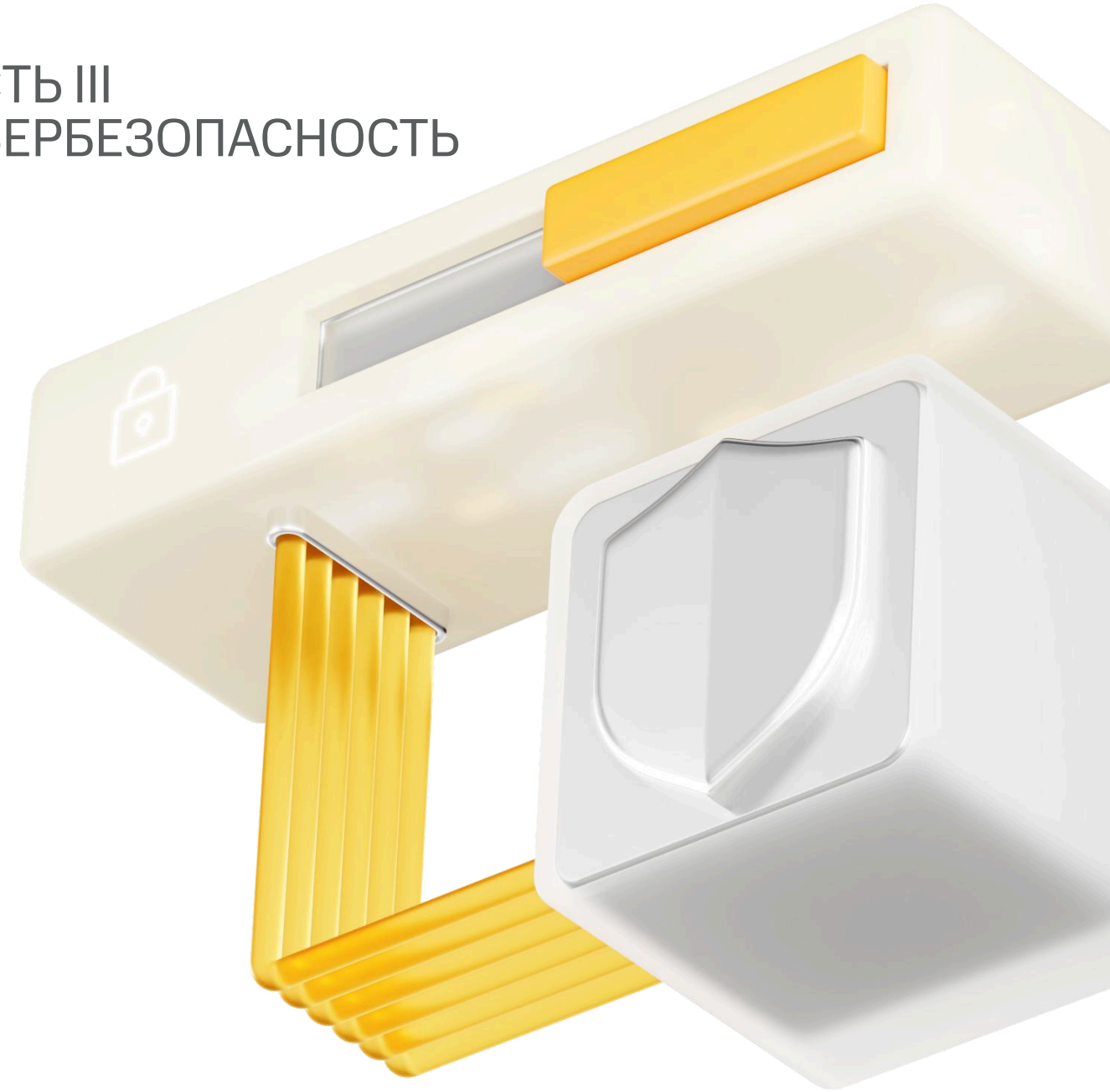
ТЕХНОЛОГИЧЕСКИЕ СТРАТЕГИИ БИЗНЕСА В РОССИИ

ЧАСТЬ III
КИБЕРБЕЗОПАСНОСТЬ



ТЕХНОЛОГИЧЕСКИЕ СТРАТЕГИИ БИЗНЕСА В РОССИИ

Исследование подготовлено Центром аналитики и исследований MWS

Вопросы и замечания по исследованию или идеи для коллаборации направляйте на почту: Intelligence_Team@mts.ru

