года продемонстрировал весьма впечатляющий рост – на 56%. При этом и кибератаки обрели новое качество, превратившись из точечных акций в перманентную угрозу, поддержанную технологическими инновациями. В 2025 году и в перспективе до 2030 года на рынке ИБ мы ожидаем:

- Основными драйверами роста российского рынка ИБ будут оставаться продолжение общей цифровизации бизнеса (с учетом вероятного замедления), увеличение масштаба и числа кибератак/киберугроз, а также ужесточение госрегулирования в вопросах защиты персональных данных. При этом, по нашему мнению, **среднегодовой темп роста российского рынка ИБ замедлится до 20% г/г с горизонтом планирования до 2030 года**, но останется выше общемирового (оценочно 12,5%).
- Динамика финансовых показателей основных российских поставщиков решений ИБ по итогам 2025 года не будет однородной. **Ключевым фактором, определяющим стратегию развития компании** для крупных игроков, по нашему мнению, **будет возможность доступа к сравнительно дешевым заимствованиям** на фоне высокой ключевой ставки Банка России. Игроки с доступом к сравнительно дешевым кредитам в 2025 году продолжат стремительное наращивание выручки и увеличение доли рынка, остальные же, вероятно, сосредоточатся на повышении операционной эффективности в рамках уже занятого объема рынка, а также на развитии инноваций и комплексных продуктов.
- В поиске новых точек роста многие поставщики решений, по нашему мнению, сосредоточат усилия на развитии/продвижении **комплексных инновационных решений в области сетевой и облачной безопасности** (в частности, решений класса NGFW), а также на расширении спектра **услуг ИБ** (в частности, услуг класса SOC/MDR) с возможным выходом на **рынок консалтинга в премиальном сегменте заказчиков.**
- Инновационно-технологическая составляющая глобального развития ИБ-решений до 2030 года, по нашему мнению, во многом будет направлена на обеспечение **комплексной проактивной защиты с элементами искусственного интеллекта**, в первую очередь, **ориентированной на защиту сетевых и облачных решений**; в более долгосрочной перспективе – на перевод наиболее значимых коммуникаций на технологии **квантового шифрования**.

Содержание

Рынок ИБ РФ в цифрах

Подходы и взгляды на оценку рынка ИБ РФ

- По оценке аналитиков МТС Web Services (MWS), опубликованной в отчете «Perspectives of IT-market 2024», объем российского рынка ИБ по итогам 2024 года составил 593,4 млрд руб., увеличившись на 30% г/г. В абсолютном выражении в 2024 году, по мнению MWS, на программно-аппаратные средства пришлось 113,19 млрд руб., на ПО — 273,58 млрд руб., на IT-услуги ИБ — 206,62 млрд руб.; в процентном выражении: на программно-аппаратные средства — 19%, на ПО — 46%, на IT-услуги ИБ — 35%.

- При этом некоторые крупные игроки и эксперты оценивают объем российского рынка ИБ в 2024 году ближе к 300 млрд руб.

- Мы полагаем, что столь существенные расхождения в оценке объема российского рынка ИБ могут быть вызваны по крайней мере двумя факторами. Во-первых, это общая закрытость рынка, особенно в контексте дополнительных антисанкционных мер отдельных компаний, что при высоких годовых темпах роста существенно влияет на точность оценки, формируемой методом прогнозирования по тренду на основе исторических данных. Во-вторых, это специфика формирования конечного продукта, когда ПО или программно-аппаратное средство (непосредственного) производителя может быть составной частью комплексного проекта интегратора или решения другого производителя либо быть продано дилером с наценкой (аналогично с сегментом услуг ИБ), что фактически удваивает, а в отдельных случаях многократно увеличивает вклад продуктовой единицы при оценке общего объема рынка.

Объем и структура российского рынка ИБ, по оценке MWS, 2024 г.

Источник: МТС Web Services.

* Под рынком кибербезопасности мы понимаем рынок программного обеспечения, программно-аппаратных решений, а также услуг и сервисов по защите от вредоносного ПО, кибермошенничества, кражи личных данных, а также от других видов киберпреступлений. Мы не разделяем такие понятия как «кибербезопасность» и «информационная безопасность» (ИБ), так как во всех случая использования термина ИБ речь идет о защите данных, представленных в цифровом виде или на цифровых носителях.

- Несмотря на то, что деятельность системных интеграторов и дистрибьютеров (включая отдельных сервис-провайдеров) является существенной составной частью рынка ИБ, мы полагаем, что оценивать рынок ИБ и анализировать его тенденции наиболее корректно с позиции непосредственных разработчиков/поставщиков решений ИБ (продуктов и услуг) при наличии соответствующих сведений.

Рынок ИБ РФ в цифрах

Объем и динамика рынка в деньгах поставщиков

- По оценке Б1*, объем российского рынка ИБ в 2024 году (в деньгах поставщиков) составил 299 млрд руб., что на 22,5% больше, чем по итогам 2023 года (244 млрд руб.). При этом в 2023 году рынок ИБ (в деньгах поставщиков) продемонстрировал более чем двукратное увеличение темпов роста год к году по сравнению с 2022 годом на фоне ухода западных производителей и резкого обострения геополитической напряженности, в том числе смещения фокуса и увеличения количества кибератак на социальную инфраструктуру. С 2022 по 2024 гг. среднегодовой темп роста рынка ИБ (в деньгах поставщиков) составил 24,8%, при том что структура рынка изменилась незначительно в сторону роста доли услуг ИБ.

₽299 млрд

объем российского рынка ИБ в 2024 году (в деньгах поставщиков) по оценке Б1*

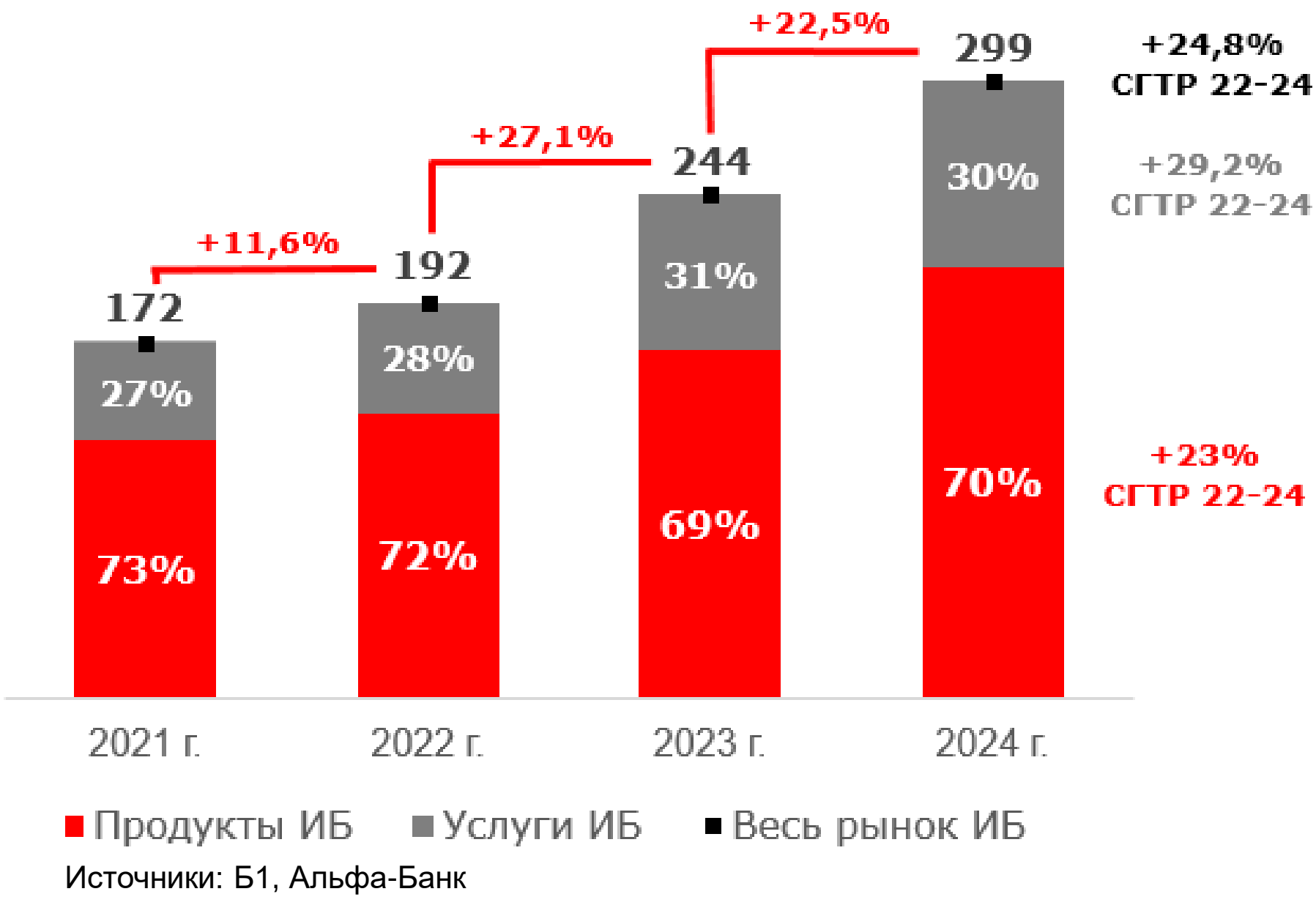
* Б1- ранее Эрнст энд Янг.