Telegram

Сайт

ЭКСПЕРТЫ

Павел Воронин

Генеральный директор MWS

Игорь Зарубинский

Исполнительный директор MWS,
CEO MWS Cloud

Денис Филиппов

Генеральный директор MWS AI

Данила Егоров

Директор по бизнес стратегии MWS Cloud

Михаил Тутаев

Директор по продуктам MWS Cloud

Полина Ли

Руководитель центра аналитики
и исследований MWS Cloud

Галина Гайдаржи

Бизнес-аналитик MWS Cloud

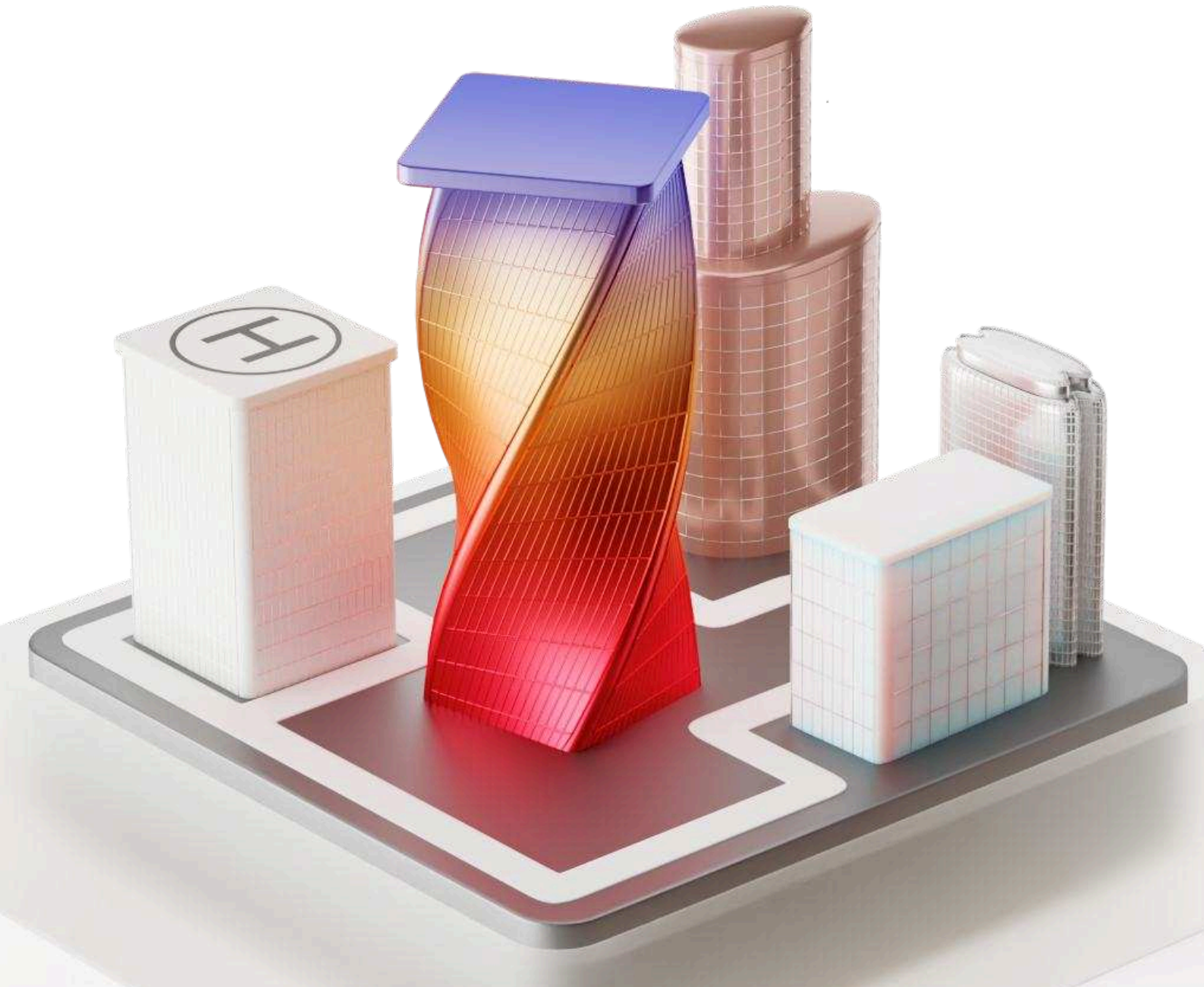
СОДЕРЖАНИЕ

ВВОДНАЯ ЧАСТЬ

ВВЕДЕНИЕ

ТАКСОНОМИЯ

МЕТОДОЛОГИЯ



ВВЕДЕНИЕ

Технологии в целом и ИТ-технологии для B2B развиваются в виде больших волн. Девяностые годы прошли под знаком персонального компьютера, софта и операционных систем для PC. Двухтысячные были временем, когда корпорации повсеместно внедряли интернет и монолитные платформы. В десятых годах компании мигрировали в облако. Каждая из волн полностью перестраивала ИТ-ландшафт.

> Мы как одна из ключевых бигтех-компаний в России видим, что ИИ-агенты уже сейчас радикально меняют подход к управлению бизнесом, клиентским сервисом и развитием цифровых продуктов — от автономной обработки рутинных задач до поддержки сложных управленческих решений в реальном времени. Мы создаем ведущие технологии: развиваем облако, строим платформы и дата-платформы, выпускаем инструменты для разработчиков, чтобы ИИ-агенты можно было встраивать напрямую в бизнес-процессы и масштабировать их эффект на всю экономику.

Павел Воронин
Генеральный директор MWS, первый вице-президент по ИТ МТС

В 2025 году мы наблюдаем, как новая технологическая волна — искусственный интеллект — стремительно формирует новый ИТ-ландшафт. При этом облака продолжают расти, количество компаний в России, обладающих объемом данных более 1 Петабайта, выросло с 10 до 29 всего за один год.

> Внедрение ИИ в течение следующих 5 лет породит новую ИТ-архитектуру, где AI, платформы и облако образуют единый стек технологий. На базе этого стека будут создаваться агенты ИИ — цифровые сотрудники. Продуктовой ценностью будет не софт, как инструмент, а сам результат выполнения бизнес-задачи. Пользователи софта превратятся из исполнителей задачи в руководителей агентов. Это сформирует совершенно новую технологическую экономику.

Игорь Зарубинский
Исполнительный директор MWS, CEO MWS Cloud

Создание любой технологии начинается с клиента. Именно наши клиенты говорят нам, какой продукт им нужен, указывают нам на недостатки и требуют улучшений. Мы бесконечно благодарны клиентам за эту обратную связь. Мы верим, что только глубокое знание задач клиента рождает великие технологии. В этом году мы решили сфокусироваться на трех технологических областях, которые в России меняются наиболее динамично. Это облака, искусственный интеллект и кибербезопасность. Исследование построено на базе ответов представителей 700 российских компаний. Мы очень благодарны участникам за то, что уделили нам время и предоставили ответы.

> В MWS мы следуем открытому подходу, поэтому делимся с вами результатами исследования и выкладываем исследование в открытом доступе. Мы надеемся, что исследование поможет вам в вашей очень непростой и очень нужной работе. Спасибо за то, что вы делаете!

Данила Егоров
Директор по бизнес стратегии MWS Cloud

ТАКСОНОМИЯ

Основой подхода, применяемого в исследовании, стала структура ИТ-рынка, впервые сформированная в исследовании «Перспективы ИТ-рынка». Согласно таксономии MWS, весь рынок сегментирован на 3 вертикали: (1) Software (Программное обеспечение), (2) Hardware (Аппаратное обеспечение), (3) IT-Services (ИТ-услуги). Каждая из вертикалей декомпозирована на составные элементы и включает решения по каждому из 3 основных технологических направлений: облака, кибербезопасность и искусственный интеллект.

За период с 2019 по 2024 годы доля российского ИТ-рынка в мировом была стабильна и составляла от 1,1 до 1,3%. Тем не менее продолжающаяся цифровая трансформация ключевых отраслей экономики способствует росту проникновения ИТ в ВВП страны. В период с 2023 по 2024 году прирост составил 0,27 п.п., что выше аналогичного показателя для других стран.

Темпы роста российского ИТ-рынка в 2019–2024 годах сопоставимы с мировыми показателями. Однако структура затрат существенно отличается. В России традиционно наблюдается более низкая доля вертикали Hardware — во многом вследствие географической и производственной специализации других стран на выпуске высокотехнологичных компонентов, а также возрастающей роли программных решений. Дополнительно на динамику вертикали Hardware влияет продолжающийся переход бизнеса на облачные модели потребления, который снижает потребность в закупке собственных вычислительных мощностей. Расширение и повышение эффективности облачных решений стимулируют этот тренд, способствуя оптимизации капитальных затрат конечных потребителей.

> “ Вертикаль Software демонстрирует устойчивый рост — как в России, так и на глобальном рынке. Среднегодовой прирост доли этого сегмента в ИТ-рынке оценивается на уровне около 2% в течение 2019–2024 годов. Основным драйвером выступает переход бизнеса на подписочные модели, которые делают ПО более доступным для компаний разных масштабов и снижают барьеры для апробации новых технологических решений.
>
> 
>
> **Павел Воронин**
> Генеральный директор MWS

Сегмент ИТ-услуг (IT-Services) показывает наименьшие темпы роста среди трех ключевых вертикалей. На динамику этого направления влияют макроэкономическая нестабильность, насыщенность отдельных рынков, а также сдвиг в сторону no-code и low-code решений, частично вытесняющих традиционные услуги. Вместе с тем ожидается, что рост числа киберугроз и активное развитие продуктов на базе искусственного интеллекта могут поддержать спрос на ИТ-услуги в краткосрочной перспективе.

Отдельного внимания заслуживает облачный рынок: ожидается, что к 2030 году доля данного рынка от всего ИТ-рынка России достигнет 6%. Высокие среднегодовые темпы роста в денежном выражении (32% за период 2021–2024 годов) создают предпосылки для заметного развития рынка в среднесрочной перспективе. Облачные решения становятся одним из ключевых элементов стратегии цифровой трансформации бизнеса в России, обеспечивая гибкость и снижение инфраструктурных затрат.

Структура российского ИТ-рынка

	2023	2024	2025	2026	2027	2028	2029	2030
Размер рынка РФ, млрд руб.	**2 702**	**3 302**	3 992	4 700	5 478	6 260	7 090	8 004
Hardware, млрд руб.	725	842	945	1 085	1 249	1 429	1 626	1 839
Software, млрд руб.	1 063	1 404	1 816	2 236	2 686	3 105	3 548	4 031
IT-Services, млрд руб.	913	1 056	1 231	1 379	1 543	1 726	1 916	2 134
Hardware, %	27%	25%	24%	23%	23%	23%	23%	23%
Software, %	39%	43%	45%	48%	49%	50%	50%	50%
IT-Services, %	34%	32%	31%	29%	28%	28%	27%	27%

Доля облачного сегмента в российском ИТ-рынке за 2023–2030 гг.

	2023	2024	2025	2026	2027	2028	2029	2030
Доля Cloud в ИТ-рынке РФ	4,4%	5,1%	5,2%	5,3%	5,4%	5,6%	5,8%	6,0%

Особый интерес в развитии облачных решений представляют подсегменты IaaS / Paas. Они составляют порядка 65% от всего рынка облачных решений и являются драйверами развития индустрии. Рост спроса обеспечивается не только повышением востребованности классических решений, но и развитием технологий искусственного интеллекта.

Проникновение российского ИТ-рынка в экономику страны

2,2%
Доля ИТ
в ВВП РФ 2025

→

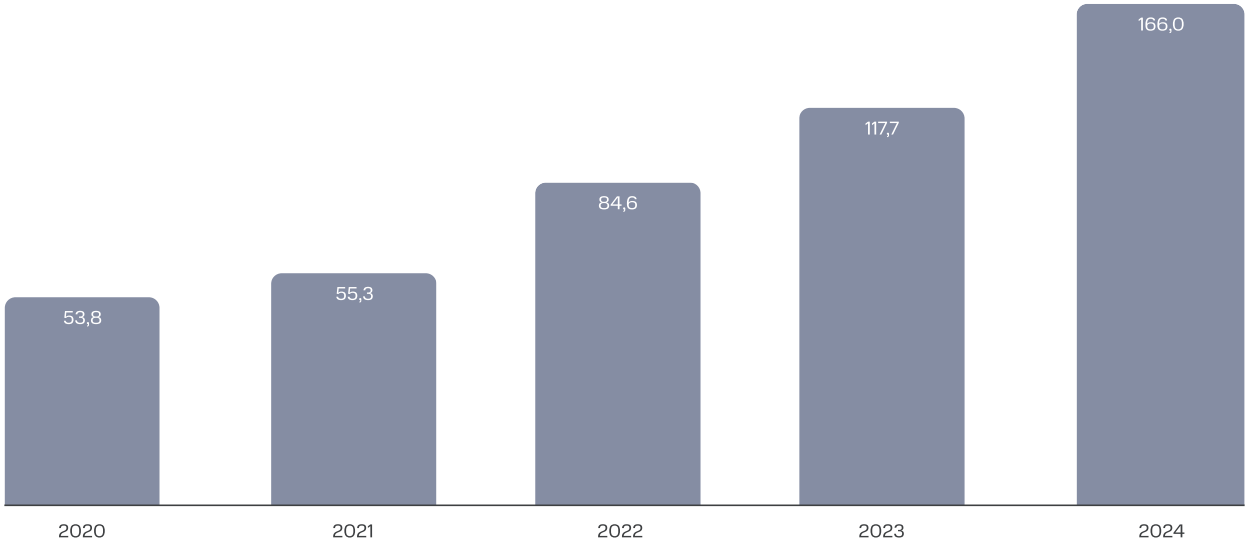
3,1%
Доля ИТ
в ВВП РФ 2030

Подсегмент IaaS / PaaS характеризуется одним из наиболее высоких темпов роста в структуре российского ИТ-рынка. В 2021–2024 годах среднегодовой прирост составил около 30%, что указывает на стремительное распространение облачных технологий в корпоративном секторе. Тем не менее, темпы роста IaaS / PaaS демонстрируют постепенное замедление, отражающее повышение зрелости рынка: в 2024 году произошло увеличение объемов на 32% в сравнении с предыдущим годом.

Подробнее о структуре ИТ-рынка в исследовании «Перспективы ИТ-рынка».

Объем облачного сегмента в российском ИТ-рынке

Объем рынка указан в млрд руб.



> Несмотря на прогнозируемый рост всех направлений ИТ-рынка в среднесрочной перспективе, сегодня мы наблюдаем качественное изменение его структуры в сторону роста Software. Ожидаемый среднегодовой темп прироста программного обеспечения в период 2023-2030 гг составляет 20,6% в год, при прогнозируемом приросте ИТ-рынка на 17,4% в год, что отражает переход бизнеса к более гибким и экономичным моделям потребления. Ускоряющаяся цифровизация ключевых отраслей создает фундамент для устойчивого роста доли ИТ в экономике страны. В наше стратегическое видение мы закладываем понимание, что "софт ест ИТ-рынок".