+24,8% г/г

среднегодовой темп роста рынка ИБ в 2022—2024 гг. (в деньгах поставщиков)

- Существенное влияние на рынок ИБ оказали регуляторные меры, в частности указ президента РФ №250 от 01.05.2022 г., в рамках которого с 01.01.2025 г. органам власти и ряду организаций запрещается использовать средства защиты информации, странами происхождения которых являются недружественные иностранные государства.

Динамика объема российского рынка ИБ в деньгах поставщиков, млрд руб.



Источники: Б1, Альфа-Банк

Рынок ИБ РФ в цифрах

Объем и динамика рынка в тратах клиентов

- Объем российского рынка ИБ в 2024 году (в тратах клиентов) составил 324 млрд руб., что на 23,2% больше, чем по итогам 2023 года (263 млрд руб.). За период с 2022 по 2024 годы среднегодовой темп роста рынка ИБ (в тратах клиентов) составил 24,8%, продемонстрировав некоторое сглаживание динамики роста по сравнению с аналогичными темпами роста в деньгах поставщиков.

- Усредненное значение «наценки» дистрибьютера/ интегратора составило около 8%, при этом «наценка» на продукты ИБ оказалась чуть большей, чем на услуги ИБ.

- По рынку ИБ в целом мы ожидаем в 2025 году снижения темпов роста до 20% г/г (как в деньгах поставщиков, так и в тратах клиентов), если не будет новых значимых драйверов роста IT-сектора в целом.

₽324 млрд

объем российского рынка ИБ в 2024 году (в тратах клиентов) по оценке Б1

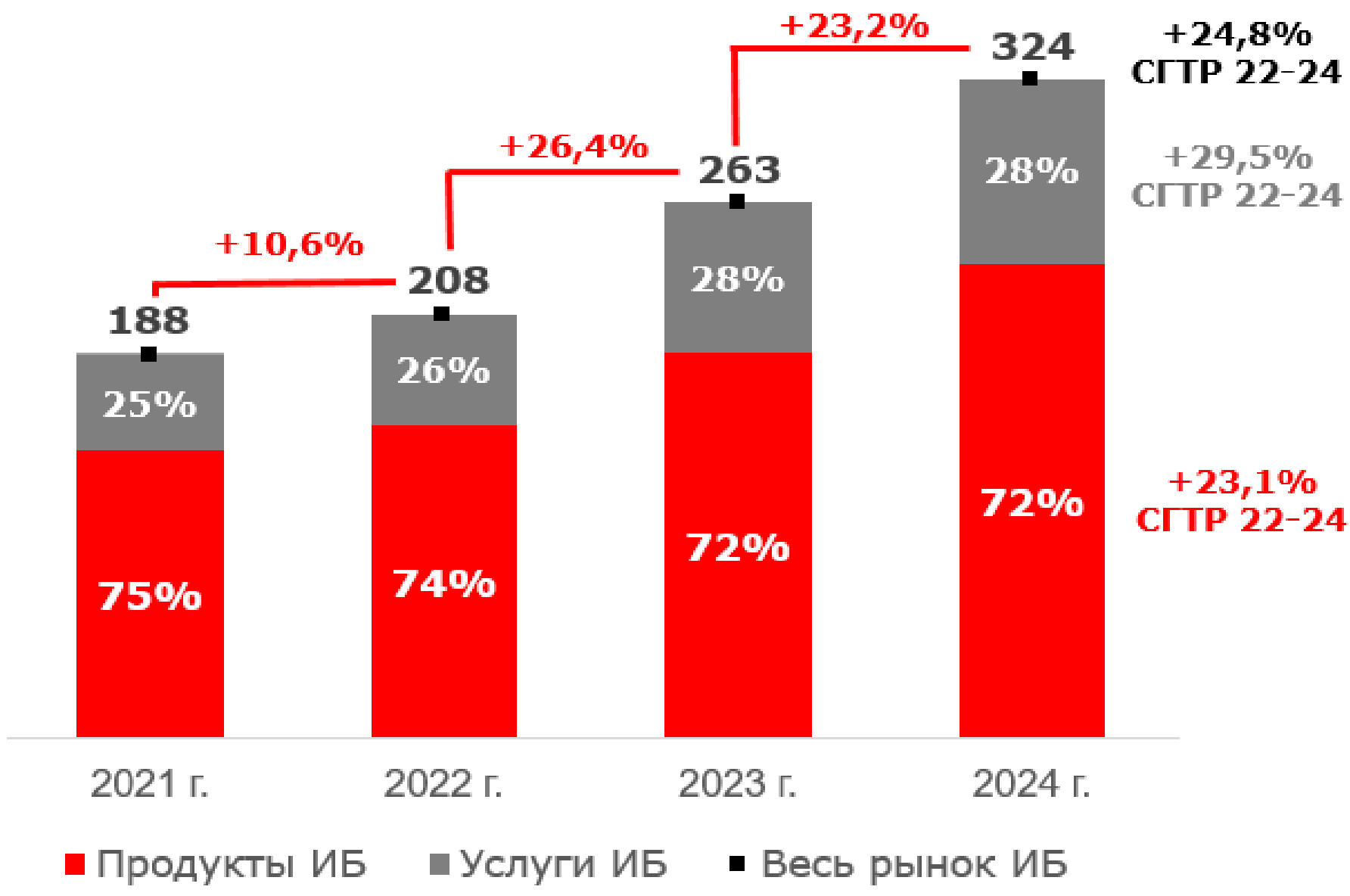
+24,8% г/г

среднегодовой темп роста рынка ИБ за 2022-2024 гг. (в тратах клиентов)

~8%

усредненная «наценка»

Динамика объема российского рынка ИБ в тратах клиентов, млрд руб.



Источники: Б1, Альфа-Банк

Рынок ИБ РФ в цифрах

Структура российского рынка ИБ

- Исходя из оценки Б1 рынка ИБ в 299 млрд руб. в деньгах поставщиков, чуть более 70%, то есть 210 млрд руб., в 2024 году пришлось на продукты ИБ, а на услуги ИБ – около 30%, или 89 млрд руб.

- Исходя из базовой классификации (детализирована в приложении), наибольшую долю рынка продуктов ИБ составляют решения в области сетевой и облачной безопасности — около 42%. В частности, существенные маркетинговые усилия производителей на текущий момент сосредоточены на продвижении решений класса NGFW. Доля решений в области анализа, контроля и реагирования на угрозы составляет 17%, так же как и решений в области защиты конечных точек. Оба сегмента в наименьшей степени фрагментированы (доля ТОП-10 производителей внутри сегмента составляет более 90%). На решения в области защиты данных и управления доступом приходится 10% и 8% соответственно, на управление рисками, навыками ИБ и прочие продукты – около 6% рынка продуктов ИБ.

- Проектные услуги в общем объеме рынка услуг ИБ составляют около 37%, с существенной оговоркой, что речь идет о проектах исключительно в области ИБ, без учета комплексных проектов интеграторов, где ИБ может являться важной (и весьма дорогостоящей) составной частью. Около 63% рынка услуг ИБ приходится на аутсорсинг и MSS**. В этом сегменте существенные маркетинговые усилия сосредоточены в продвижении решений класса SOC/MDR*** (как услуги), также отмечается высокая необходимость и финансовая перспективность направлений консалтинга и предоставления образовательных услуг.

Структура рынка продуктов ИБ, 2024 г.

Структура рынка услуг ИБ, 2024 г.

Источник: Б1.

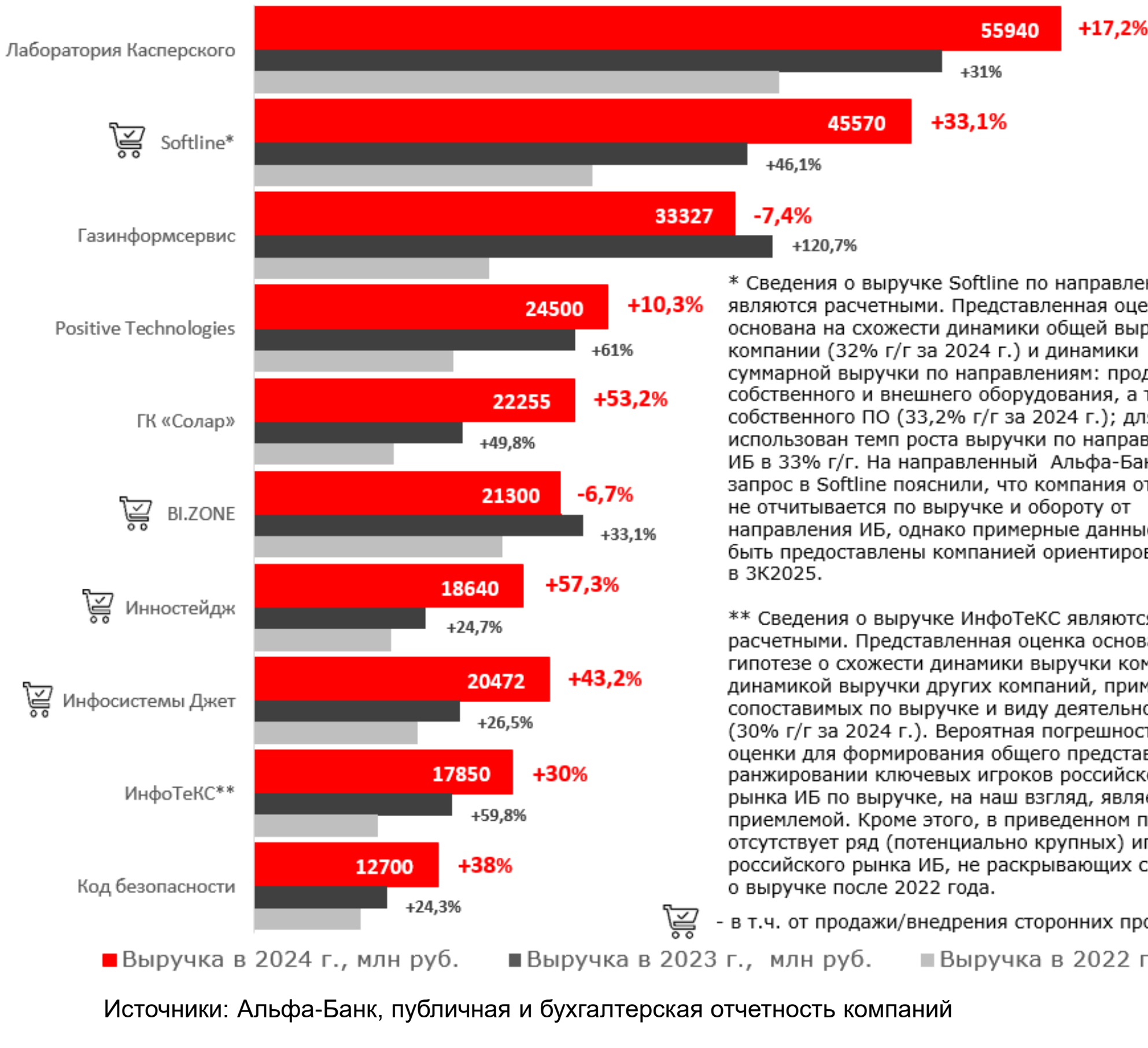
* NGFW (*Next Generation Firewall*) — Межсетевой экран нового/следующего поколения.
** MSS (*Managed Security Service*) — Управляемые сервисы кибербезопасности.
*** SOC (*Security Operation Center*) — Центр мониторинга информационной безопасности.
MDR (*Managed Detection and Response*) — Служба мониторинга, обнаружения и реагирования на угрозы.

Рынок ИБ РФ в цифрах

Ключевые поставщики решений рынка ИБ

- Согласно собственному исследованию Альфа-Банка, в десятку крупнейших поставщиков решений рынка ИБ (по объему годовой выручки) по итогам 2024 года входят: **Лаборатория Касперского**, **Softline**, **Газинформсервис**, **Positive Technologies**, **ГК «Солар»**, **BI.ZONE**, **Инностейдж**, **Инфосистемы Джет**, **ИнфоТеКС**, **Код безопасности**. Рейтинг составлен с учетом выручки отдельных компаний от продажи/внедрения сторонних продуктов, при условии, что сами компании имеют существенный объем собственного производства продуктов ИБ или (собственного) оказания услуг ИБ. Также в рейтинг не вошли ряд заметных компаний, не раскрывающих сведения о своей деятельности в рамках антисанкционной политики. Всех представителей ТОП-10 можно отнести по годовой выручке к условной категории «10 млрд руб.+»; на 11-м месте, по нашей оценке, оказалась **UserGate** (также весьма заметная на рынке ИБ) с выручкой 7 950 млн руб. и темпом роста 27,7% г/г в 2024 году.

Крупнейшие поставщики решений российского рынка ИБ по выручке, 2024 г.



* Сведения о выручке Softline по направлению ИБ являются расчетными. Представленная оценка основана на схожести динамики общей выручки компании (32% г/г за 2024 г.) и динамики суммарной выручки по направлениям: продажа собственного и внешнего оборудования, а также собственного ПО (33,2% г/г за 2024 г.); для расчета использован темп роста выручки по направлению ИБ в 33% г/г. На направленный Альфа-Банком запрос в Softline пояснили, что компания отдельно не отчитывается по выручке и обороту от направления ИБ, однако примерные данные могут быть предоставлены компанией ориентировочно в 3К2025.

** Сведения о выручке ИнфоТеКС являются расчетными. Представленная оценка основана на гипотезе о схожести динамики выручки компании с динамикой выручки других компаний, примерно сопоставимых по выручке и виду деятельности (30% г/г за 2024 г.). Вероятная погрешность данной оценки для формирования общего представления о ранжировании ключевых игроков российского рынка ИБ по выручке, на наш взгляд, является приемлемой. Кроме этого, в приведенном перечне отсутствует ряд (потенциально крупных) игроков российского рынка ИБ, не раскрывающих сведения о выручке после 2022 года.

- в т.ч. от продажи/внедрения сторонних продуктов ИБ.

Источники: Альфа-Банк, публичная и бухгалтерская отчетность компаний

Рынок ИБ РФ в цифрах

Ключевые поставщики решений рынка ИБ

	Выручка в 2024 г., млн руб.	Выручка в 2023 г., млн руб.	Выручка в 2022 г., млн руб.	Динамика 2023-24, г/г	Динамика 2022-23, г/г	Ключевые виды деят. в части ИБ
Лаборатория Касперского	**55 940**	47 736	36 439	17,2%	31,0%	
Softline*	**45 570**	34 240	23 428	33,1%	46,1%	
Газинформсервис	**33 327**	35 985	16 305	-7,4%	120,7%	
Positive Technologies	**24 500**	22 213	13 800	10,3%	61,0%	
ГК «Солар»	**22 255**	14 513	9 690	53,3%	49,8%	
BI.ZONE	**21 300**	22 830	17 156	-6,7%	33,1%	
Инностейдж	**18 640**	11 849	9 500	57,3%	24,7%	
Инфосистемы Джет	**20 472**	14 295	11 300	43,2%	26,5%	
ИнфоТеКС*	**17 850**	13 737	8 598	29,9%	59,8%	
Код безопасности	**12 700**	9 200	7 400	38,0%	24,3%	

- разработка программных продуктов ИБ
- разработка аппаратных продуктов ИБ
- услуги ИБ
- продажа/внедрение сторонних продуктов ИБ

* комментарии и оговорки приведены выше.

Источники: Альфа-Банк, публичная и бухгалтерская отчетность компаний

- В целом, можно сказать, что состав ТОП-10 поставщиков решений рынка ИБ (по объему годовой выручки), по нашей оценке, не изменился. Лидером по итогам 2024 года остается **Лаборатория Касперского** с выручкой в 55 940 млрд руб. и годовым темпом роста 17,2% (глобальная выручка компании достигла $822 млн, это максимальный показатель за всю историю ее деятельности, годовой темп роста составил 11%). **Softline** переместился на вторую строку рейтинга, продемонстрировав за прошедшие два года не только высокие, но и устойчивые годовые темпы роста, вместе с **ГК «Солар»**, **Инностейдж** и **Инфосистемы Джет**.

- **Газинформсервис** и **Positive Technologies** в 2024 году скорее адаптировались к достигнутым уровням, на фоне рекордных темпов роста выручки в 2023 году.

- Наиболее впечатляющей выглядит динамика **ГК «Солар»** со среднегодовым темпом роста выручки за последние три года более 50%*. В качестве одной из вероятных причин успеха, обеспечивающих возможность для столь агрессивной экспансии с элементами поглощения, помимо общей операционной эффективности, можно назвать доступ к сравнительно дешевому кредитованию у материнской компании ПАО «Ростелеком» (по сведениям, указанным в публичной отчетности компании, по ставке кредитования около 13% годовых).

* При сравнении динамики выручки среди публичных компаний ГК «Солар» уступает только ГК «Астра» (среднегодовой темп роста выручки за последние три года – более 80%).

Рынок ИБ РФ в цифрах

Доля крупных игроков по сегментам рынка

- Исходя из оценки Б1 объема рынка ИБ в 2023 году в деньгах поставщиков, наименее фрагментированными являются сегменты «Защита конечных точек», «Защита данных», а также «Управление рисками и навыками ИБ». В этих сегментах доля десяти (локально) крупнейших игроков превосходит 90%.

- Наиболее фрагментированными являются сегменты «Проектные услуги», «Сетевая и облачная безопасность», «Поставка ИБ-продуктов», в которых доля десяти (локально) крупнейших игроков не превосходит 2/3, причем в сегменте «Проектные услуги» их доля составляет менее 1/2.

- Наиболее заметными игроками, входящими в ТОП-10 внутри отдельных сегментов, но не вошедшими в ТОП-10 ключевых поставщиков ИБ-решений, являются: **UserGate**, **Angara Security**, **ГК «Гарда»**, **Информзащита**, **Rubytech**, **ДиалогНаука**, **Доктор Веб**, **Конфидент**, **Sitronics**, **Амикон**, **InfoWatch**, **С-Терра СиЭсПи**, **КриптоПРО**, **ИВК**.

Доля ТОП-10 игроков внутри сегмента по отношению во всему сегменту, в деньгах поставщиков, 2023 г.