Игорь Зарубинский
Исполнительный директор MWS, CEO MWS Cloud

МЕТОДОЛОГИЯ

Данное исследование является логическим продолжением предыдущего исследования «Перспективы ИТ-рынка» и фокусируется на оценке ситуации со стороны спроса. Его результаты будут особенно полезны компаниям, ориентированным на повышение эффективности за счет внедрения цифровых технологий, в частности, командам аналитики, продаж, продуктового менеджмента, стратегии и маркетинга, а также руководителям, принимающим ключевые решения.

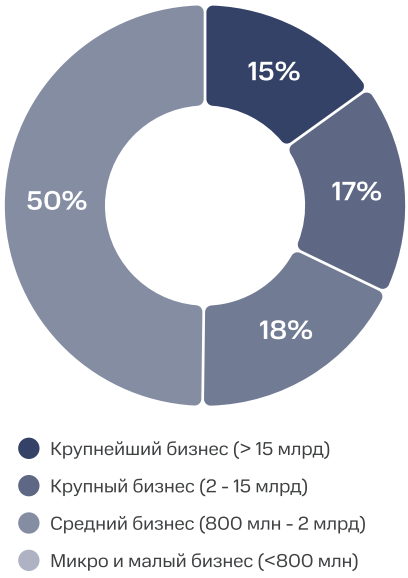
Основой исследования является анкетный опрос представителей более чем 700 российских компаний. Для расширения понимания отдельных аспектов исследования дополнительно были проведены глубинные интервью с частью респондентов.

В выборку вошли исключительно компании, которые подтвердили наличие бюджетов на закупку, развитие или использование в операционной деятельности хотя бы одной из трех технологий: облачных решений, кибербезопасности и искусственного интеллекта.

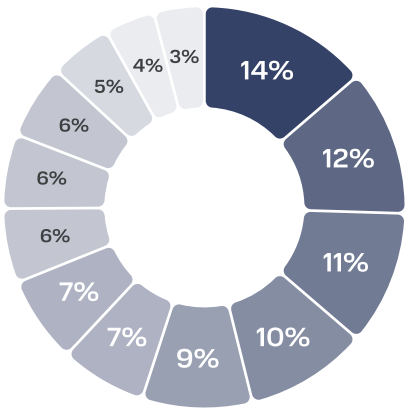
Респонденты исследования сбалансированно представляют различные сегменты бизнеса. Половину выборки составляют микро- и малые компании, оставшиеся 50% — представители среднего, крупного и крупнейшего бизнеса, причем эти доли распределены равномерно.

Структура респондентов по сегментам бизнеса

Размер выручки, руб.



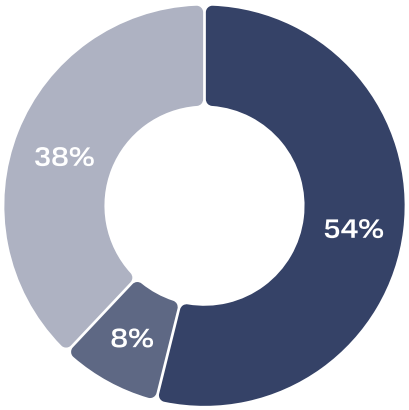
Структура респондентов по индустриям



- ИТ
- Промышленность
- Ритейл
- Недвижимость и строительство
- Транспорт и логистика
- Финансы и страхование
- Развлечения и медиа
- Здравоохранение
- Профессиональные услуги
- HoReCa
- Наука и образование
- Добыча и переработка полезных ископаемых
- Прочее

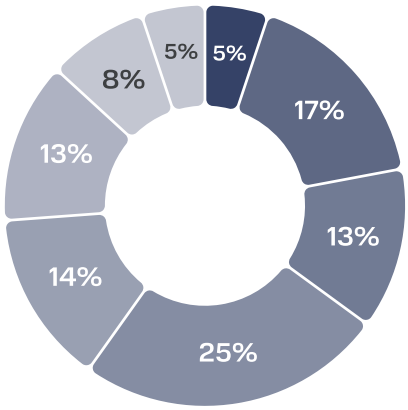
Большинство компаний-респондентов расположены в Москве и Московской области, однако свыше трети опрошенных представлены региональным бизнесом, что обеспечивает широкий географический охват. По численности персонала выборка также разнообразна: 26% компаний относятся к малому бизнесу с численностью менее 100 сотрудников, доля крупных (от 1 000 до 4 999 сотрудников) и крупнейших компаний (от 5 000 до 9 999 сотрудников) составляет 13% и 17% соответственно.

Структура респондентов по главному офису компании



- Москва и МО
- Санкт-Петербург и ЛО
- Регионы

Структура респондентов по численности сотрудников

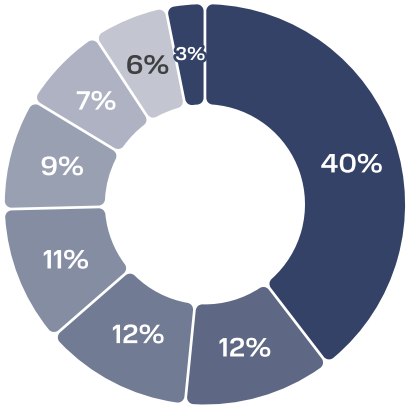


- 5 000 – 9 999
- 1 000 – 4 999
- 500 – 999
- 100 – 499
- 50 – 99
- 10 – 49
- < 10

Опрос проводился среди специалистов, компетентных в вопросах развития цифровых решений. Отбор сотрудников разных уровней обусловлен индустрией и профилем деятельности: организация процессов цифровой трансформации в компаниях сильно зависит от их отраслевой специфики и внутренних бизнес-процессов. Более половины участников представляют высший менеджмент, что подчеркивает высокий уровень экспертизы представителей компаний из выборки.

Таким образом, структура выборки обеспечивает репрезентативность для всех компаний России, уже внедряющих или использующих рассматриваемые технологии. Высокий уровень компетенций респондентов гарантирует достоверность собранных данных и позволяет делать обоснованные выводы о текущем и потенциальном спросе на облачные решения, технологии кибербезопасности и искусственный интеллект в российском бизнесе.