Источники: Б1, Альфа-Банк

* в тратах клиентов

Мнения по вопросу возможных направлений роста

- В апреле 2025 года на конференции UserGate 2025 представители компании презентовали результаты собственного исследования и видения перспектив роста на рынке ИБ. Так, по мнению представителей компании, для поставщиков решений рынка ИБ приоритетом должен быть экосистемный подход, когда клиентам предоставляется качественная техподдержка и всесторонняя защита, покрывающая все потребности инфраструктуры, от одного поставщика. Состоявшееся затем в рамках конференции голосование с участием заказчиков и экспертов отрасли не в полной мере подтвердило данный тезис, для клиентов все же оказалась не менее ценной качественная составляющая отдельных решений ИБ в ущерб их бесшовной интеграции, обеспеченной одним поставщиком. Недоумение выразили и интеграторы, прямо заявившие о возможном конфликте интересов в случае увеличения доли поставщиков ИБ-решений в сегменте ИБ-консалтинга. Была сделана отсылка к результатам исследования, свидетельствующим о том, что для поставщиков решений на рынке ИБ, не имеющих обширного опыта непосредственной работы с заказчиками (конечными клиентами), для продвижения собственных консалтинговых услуг может быть интересен в первую очередь условно премиальный сегмент заказчиков (у которых годовая выручка превосходит 5 млрд руб.), в котором придется конкурировать не столько с интеграторами, сколько с собственной IT-службой заказчика.

С кем комфортнее работать в части комплексного подхода к ИБ

	B2E	B2B Ст	B2B Ср	B2CMБ	B2G
Вендор (экспертиза в услугах и продуктах в профильных категориях)	V	V	V	V	
Интегратор (установка «под ключ»)	X	V		V	V
Сервис-провайдер				V	

Однако, на текущий момент для каждого типа объектов выбирается свой поставщик решений

UserGate

* B2E – годовая выручка >₽50 млрд в год;
B2B Ст - > ₽5 млрд;
B2B Ср - ₽0,8-5 млрд;
B2CMБ - до ₽0,8 млрд;
B2G - ФОИВ/РОИВ.

Источник: UserGate.

- В целом же, большинство крупных участников рынка видит для себя наилучшие перспективы в развитии сервисной модели ИБ, расширении продуктовой линии с упором на инновации и создании комплексных решений на ее основе, а также в максимальном наращивании экспертизы по ключевым направлениям обеспечения ИБ для комплексного покрытия потребностей заказчика. В частности, крупные игроки активно продвигают и во многом делают ставку на собственные решения класса NGFW, а также на комплексные сервисы SOC/MDR, также называя эффективным способом ускоренного наращивания экспертизы поглощение небольших перспективных игроков.

Наиболее заметные M&A сделки 2024 года

Год	Объект	Покупатель	Сведения о компании
2024	10% Luntry (ООО «Клаудран»)	**ГК «Солар»**	Разработчик средств защиты контейнеров Kubernetes.
2024	100% акций Digital Security	**ГК «Солар»**	Разработчик решений для безопасности ERP-систем, аудитор кибербезопасности, крупный игрок на рынке пентестинга.
2024	51% «Элвис-Плюс», доля доведена до 100%	**ГК «Солар»**	Системная интеграция на рынке ИБ, сервисы информационной безопасности, разработка и поставка собственного ПАК «Застава» для защиты каналов связи и межсетевого экранирования.
2024*	F.A.C.C.T (бывшее подразделение Group-IB), передача активов новой компании: инженерные технологии, экспертизу, интеллектуальную собственность и текущие контракты	Инвестфонд Сайберус (аффилирован с **Positive Technologies**) – 47%, частные инвесторы	Разработчик линейки технологий для предотвращения и расследования киберпреступлений.

* полное завершение всех юридических процедур в 2025 году.

- **ГК «Солар»** в 2024 году завершила сделку по покупке 10%-й доли в разработчике решений контейнерной безопасности Luntry (ООО «Клаудран»). Сумма сделки не раскрывается. Как предположил один из опрошенных Cnews экспертов, стоимость Luntry, исходя из публичной отчетности, может составлять до 500 млн руб., а сумма сделки – порядка 50 млн руб.

- Также в 2024 году **ГК «Солар»** завершила сделку по покупке 100% акций Digital Security, второго по величине игрока на российском рынке пентестинга. Команда Digital Security насчитывает более 60 исследователей и пентестеров, специализирующихся на анализе защищенности корпоративных сетей и IT-инфраструктуры, а также на тестировании на проникновение и анализе защищенности приложений. Сумма сделки не раскрывается, но оценивается экспертами в диапазоне от 170 млн руб. до 400 млн руб.

- 23 декабря 2024 года **ГК «Солар»** завершила сделку по приобретению 51% акций компании «Элвис-Плюс», доведя свою долю в этом активе до 100%. К основным направлениям деятельности Элвис-Плюс относятся системная интеграция на рынке ИБ, сервисы информационной безопасности, разработка и поставка собственного ПАК «Застава» для защиты каналов связи и межсетевого экранирования.
- После того как основатель F.A.C.C.T. и Group-IB Илья Сачков был осужден за госизмену, основные активы F.A.C.C.T были выкуплены фондом «Сайберус», специализирующимся на ИБ. Этот фонд был создан сооснователем ИБ-вендора **Positive Technologies** Юрием Максимовым и частными инвесторами. Сумма сделки не раскрывается.

Мировой рынок ИБ

Ключевые показатели мирового рынка ИБ

- В вопросе оценки объема мирового рынка ИБ также (по аналогии с российским рынком ИБ) нет единого мнения. Так, по оценке Business Research Company, объем мирового рынка ИБ в 2024 году составил $267,5 млрд, увеличившись на 10% г/г, при этом на период до 2029 г. прогнозируется среднегодовой темп роста 12,9% г/г. Mordor Intelligence оценивает объем мирового рынка ИБ в 2024 году в $203,8 млрд с годовым темпом роста 11,4% г/г.

- Большинство же аналитиков и отраслевых экспертов исходят из представленной в сентябре 2024 года оценки Gartner, что объем рынка ИБ в 2024 году составит $183,87 млрд в тратах клиентов.

- Согласно данным Gartner и Statista, по состоянию на конец 2024 года в ТОП-10 стран – лидеров в сегменте ИБ входят США (44% рынка), Китай (8%), Великобритания (6%), Япония (5%), Германия (4%), Франция (3%), Австралия (2%), Канада (2%), Россия (2%), Южная Корея (2%). При этом доля остальных стран составляет порядка 22%. В качестве основных факторов можно выделить историческое лидерство США в области IT и использование наиболее передовых технологий, а также традиционно высокое внимание к безопасности и защите национальных интересов и критической инфраструктуры.

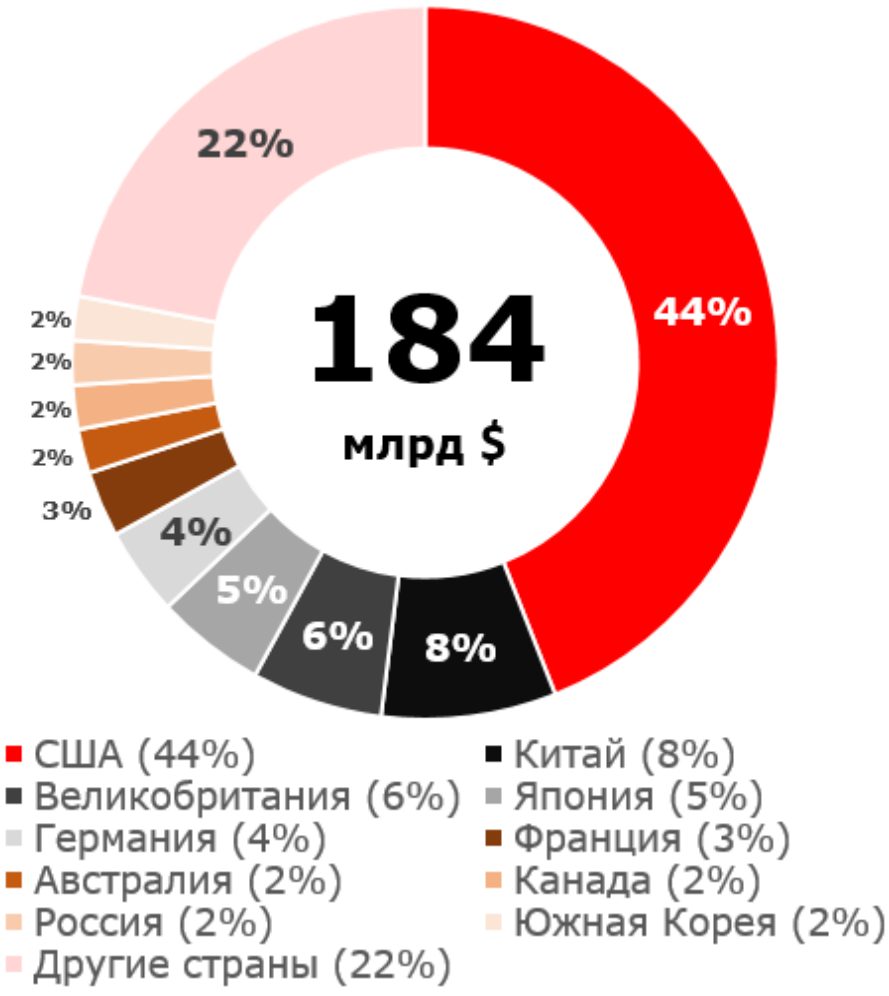
$267,5 млрд

объем мирового рынка ИБ в 2024 году по оценке Business Research Company

$203,8 млрд

объем мирового рынка ИБ в 2024 году по оценке Mordor Intelligence

Доля ТОП-10 стран в общих тратах клиентов на ИБ, 2024 г.