Структура респондентов по должности сотрудника, проходившего опрос



- Директор / Руководитель (ИТ)
- Директор / Руководитель (бизнес)
- Менеджер (ИТ)
- Специалист / Аналитик (ИТ)
- Менеджер (бизнес)
- Специалист / Аналитик (бизнес)
- Другое (бизнес)

МТС WEB SERVICES

Бигтех-компания, предоставляющая облачные и AI-сервисы и платформенные решения под разные задачи бизнеса: от работы с данными до разработки продуктов и оптимизации процессов

15

зон доступности на базе ЦОД уровня Tier III

~ 280 000

километров собственных каналов связи

Поддержка стандартов

УЗ-1, ГИС К1, 152-ФЗ, PCI DSS, ГОСТ Р 57580

№ 1

в рейтинге IaaS Enterprise 2024

ТОП-5

русскоязычных ИИ-решений по оценке Mera

Топ-3

бенчмарка NIST по качеству алгоритмов распознавания лиц

15 млн

экосистемных пользователей

№ 1

в рейтинге GPU CLOUD

№ 1

LLM по точности кодинга в России

КЛЮЧЕВЫЕ КОМПЕТЕНЦИИ MWS

Сервисы для разработки

- Импортонезависимый стек технологий
- Более 30 платформ, ускоряющих разработку в крупном бизнесе
- Команда разработки мирового уровня (10 000 человек)

Искусственный интеллект

- Собственная большая языковая модель (LLM) для бизнеса
- Вошли в мировой топ-3 по ИИ-технологии распознавания лиц
- Создали лучший сервис синтеза и распознавания речи
- Сильнейшая команда в РФ; более 800 специалистов по ИИ

Бизнес-приложения

- Разработали no-code решение для управления проектами и совместной работы
- Обустроили 100+ тыс. рабочих мест для крупнейшего бизнеса в стране: почта, мессенджеры, АКС, ВКС
- Защищённая инфраструктура для ERP-систем

Управление данными

- Решения для хранения промышленных объёмов данных
- Гипермасштабируемые on-prem хранилища данных
- AI-инструменты в данных
- Лучшая команда дата-инженеров в России: 700 специалистов

Облачная инфраструктура

- Собственная облачная платформа уровня мирового гиперскейлера
- ИИ-облако и суперкомпьютер
- Полностью импортозамещённое облако
- Собственные on-prem-платформы для создания гибридных облаков
- Комплексные проекты Киберзащита инфраструктуры по международным стандартам
- Сильнейшая команда инженеров: 500 специалистов

ТЕХНОЛОГИЧЕСКИЕ СТРАТЕГИИ БИЗНЕСА

ИТ-БЮДЖЕТЫ

В 2024 г. размер ИТ-бюджета российских компаний составил в среднем 2-3% от годовой выручки, что сопоставимо с мировой практикой: так, согласно исследованию Gartner, в 2024 году медианное значение ИТ-расходов фирм по всему миру равнялось 3,1% от выручки. В абсолютном выражении у большинства (>65%) опрошенных российских компаний годовой ИТ-бюджет не превышает 100 млн руб. и лишь у 14% фирм он превышает 1 млрд руб.

> Наибольший ИТ-бюджет в 4 индустриях: ИТ, финансы и страхование, добыча и переработка полезных ископаемых, развлечения и медиа

ИТ-бюджеты респондентов по индустриям

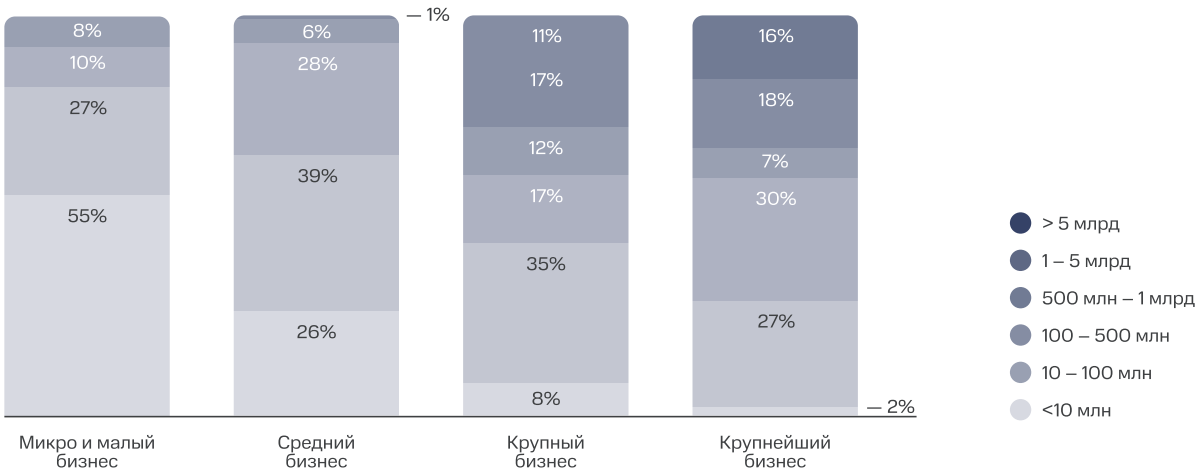
	< 10 млн	10 – 100 млн	100 – 500 млн	500 млн – 1 млрд	1 – 5 млрд	> 5 млрд
ИТ	24%	28%	13%	13%	11%	10%
Финансы и страхование	33%	19%	11%	8%	20%	9%
Добыча и переработка полезных ископаемых	33%	32%	8%	7%	11%	9%
Развлечения и медиа	22%	25%	36%	6%	3%	8%
Здравоохранение	33%	39%	15%	4%	4%	5%
Профессиональные услуги	53%	25%	5%	12%	1%	4%
HoReCa	43%	30%	13%	6%	5%	3%
Наука и образование	37%	27%	20%	4%	3%	3%
Ритейл	54%	26%	8%	4%	4%	3%
Недвижимость	54%	26%	9%	3%	5%	2%
Транспорт и логистика	45%	23%	18%	10%	1%	2%
Промышленность	46%	37%	7%	6%	4%	2%

Сохраняется высокий уровень дифференциации распределения ИТ-бюджетов в зависимости от отраслевой принадлежности и размера компании. Наибольшие ИТ-затраты приходятся на компании ИТ-рынка, чьи продукты преимущественно основаны на цифровых решениях, а также на крупнейшие фирмы из традиционных для экономики отраслей (промышленность, добыча полезных ископаемых), которые также активно инвестируют в инструменты для автоматизации производственных процессов и повышения эффективности.

Ожидаемо, что в наибольшей степени размер ИТ-бюджета связан с размером выручки: для подавляющего числа компаний (>68%) микро и малого бизнеса (выручка <800 млн руб.) ИТ-бюджет не превышает 10 млн руб., тогда как у крупнейших фирм с выручкой >15 млрд руб. наблюдается значительно большее разнообразие размеров бюджетов. Так, более трети крупнейших компаний имеет ИТ-бюджет более 1 млрд руб.. По мере роста выручки увеличивается вариативность размеров ИТ-бюджетов, что отражает сложность и многогранность задач, решаемых компаниями: от базовой автоматизации и поддержки действующей ИТ-инфра-структуры до внедрения более продвинутых AI / ML-решений.

ИТ-бюджеты респондетов по сегментам бизнеса

Каждый столбец — сегмент бизнеса на основе выручки, цветами обозначен размер ИТ-бюджета



Эффективное управление ИТ-бюджетом для большинства компаний предполагает регулярный пересмотр в зависимости от изменения приоритетов бизнеса и внешней конъюнктуры. Основная доля компаний вне зависимости от размера выручки (>60%) осуществляет корректировку ИТ-бюджета от 1 до 2 раз в год.

По мере увеличения размера компании увеличивается и частота пересмотра ИТ-бюджета: среди микро и малого бизнеса (выручка до 800 млн руб.) чаще всего встречаются компании, корректирующие ИТ-бюджет реже одного раза в год, что может свидетельствовать об ограниченной зрелости и необходимости использования механизмов актуализации затрат. При этом, для крупнейших компаний (с выручкой >15 млрд руб.) наиболее характерна актуализация бюджетов на ежегодной основе, что может быть обусловлено длительным циклом согласования и утверждения финансовых показателей, а также постановкой стратегических целей годового планирования.

В рамках исполнения ИТ-бюджетов величина расходов на различные технологические решения распределяется неравномерно. По результатам опроса, на три ключевых технологических направления — облачные решения, системы кибербезопасности (КБ) и искусственного интеллекта (ИИ) — приходится 17% от общей суммы ИТ-бюджетов российских компаний.

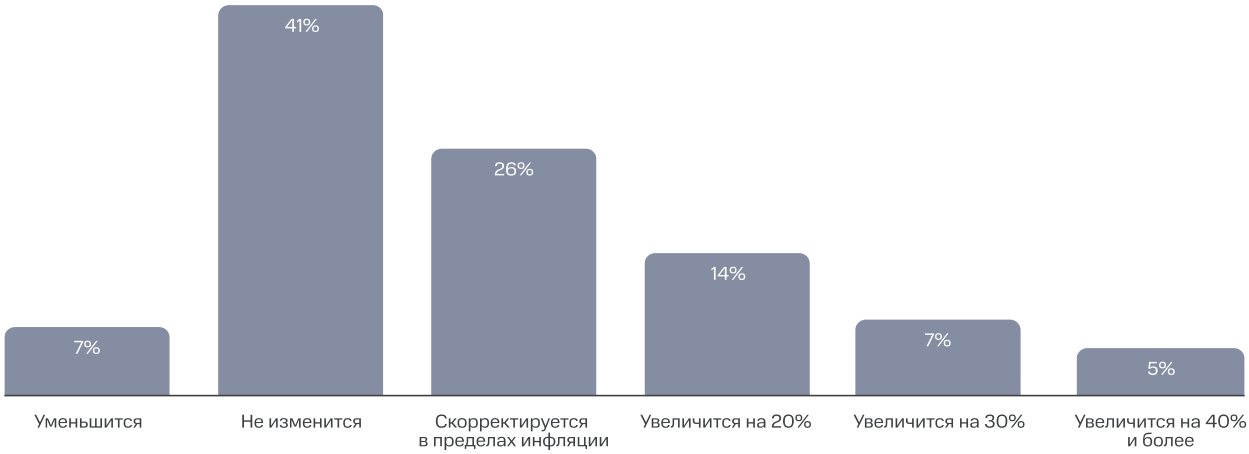
По величине расходов на данные технологические направления отечественные компании все еще отстают от международных игроков, у которых сопоставимые затраты могут достигать 50%. Кроме того, отличается и структура ИТ-бюджетов в мире и России: в международной практике лидирующие позиции занимают облачные решения, второе место — КБ, а третье место — ИИ. В России же по объемам бюджета лидирует КБ, на втором месте облака, на третьем — ИИ. Различия могут быть связаны с растущими угрозами в области защиты информации в России. Растет общее число кибератак, особенно актуальны DDoS-атаки и атаки на крупных игроков с целью последующей компрометации чувствительных данных, также увеличивается количество APC-группировок, атакующих Россию и страны СНГ. Ответом на возрастающие киберугрозы является усложнение законодательства: в 2024 году произошли ужесточения 187-ФЗ и 152-ФЗ, разработан новый регламент ФСТЭК.

Облачные технологии и кибербезопасность имеют нелинейное распределение в ИТ-бюджете: их доля увеличивается на 1–2 п. п. при росте выручки, достигая максимума у средних компаний (выручка от 800 млн руб. до 2 млрд руб.), после чего происходит снижение долей этих технологий. Данная тенденция может быть обусловлена высоким минимальным порогом затрат, необходимым для развертывания технологий кибербезопасности и при этом сравнительно низкой стоимостью дальнейшего масштабирования и поддержания работоспособности решений. Доля ИИ в структуре сохраняется в пределах 2-4% и не имеет значительных различий в зависимости от размера выручки компании.

> В условиях усложнения угроз и усиления нормативного давления рынок уже движется к более взвешенному распределению инвестиций между базовой ИТ-инфраструктурой, кибербезопасностью и передовыми цифровыми решениями. При этом вклад ИТ-сектора в мировой ВВП достигает порядка 2,62% и превышает аналогичный показатель в России на 43%. Для выхода на соответствующий уровень, необходим опережающий рост инвестиций прежде всего в наиболее перспективные направления ИТ — облачные сервисы и решения на базе искусственного интеллекта, которые формируют новый уровень эффективности и управляемости бизнеса.

Игорь Зарубинский
Исполнительный директор MWS, CEO MWS Cloud

Ожидаемое изменение ИТ-бюджетов в 2025 году по сегментам бизнеса



Инвестиции в облачные технологии, КБ и ИИ становятся стандартной статьей ИТ-бюджета в самых разных секторах — от ритейла до промышленности. Это подтверждает рост зрелости цифровых стратегий и распространение ИИ-практик за пределами ИТ и финансов. Высокий уровень инвестиций в традиционно менее цифровых отраслях свидетельствует о том, что технологическое развитие и трансформация экономики ускоряются — важной составляющей данного направления является внедрение облаков, средств КБ и ИИ.