Источники: Gartner, Statista

- С точки зрения экспортного потенциала, российские ИБ-решения наиболее востребованы в странах СНГ, Юго-Восточной Азии и Ближнего Востока, предлагая разумный баланс эффективности защиты и стоимости решения. Здесь в полной мере проявляется негативное влияние санкций недружественных стран, которые не только ограничили трансграничные платежные операции, но и существенно увеличили стоимость программно-аппаратных решений ИБ с учетом схемы параллельного импорта комплектующих. Отмена введенных санкционных ограничений, по мнению многих экспертов рынка ИБ, в значительной степени нивелирует возможное негативное влияние усиления конкуренции в случае возвращения западных решений на российский рынок.

Мировой рынок ИБ

Ключевые показатели мирового рынка ИБ

- Исходя из оценки Gartner мирового рынка ИБ в $183,9 млрд в тратах клиентов, в 2024 году около 60% ($110 млрд) пришлось на продукты ИБ, около 27% ($49 млрд) — на проектные услуги, и около 13% ($24 млрд) — на аутсорсинг и MSS.

- При этом, несмотря на ускорение темпа роста год к году в 2024 году (13,6%) по сравнению с 2023 годом (12,5%), ожидается возвращение СГТР с горизонтом оценки до 2028 года к 12,5%.

- Ожидается незначительное перераспределение долей в структуре мирового рынка ИБ в пользу услуг аутсорсинга и MSS (до 14% в 2028 году), со снижением доли проектных услуг (до 26% в 2028 году) и сохранением доли продуктов ИБ (60% в 2028 году). В целом, в достаточно долгосрочной перспективе долю рынка продуктов ИБ в 60% можно рассматривать для российского рынка ИБ как целевую.

$183,9 млрд

объем мирового рынка ИБ в 2024 году в тратах клиентов по оценке Gartner

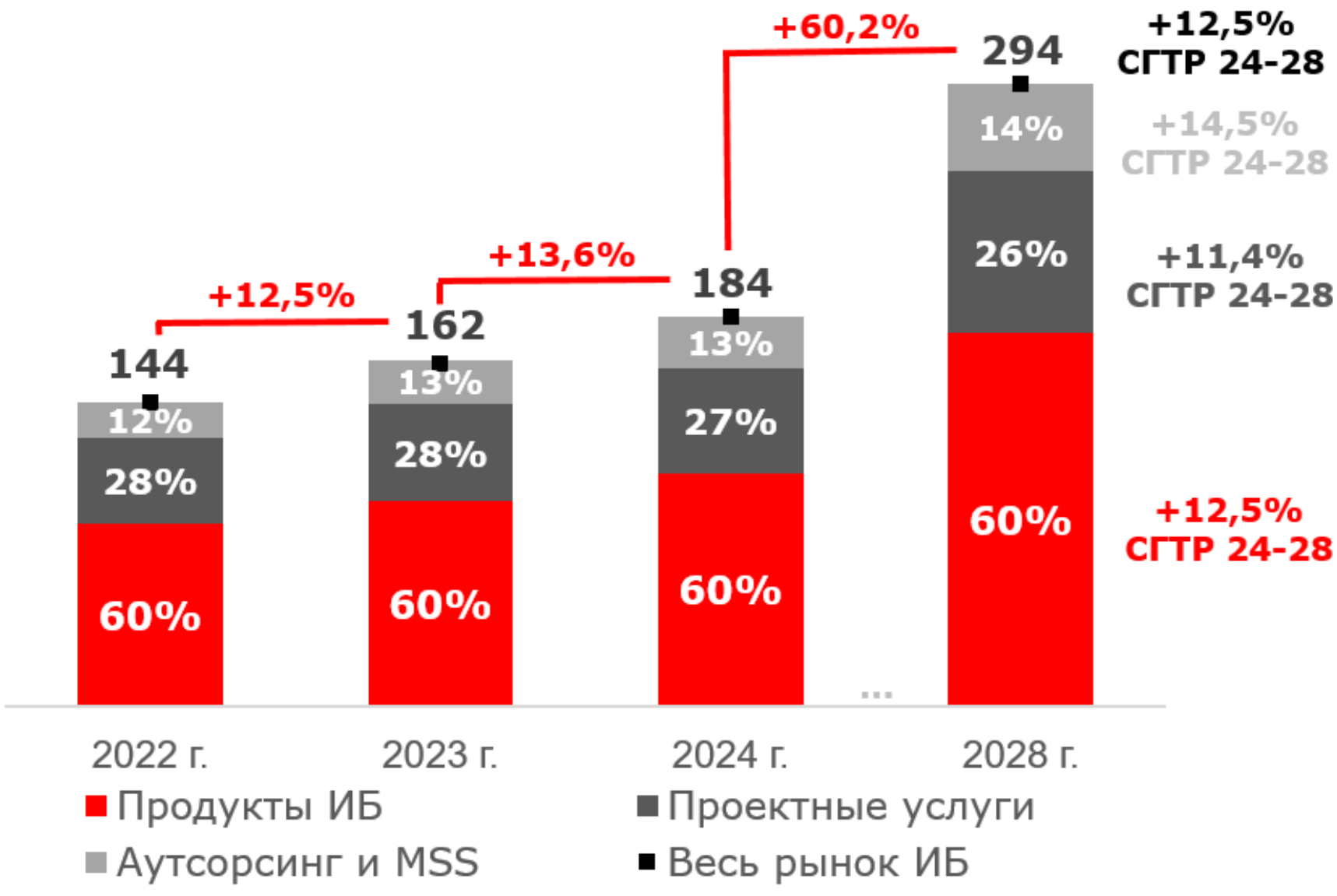
+12,5%

среднегодовой темп роста (г/г) рынка ИБ до 2028 года (в тратах клиентов)

+14,5%

опережающий среднегодовой темп роста (г/г) рынка аутсорсинга ИБ до 2028 года

Динамика мирового рынка ИБ (в тратах клиентов) в 2024 г., млрд. $



Источник: Gartner, Statista

Мировой рынок ИБ

Крупнейшие мировые игроки

Название	Специализация	Кол-во сотрудников	Штаб-квартира	Рыночная капитализации
Microsoft Security	Аудит кибербезопасности, SIEM, анализ, контроль и реагирование на угрозы ИБ, управление доступом	10 тыс. +	Редмонд, Вашингтон, США	~$3,16 трлн
Cisco	Сетевая и облачная безопасность	10 тыс. +	Сан-Хосе, Калифорния, США	~$245 млрд
Palo Alto Networks	Анализ, контроль и реагирование на угрозы ИБ (на основе ИИ)	10 тыс. +	Санта-Клара, Калифорния, США	~$126 млрд
CrowdStrike	Безопасность конечных устройств, анализ угроз и расширенное обнаружение и реагирование (XDR)	10 тыс. +	Остин, Техас, США	~$107 млрд
Fortinet	Сетевая безопасность и операционная безопасности, защита конечных точек, обнаружение вторжений	10 тыс. +	Саннивейл, Калифорния, США	~$80 млрд
Zscaler	Облачная платформа безопасности с VPN, ZTA и защитой от киберугроз	7,5 тыс. +	Сан-Хосе, Калифорния, США	~$35 млрд
Check Point	Сетевая и облачная безопасность, защита конечных точек	6 тыс. +	Тель-Авив, Израиль Сан-Карлос, Калифорния, США	~$25 млрд
McAfee	Антивирус, решения для обеспечения безопасности мобильных устройств и мониторинга идентификационных данных	1,8 тыс. +	Санта-Клара, Калифорния, США	~$11 млрд
SentinelOne	Платформа защиты конечных точек нового поколения (NG-EPP), предотвращения угроз на основе ИИ	2,5 тыс. +	Маунтин-Вью, Калифорния, США	~$5 млрд
Tenable (Nessus)	Анализ, контроль и реагирование на угрозы ИБ	2 тыс. +	Колумбия, Мэриленд, США	~$4 млрд

* Примерная величина рыночной капитализации указана по состоянию на начало мая 2025 г., для Microsoft Security указан объем капитализации головной компании Microsoft Inc.

- Исходя из общего размера рыночной капитализации, 10 из 10 представленных в мировом рейтинге компаний имеют штаб-квартиру в США.

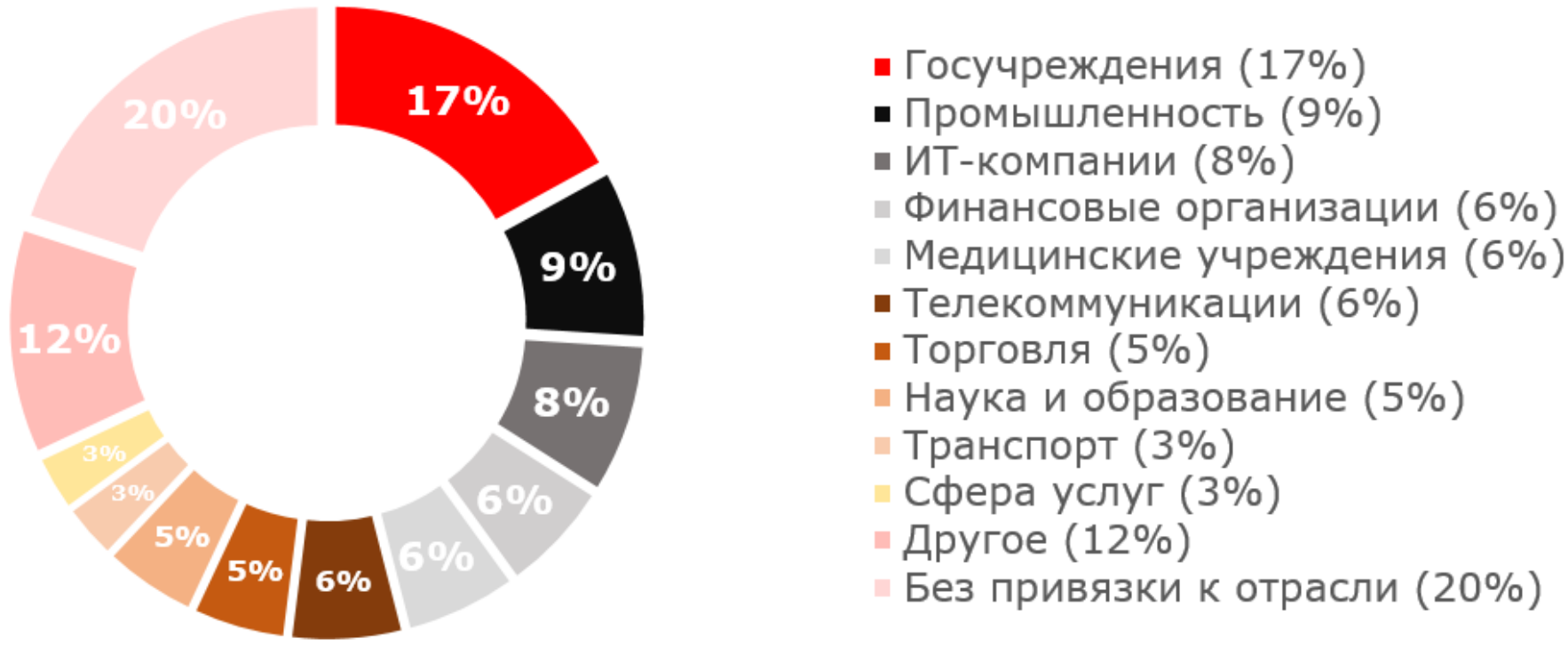
Ключевая статистика по киберпреступлениям

Киберпреступления и киберугрозы в цифрах

- Как сообщает ТАСС, число преступлений с использованием IT в 2024 году составило 40% от общего числа зарегистрированных в России преступлений, что является максимумом с 2020 года. Всего, с января по декабрь 2024 года в России зарегистрировано 765,4 тыс. киберпреступлений, что на 13,1% больше, чем за аналогичный период 2023 года.

- По данным МВД, в 2024 году четыре преступления из пяти (84,8%) были совершены с использованием интернета. Всего зарегистрировано 649,1 тыс. таких преступлений (на 23% больше, чем в 2023 году). Число киберпреступлений, совершенных с использованием средств мобильной связи, составило 346 тыс. (на 14% больше, чем в 2025 году). При этом генеральный прокурор России Игорь Краснов в октябре 2024 года заявил о снижении уровня раскрываемости преступлений в сфере IT до 25,9%.

Доли кибератак по отраслям, 4К24 – 1К25



Источник: Positive Technologies Expert Security Center

- Согласно данным Positive Technologies Expert Security Center за четвертый квартал 2024 года и первый квартал 2025 года, основным инструментом злоумышленников остается вредоносное ПО. Такое ПО применялось в 66% успешных атак на организации и в 51% атак на частных лиц. Против организаций чаще всего использовались шифровальщики (42%) и вредоносное ПО для удаленного управления (38%), против частных лиц — шпионское ПО (48%) и, в частности, банковские трояны (19%). Социальная инженерия остается одним из наиболее популярных методов для атак как на организации (50%), так и на частных лиц (88%). Основным каналом социальной инженерии для организаций остается электронная почта (84%), для частных лиц — сайты (44%). Также Positive Technologies фиксирует рост активности ботнетов, успешно атакующих сетевое оборудование, IoT-устройства и веб-серверы.

- Отдельно стоит выделить новый сформировавшийся тренд – атака через подрядчика, по которому количество инцидентов по некоторым оценкам выросло за 2024 год в три раза.

Ключевая статистика по киберпреступлениям

Киберпреступления и киберугрозы в цифрах

- Как сообщает Rubrik Zero Labs в своем отчете «Состояние безопасности данных в 2025 г.: распределенный кризис» (цитирует Scoop Business и CNews), кибератаки в последнее время по всему миру стали перманентной угрозой, а ставка на облачные сервисы как на дополнительную гарантию безопасности не всегда оправдывается.

- Согласно приведенной статистике, только в 2024 г. почти пятая часть организаций во всем мире столкнулась с 25 и более кибератаками. Наиболее распространенными векторами атак, по оценке Rubrik Zero Labs, были утечки данных (30%), вредоносное ПО (29%), утечки облачных или SaaS-решений (28%), фишинг (28%) и внутренние угрозы (28%). При этом 37% респондентов сообщили, что понесли по итогам проведенных атак репутационный урон и столкнулись с потерей доверия со стороны клиентов, в 33% компаниях в результате успешной кибератаки сменилось руководство.

- Из числа организаций, которые в 2024 г. подверглись успешной атаке вредоносного ПО, 86% признались, что вынуждены были заплатить выкуп, чтобы восстановить свои данные. В 74% случаев злоумышленникам удалось частично, а в 35% полностью скомпрометировать системы резервного копирования и восстановления. В 28% случаях были скомпрометированы учетные данные.

- Главной проблемой защиты данных респондентами Rubrik Zero Labs была названа разрозненность экосистемы крупных компаний (35% респондентов), на втором месте – отсутствие централизованного управления (30%), на третьем – отсутствие прозрачности и контроля над облачными данными (29%).

- Согласно статистике Kaspersky ICS CERT в области промышленной кибербезопасности*, с начала 2025 года 22,58% компьютеров АСУ в мире и 19,84% в России были атакованы вредоносным ПО, аналогичная статистика за весь 2024 год – 38,34% и 36,68% соответственно. Основными источниками угроз, заблокированных в 2024 году по всему миру были: интернет – 20,73%, почтовые клиенты – 4,15%, съемные носители – 1,68%, сетевые папки – 0,23%; в России: интернет – 20,24%, почтовые клиенты – 1,39%, съемные носители – 0,70%, сетевые папки – 0,17%.

* Сведения собраны при помощи Kaspersky Security Network от пользователей продуктов «Лаборатории Касперского», предоставивших свое согласие на автоматизированный анонимный сбор данных.

positive technologies Rubrik Zero Labs kaspersky

Перспективные технологии

Инновации являются важной составляющей лидерства в любом сегменте IT. На что стоит обратить внимание уже сегодня применительно к рынку ИБ:

- **Искусственный интеллект и машинное обучение.** Применительно к кибербезопасности ИИ-решения направлены, в первую очередь, на более быстрое и точное обнаружения угроз и уязвимостей, автоматизацию реагирования на атаки и обнаружение аномалий. Также элементы искусственного интеллекта хорошо применимы для противодействия фишингу, за счет автоматического анализа электронной почты и открываемых интернет-ресурсов на предмет наличия сомнительно контента. При этом не в последнюю очередь по значимости отмечается проблема обеспечения конфиденциальности обрабатываемой информации, в том числе накапливаемой в рамках процедур и алгоритмов машинного обучения. Обратной стороной эффективного поиска уязвимостей является возможность применения полученных сведений не для совершенствования системы защиты, а для планирования кибератак. Кроме того, LLM давно адаптированы к написанию вредоносного кода (например, из новаций конца 2024 года: сгенерированный PowerShell-скрипт, загружающий шпионское ПО Rhadamanthys и бэкдор CleanUpLoader).

- **Поведенческая биометрия.** В отличие от традиционной биометрии, которая полагается на физические признаки, такие как отпечатки пальцев, особенности лица или узор сетчатки глаза, поведенческая биометрия отслеживает как люди взаимодействуют со своими устройствами в динамике: сочетание частотных и статистических характеристик голоса, особенности подчерка или частоты нажатий на клавиши клавиатуры, мимика лица при произнесении кодового слова. Есть и ряд ограничений. В настоящее время сбор биометрических данных россиян регламентируется федеральным законом №572-ФЗ. В частности, коммерческие организации, колл-центры и другие организации не могут собирать информацию подобного типа. Зарегистрировать биометрические данные можно на портале госуслуг, в прошедших аккредитацию банках и в МФЦ.

- **Квантовая криптография.** В основе технологии квантовой криптографии лежит принцип использования квантовых битов («кубитов»). Этот принцип позволяет создавать квантовые ключи, которые обладают особыми свойствами, включая невозможность перехвата или подмены информации без обнаружения данного события (любая попытка перехватить квантовую информацию приводит к немедленному нарушению ее состояния, что позволяет обнаруживать такие попытки). Исследования в области квантовой криптографии ведут такие компании и организации как IBM, Google, Intel, Mitsubishi, LG, Caltech, NICT и другие. С 2020 года центром компетенций по развитию квантовых коммуникаций в России является РЖД. В настоящее время технология применяется для выработки и распределения симметричных криптографических ключей. Уже разработан опытный образец квантового шифратора для высокоскоростной передачи данных (со скоростью 180 Гбит/с). Ожидается, что к 2030 году протяженность квантовых сетей в России составит более 15 тыс. км.