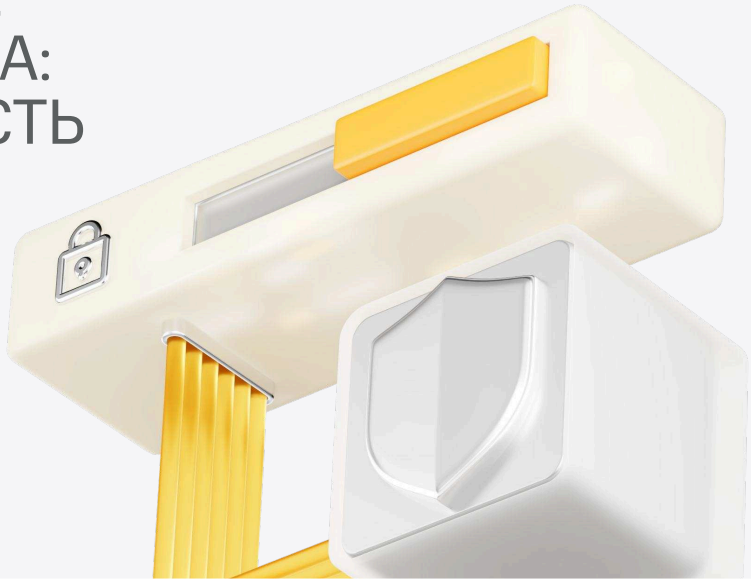
Только 28% опрошенных компаний планирует расширить размер бюджета на рассматриваемые технологии более, чем на уровень инфляции. Лидирующим направлением для расширения потребления является искусственный интеллект.

Среди всех респондентов наблюдается прямая зависимость между размером выручки компаний и масштабами планируемого изменения потребления: чем выше доходы организации, тем чаще фирмы декларирует планы наращивания инвестиций и тем значительнее величина роста. Данная закономерность прослеживается для всех категорий технологий, за исключением облачных решений, где потенциальный объем расширения использования остается более равномерным в зависимости от размера бизнеса. Наибольший же рост потребления планируется для ИИ, что обусловлено низкими объемами текущего внедрения, а также значительным ожидаемым потенциалом повышения эффективности бизнес-процессов практически во всех отраслях.

TOP-5 индустрий по затратам на облако, КБ и ИИ в ИТ-бюджете

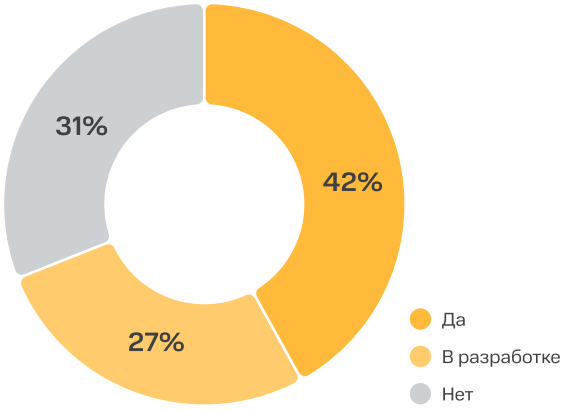
ИТ
Финансы и страхование
Развлечения и медиа
Ритейл
Добыча и переработка полезных ископаемых

ТЕХНОЛОГИЧЕСКИЕ СТРАТЕГИИ БИЗНЕСА: КИБЕРБЕЗОПАСНОСТЬ



Обеспечение информационной безопасности становится неотъемлемой частью устойчивой цифровой инфраструктуры, необходимой как для управления производственными процессами, так и для эффективной работы с большими данными и ИИ. Согласно данным опроса, 42% компаний уже имеют сформированную стратегию по КБ, ещё 27% находятся на этапе её разработки. Это подтверждает, что системный подход к анализу уязвимостей и управлению рисками получает всё большее распространение. Фокус смещается в сторону более широкого системного управления КБ во всех сегментах, что отражает общерыночную установку на минимизацию киберрисков и подготовку базы для последующих инвестиционных этапов в цифровизацию.

Наличие стратегии по внедрению КБ

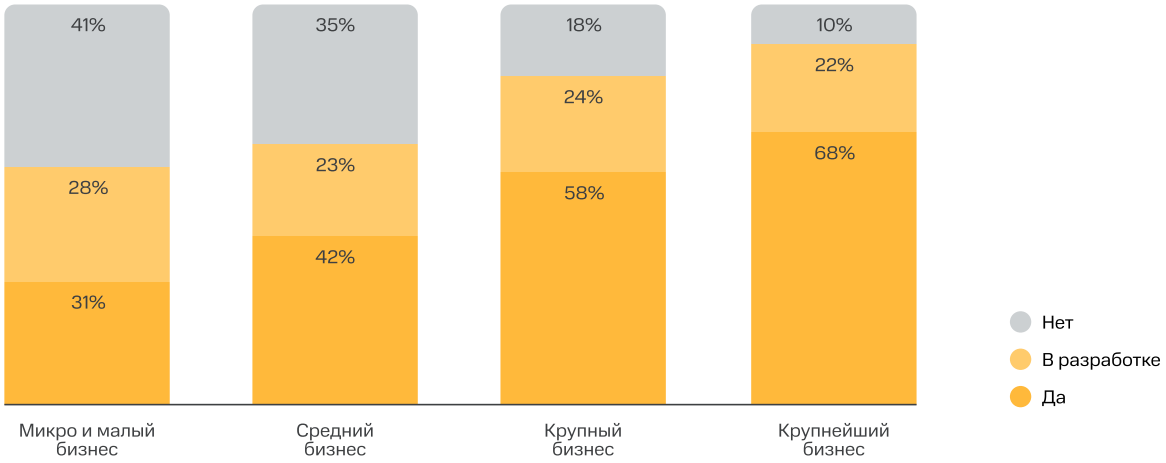


> Сегодня рынок облачных решений для кибербезопасности демонстрирует качественный сдвиг — защита информации перестает быть локальной задачей отдельных подразделений и становится фундаментом устойчивой цифровой экосистемы компаний. Все больше организаций подходят к вопросам КБ стратегически, выстраивая системные модели управления рисками и уязвимостями. Этот тренд отражает зрелость рынка и готовность бизнеса инвестировать в долгосрочные инструменты, обеспечивающие надежность обработки больших данных и внедрение ИИ.

Михаил Тутаев
Директор по продуктам MWS Cloud

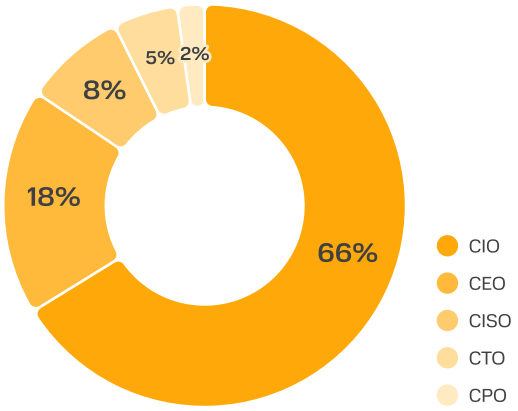
Зависимость уровня зрелости стратегий КБ от масштаба бизнеса прослеживается достаточно чётко. Среди крупнейших компаний (с выручкой >15 млрд руб.) стратегия КБ сформирована только в 68% случаев, тогда как у предприятий с выручкой <800 млн руб. этот показатель составляет лишь 31%. При этом, разработка стратегий по КБ практически одинаково характерна для компаний малого и среднего сегмента. Для них это во многом отражает процесс догоняющего развития и закрытия текущих уязвимостей. В то же время у крупных компаний зачастую уже выстроена целевая архитектура КБ, что снижает долю тех, кто находится именно в стадии разработки стратегии.