Современные подходы и парадигмы обеспечения ИБ

- **Парадигма «нулевого доверия» (Zero Trust)**. Парадигма Zero Trust основывается на принципе «никому не доверяй». Каждый запрос на доступ к ресурсу должен пройти через строгую аутентификацию и авторизацию — проверку подлинности пользователя, устройства и контекста выполнения операции. При этом наиболее предпочтительной является модель наименьших привилегий, когда субъектам назначается строго минимальное количество прав, необходимый для выполнения заявленных задач. Все действия пользователей и устройств, логируются и анализируются в реальном времени с целью выявления аномальной активности и, при необходимости, оперативного принятия контрмер. Zero Trust, как концепция, наилучшим образом применима для контроля доступа большого количества удаленных сотрудников/распределенных команд к корпоративных ресурсам при работе с чувствительными данными, активно используется в рамках облачных сервисов по модели SaaS.

- **Парадигма «Предположение о проникновении».** Парадигма основана на базовом предположении, что абсолютной безопасности не бывает, и в какой-то момент злоумышленник все же может оказаться внутри защищаемого контура. При этом каждый ресурс (приложение, сервис, данные) защищается собственными настройками безопасности. Данный подход несколько усложняет общее администрирование, но при этом существенно затрудняет продвижение и сбор информации о системе злоумышленником, что в конечном счете позволяет выиграть время и исключить или снизить возможный урон.

- **Парадигма «Обнаружение и реагирование на угрозы на конечных точках» (EDR).** В отличие от традиционных антивирусных программ, которые фокусируются на обнаружении известных угроз, EDR обеспечивает проактивный подход к кибербезопасности, позволяя обнаруживать и реагировать на новые и сложные атаки, при этом также работая с локальными данными. В основу EDR парадигмы заложены принципы обеспечения непрерывного мониторинга активности конечных точек (устройств), быстрое выявление потенциальных инцидентов безопасности, автоматизация изоляции для ограничения последствий.

- **Кибербезопасность, как стратегическая цель и элемент корпоративной культуры.** Несмотря на наличие качественных решений по отдельным составляющим, большинство экспертов в области ИБ сходятся во мнении, что единственно возможным эффективным подходом к обеспечению ИБ может быть только комплексный и целостный подход, заложенный на базовом уровне корпоративной стратегии и культуры. При этом, если больше половины российских компаний (53,8% согласно данным Киберпротект) в 2024 году увеличили свои бюджеты на ИБ, то среди направлений, на которые компании направили дополнительные расходы, обучение ИБ сотрудников занимает второе место (60,9%), уступая лишь закупке ПО (82%) и существенно опережая закупку оборудования (34,4%).

Тенденции и прогнозы

Наше видение перспектив

1. **Основными драйверами роста российского рынка ИБ будут оставаться продолжение общей цифровизации бизнеса (с учетом вероятного замедления), увеличение масштаба и числа кибератак/киберугроз, а также ужесточение госрегулирования в вопросах защиты персональных данных. При этом, по нашему мнению, среднегодовой темп роста российского рынка ИБ замедлится до 20% г/г, с горизонтом планирования до 2030 года, но останется выше общемирового (оценочно 12,5%)**

- Не в последнюю очередь из-за высокой ключевой ставки и под влиянием геополитических факторов даже крупные и прибыльные российские компании замораживают инвестиционные проекты, перераспределяя средства в основные активы. Основной спрос на российские IT-решения постепенно смещается из области инноваций в область оптимизации операционной деятельности в контексте общего импортозамещения. При этом потребность в цифровизации бизнеса и сопутствующие киберриски остаются высокими, подогревая интерес к актуальным решениям в области ИБ.

- В части нормативного регулирования, существенную поддержку российскому рынку ИБ оказал указ президента РФ от 01.05.2022 г. №250 «О дополнительных мерах по обеспечению информационной безопасности Российской Федерации», в частности, вводящий запрет на использование средств защиты, произведенных в недружественных странах, с 1 января 2025 г. При этом фактически требуемая принудительная замена в большинстве случаев уже была произведена (тем, кто хотел и финансово мог это себе позволить) в период 2022-2024 гг. и не может рассматриваться как существенный действующий фактор дальнейшего развития рынка ИБ. В то же время, новым, пусть несколько косвенным, но в достаточной степени мотивирующим и имеющим длительное действие фактором роста является принятие федерального закона от 30.11.2024 №420-ФЗ «О внесении изменений в Кодекс Российской Федерации об административных правонарушениях». Этот закон, в частности, увеличивается штрафы за утечку персональных данных, а также вводит оборотные штрафы за повторную утечку. Дата вступления указанного ФЗ в силу – 30 мая 2025 г. При этом, по некоторым оценкам («Стахановец»), с момента принятия закона спрос со стороны бизнеса на решения для защиты данных краткосрочно увеличился на 40%, что, на наш взгляд, в части обеспечения высокого темпа роста рынка ИБ не будет носить долгосрочный характер.

- С учетом описанных факторов, среднегодовой темп роста российского рынка ИБ, по нашему мнению, замедлится примерно с 25% г/г (за период 2022-2024 гг.) до 20% г/г, с горизонтом планирования до 2030 года (при отсутствии новых значимых драйверов роста IT-сектора в целом), но останется выше общемирового (около 12,5% г/г).

Тенденции и прогнозы

Наше видение перспектив

2. **Динамика финансовых показателей по итогам 2025 года основных российских поставщиков решений ИБ не будет однородной. Ключевым фактором, определяющим стратегию развития компании для крупных игроков, по нашему мнению, будет возможность доступа к сравнительно дешевым заимствованиям на фоне высокой ключевой ставки Банка России. Игроки с доступом к сравнительно дешевым кредитам в 2025 году продолжат стремительное наращивание выручки и увеличение доли рынка, остальные же, вероятно, сосредоточатся на повышении операционной эффективности в рамках уже занятого объема рынка и на развитии инноваций и комплексных продуктов**

- Основные российские поставщики решений ИБ на протяжении последних двух лет на фоне взрывного роста выручки не продемонстрировали единой динамики финансовых показателей. Так, **Газинформсервис**, **Positive Technologies** и **ИнфоТеКС** по итогам 2023 года сразу продемонстрировали более чем 50% рост выручки (Газинформсервис: темп роста выручки – 120% г/г), после чего они ощутимо замедлились в 2024 году, адаптируясь к занятому объему рынка. **Инностейдж**, **Инфосистемы Джет**, напротив, со сравнительно невысокой позиции годового темпа роста (около 25%) в 2023 году, практически удвоили темпы прироста выручки год к году в 2024 году, демонстрируя «догоняющий» рост. Абсолютным же «чемпионом» по высокой и устойчивой динамике роста является **ГК «Солар»**, демонстрируя стабильно высокий годовой темп роста выручки на протяжении последних двух лет на уровне 50% г/г. При этом мы полагаем, что одним из наиболее значимых факторов, позволяющим поддерживать **ГК «Солар»** столь высокие темпы роста, является доступ к сравнительно дешевым кредитам и совместным проектам материнской компании Ростелеком.

- В 2025 году мы ожидаем дальнейшего снижения темпов роста годовой выручки основных российских поставщиков решений ИБ с адаптацией к уже занятому объему рынка и попыткой его конвертировать в прибыль компании (исключением может стать **ГК «Солар»** с учетом специфики стратегических приоритетов материнской компании).

- Хуже рынка (ИБ) в целом будут чувствовать себя небольшие игроки, поставщики решений, которые исторически не были готовы активно заниматься маркетингом и конкурировать на этом поле с лидерами. Привлечение инвестиций на развитие производства и внедрение инноваций в свои решения для них также доступно преимущественно через достаточно дорогое кредитование. По нашей оценке, поглощения небольших, но перспективных игроков лидерами рынка ИБ в 2025 году и далее продолжатся.

Наше видение перспектив

3. **В поиске новых точек роста многие поставщики решений, по нашему мнению, сосредоточат усилия на развитии/продвижении комплексных инновационных решений в области сетевой и облачной безопасности (в частности, решений класса NGFW), а также на расширении спектра аутсорсинговых услуг (в частности, услуг класса SOC/MDR) с возможным выходом на рынок консалтинга в премиальном сегменте заказчиков**

- Для крупных поставщиков решений рынка ИБ, во многом делающих существенную ставку на маркетинг, важной точкой роста будет инновационная составляющая решения. Также на фоне сравнительно высокой уязвимости облачных решений (в силу их специфики), а также сетевой инфраструктуры с множеством точек подключения, основной ажиотаж вокруг инновационных решений в области обеспечения сетевой и облачной безопасности, на наш взгляд, будут сосредоточен в решениях класса NGFW. В части аутсорсинговых услуг будут востребованы, не в последнюю очередь благодаря маркетинговым усилиям, решения класса SOC/MDR.

- Для продвижения собственных консалтинговых услуг для поставщиков решений рынка ИБ может быть интересен, в первую очередь, условно премиальный сегмент заказчиков (у которых годовая выручка превосходит 5 млрд руб.), где придется конкурировать не столько с интеграторами, сколько с собственной IT-службой заказчика.

4. **Инновационно-технологическая составляющая глобального развития ИБ решений до 2030 года, по нашему мнению, во многом будет направлена на обеспечение комплексной проактивной защиты с элементами искусственного интеллекта, в первую очередь, ориентированной на защиту сетевых и облачных решений, а в более долгосрочной перспективе – на перевод наиболее значимых коммуникаций на технологии квантового шифрования**

- Оставляя за скобками отдельные прикладные и узкоспециализированные инновации, в которых отечественные решения ИБ не испытывают недостатка, в качестве основных глобальных инновационных перспектив развития ИБ решений до 2030 года следует назвать технологии проактивной защиты на основе искусственного интеллекта, способные более точное обнаруживать угрозы и уязвимости, автоматически реагировать на атаки и обнаруживать аномалии. Наиболее перспективной точкой применения может быть защита сетевой и облачной инфраструктуры из-за высокой востребованности подобных решений, а также изначально высокой сетевой связности.

- В более долгосрочной обозримой перспективе, на наш взгляд, существенный практический потенциал имеют квантовые технологии применительно к решению задач квантовой криптографии.

Термины и сокращения

Используемые сокращения и основные термины

АСУ – автоматизированные системы управления;

ГК – группа компаний;

ИБ – информационная безопасность;

IT – информационные технологии;

МФЦ – многофункциональный центр;

ООО – общество с ограниченной ответственностью;

ПО – программное обеспечение;

СГТР – среднегодовой темп роста;

СНГ – Содружество Независимых Государств;

ФЗ – федеральный закон.

DDoS (Distributed Denial of Service*, Распределенный отказ в обслуживании)* – атака с множества устройств, создающая чрезмерную нагрузку на серверы с целью вызвать отказ обслуживания.

EDR (*Endpoint Detection and Response,* Обнаружение и реагирование на угрозы на конечных точках *)* – технология защиты информационных систем, которая обеспечивает постоянный мониторинг и быстрое обнаружение угроз на конечных устройствах.

IoT (*Internet of Things, И*нтернет вещей) – технология, позволяющая различным физическим устройствам обмениваться данными между собой.

LLM (*Large Language Model*, Большая языковая модель) – нейронная лингвистическая сеть, обученная на большом количестве данных для понимания и обработки текста.

MDR (*Managed Detection and Response,* Служба мониторинга, обнаружения и реагирования на угрозы) — Единая служба, объединяющая мониторинг, обнаружение и реагирование на угрозы. Предназначена, в первую очередь, для выявления атак и инцидентов безопасности в реальном времени, а также активного реагирования на них для снижения возможного ущерба.

MSS/ MSSP (*Managed Security Service / Managed Security Service Provider*, Управляемые сервисы кибербезопасности / Провайдер управляемых сервисов кибербезопасности) – провайдер отдельных управляемых сервисов кибербезопасности, в состав которых может входить: защита почтового трафика; мониторинг, обнаружение и реагирование на угрозы; управление уязвимостями; защита от DDoS-атак; защита веб-приложений; обучение и повышение осведомленности сотрудников в области ИБ; консультационная и экспертная поддержка. Принципиальные отличием MSS от аутсорсинга ИБ является отсутствие комплексного подхода к обеспечению информационной безопасности организации и фокусирование на ее отдельных составляющих (сервисах).

NGFW (*Next Generation Firewall*, Межсетевой экран нового/следующего поколения) – по сравнению с обычным межсетевым экраном выполняют более глубокую проверку сетевого трафика, идентифицирует и контролируют использование приложений, независимо от порта и протокола, обеспечивает идентификацию и контроль доступа пользователей, дает возможность проверки зашифрованного SSL-трафика, обеспечивает распознавание и блокировку атак на основе DNS-туннелей и прочее.

SOC (*Security Operation Center*, Центр мониторинга информационной безопасности) – комплексная система, которая объединяет оборудование, программное обеспечение, процессы и специалистов для защиты организации от киберугроз (может быть внутренней – в составе организации, внешней - как услуга, или гибридной).

Базовая классификация

Базовые классификация рассматриваемых решений

1. Сетевая и облачная безопасность	
Защита сетей	Виртуальная частная сеть (VPN)
	Сетевой доступ с нулевым доверием (ZTNA)
	Контроль доступа к сети (NAC)
	Межсетевой экран и универсальный шлюз безопасности (Firewall/UTM)
	Межсетевой экран нового поколения (NGFW)
	Системы обнаружения / предотвращения вторжений (IDS/IPS)
	Шлюз веб-безопасности, проксирование доступа (SWG)
	Защита электронной почты (SEG)
	Сегментация сети
Защита веб-приложений	Защита DNS (SecDNS)
	Защита от атак распределенного отказа в обслуживании (DDoS)
	Межсетевой экран для защиты веб-приложений / экран прикладного уровня (WAF)
	Безопасность API и защита приложений на уровне API
Защита облаков, виртуализации и контейнеризации	Брокер безопасности доступа к облаку (CASB)
	Средства защиты контейнеров (Container Security)
	Комплексная платформа защиты облачных приложений (CNAPP)
	Управление безопасностью облачной инфраструктуры (CSPM)
	Защита рабочих нагрузок в облаке (CWPP)
	Мониторинг и аналитика облачной и виртуальной инфраструктуры
	Управление доступом в облачных средах (CIEM)
	Облачный межсетевой экран
	Межсетевой экран уровня гипервизора
2. Анализ, контроль и реагирование на угрозы ИБ	
Анализ, контроль и управление уязвимостями и угрозами ИБ	Выявление и устранение уязвимостей (VM)
	Мониторинг поверхности атак (ASM)
	Симуляция атак и тестирование безопасности (BAS)
	Управление безопасностью конфигураций (CSAM)
	Управление событиями и информацией безопасности (SIEM)
	Аналитика сетевого трафика (NTA)
	Обнаружение и реагирование на сетевые угрозы (NDR)
	Расширенное обнаружение и реагирование в облаке (Cloud-native XDR)
	Аналитика поведения пользователей и сущностей (UEBA)
	Информация и аналитика по угрозам (TI)
Оркестрация и автоматизация реагирования на угрозы ИБ	Автоматизация безопасности и реагирования (SOAR)
	Платформа реагирования на инциденты (IRP)
	Автоматизация межсетевых экранов
Контроль безопасности кода приложений и тестирование приложений на проникновение	Статический анализ безопасности кода (SAST)
	Динамический анализ безопасности приложений (DAST)
	Анализ безопасности мобильных приложений (MAST)
	Интерактивный анализ безопасности приложений (IAST)
	Композиционный анализ кода (SCA)
	Тестирование на проникновение (CPT)

* под оценку Б1 структуры рынка ИБ.

Базовая классификация

Базовые классификация рассматриваемых решений

3. Защита конечных точек	
	Платформа защиты конечных точек (EPP)
	Обнаружение и реагирование на угрозы на конечных точках (EDR)
	Расширенное обнаружение и реагирование (XDR)
	Средства доверенной загрузки (АПМДЗ)
	Защита от несанкционированного доступа (НСД)
	Антивирус
	Защита конфиденциальных данных
	Информирование об утечках персональных данных и компрометации аутентификации
	Родительский контроль
4. Защита данных	
Защита информации	Системы предотвращения утечек данных (DLP)
	Управление доступом к данным (DAG)
	Контроль доступа к данным и аналитика их использования (DCAP)
	Защита базы данных (DBF)
	Виртуальная комната данных для безопасного обмена
Цифровая идентичность и защита данных	Криптографические средства защиты и шифрование данных
	Токенизация
	Маскировка данных
	Инфраструктура открытых ключей (PKI), средства управления ключами и сертификатами
	Таргетированное управление правами доступа к информации (IRM)
	Средства хранения секретов (Vault)
5. Управление доступом	
Защита доступа	Единый логин для всех систем / однократная аутентификация в информационных системах (SSO)
	Управление идентичностями и доступом (IGA)
	Управление идентификацией (IDM)
	Управление доступом и идентификацией (IAM)
	Многофакторная аутентификация (MFA)
	Управление идентификацией клиентов (CIAM)
	Обнаружение и реагирование на угрозы идентификации (ITDR)
	Провайдер идентификации (IDP)
	Аутентификация без паролей (NoPass)
Привилегированный доступ	Управление привилегированным доступом (PAM)
	Аппаратные токены и USB-ключи
6. Управление рисками и навыками ИБ, предотвращение мошенничества	
	Управление навыками ИБ (SA)
	Киберполигоны
	Управление рисками и соблюдение нормативных требований (GRC)
	Предотвращение цифрового мошенничества (антифрод)
	Разведка на основе открытых данных (OSINT)
	Изолированная среда для анализа угроз (Sandbox)
	Реагирование на инциденты и криминалистика (DFIR)
	Разведка угроз и реализация проактивного подхода к минимизации цифровых рисков (DRP)

Базовая классификация

Базовые классификация рассматриваемых решений

7. Проектные услуги	
	Консалтинг
	Аудит
	Поставка, внедрение и развертывание отдельных ИБ-решений
	Внедрение комплексных ИБ-проектов
	Тестирование на проникновение (Pentest)
	Образовательные услуги
8. Аутсорсинг и MSS	
	Услуги центра мониторинга и обеспечения кибербезопасности (SOC, MDR)
	Управляемые сервисы безопасности (MSS)
	Аутсорсинг процессов обеспечения ИБ
	Услуги технической поддержки средств и решений ИБ помимо стандартной поддержки поставщика

Контакты

Дмитрий Протас,
старший отраслевой аналитик

DProtas@alfabank.ru

Telegram-канал
«Масштабный бизнес»
для корпоративных
клиентов