Стратегия по внедрению КБ по сегментам



Наибольшее влияние на принятие решений в области информационной безопасности, как и в случае с облачными технологиями, принадлежит CIO — руководителю ИТ-направления. Его назвали ключевым лицом, принимающим решения (ЛПР), 66% опрошенных компаний.
Это подтверждает сохраняющийся уклон в ИТ-домен, когда управление КБ воспринимается прежде всего как зона ответственности технического блока.

Ключевые сотрудники (ЛПР) в процессе принятия решения о внедрении КБ



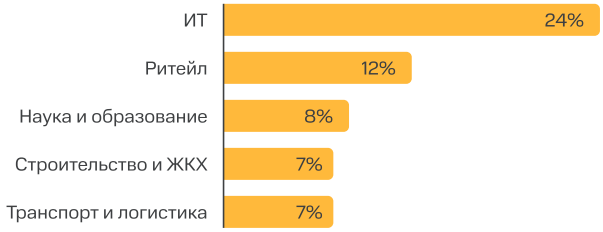
Для большинства компаний процесс внедрения средств информационной безопасности оказывается достаточно быстрым: у 73% он занимает не более полугода. Наиболее распространённый срок — от одного до трёх месяцев (31%), за ним следует период в 3–6 месяцев (24%).

Такие результаты демонстрируют, что для значительной части бизнеса проекты по КБ реализуются в достаточно сжатые сроки, что может говорить либо о типовом характере внедряемых решений, либо о высокой степени их готовности к быстрой интеграции в существующую инфраструктуру. Доля компаний, у которых проекты по КБ длятся более года, составляет лишь 14%, что подчеркивает их исключительность и, вероятно, указывает на масштабные или специализированные инициативы в крупных организациях.

Количество кибератак в 2025 году выросло на 30%

Актуальность внедрения средств безопасности обусловлена не только нормативными требованиями. 35% респондентов столкнулись с DDoS-атаками в 2024 году.
При этом наблюдается прямая зависимость: чем больше компания, тем выше вероятность подобной атаки. Среди крупных компаний, около 50% подвергались DDoS-атакам, в то время как среди респондентов крупнейшего бизнеса этот показатель достигает 60%.

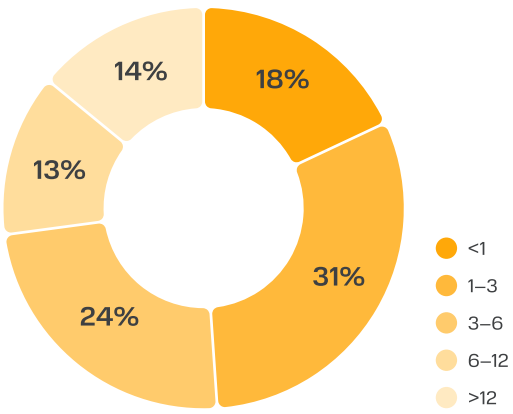
DDoS-атаки в 2024 году по индустриям



За 2025 год зафиксирован рост кибератак более чем на 25%. Наиболее масштабными кейсами стали кибератаки на транспортные и промышленные компании, а также компании сектора ритейл. Так, одна из крупнейших атак на телеком-оператора привела к выводу из строя ключевых элементов сети и ограничения доступа для клиентов из 4 субъектов РФ. Другая атака, произведенная на одного из крупных игроков промышленного сектора. Злоумышленники взломали внутренние сервисы, ограничили доступ к данным. В результате, были остановлены операционные процессы, нарушены логистические цепочки. Последствиями кибератак являются не только нарушение бизнес-процессов и компрометация данных предприятия, но и допол- нительные проверки со стороны регуляторов, а также риски уголовного преследования топ-менеджмента в случае выявленных нарушений эксплуатации средств хранения, обработки или передачи информации. Согласно проведенному опросу, отраслевая специфика значительно влияет на частоту атак: наиболее часто DDoS-атакам подвергались компании из ИТ-сектора, ритейла и научных учреждений. Такие данные говорят о том, что DDoS-атаки остаются актуаль-ной угрозой для бизнеса, особенно для крупных компаний и определенных отраслей. Это под-черкивает значимость внедрения эффективных мер по кибербезопасности для защиты от подобного рода атак.

Развертывание средств информационной безопасности наиболее распространено в собственной инфраструктуре: On-Premise решения используют 43% респондентов.
Это объясняется необходимостью полного контроля над системой и данными, особенно в условиях растущих требований к конфиденциальности и соблюдению регуляторных норм. На втором месте — гибридное облако (32%), которое чаще позволяет сохранить баланс между экономической эффективностью и надежностью в том числе путем обработки чувствительных данных, включая коммерческую тайну и персональные данные клиентов. Такой выбор даёт компаниям возможность совместить преимущества облачных технологий с защищенным управлением доступом и сегментацией данных.

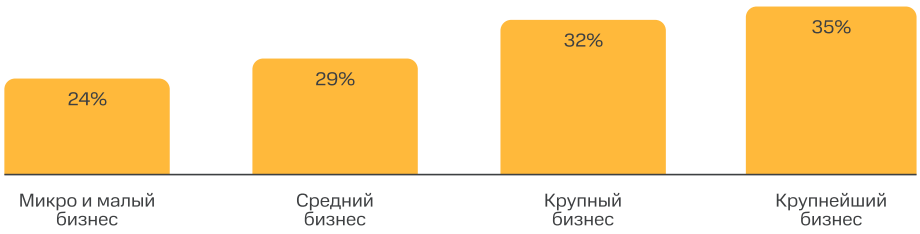
Длительность процесса внедрения средств КБ в месяцах



Доля использования частных и локальных решений возрастает с увеличением размера бизнеса: среди крупнейших компаний (с выручкой >15 млрд руб.) On-Premise и Private используют уже 50%. Для крупного бизнеса характерна более избирательная модель размещения критичных компонентов КБ вне публичных инфраструктур, что подтверждает стратегический приоритет защиты данных и минимизации внешних рисков.

Развитие получают multi кибербез решения

Доля средств КБ, используемых компаниями в облаке по сегментам бизнеса



По мере увеличения масштабов бизнеса возрастает и средняя доля средств КБ, вынесенных в облако. Так, у компаний микро и малого бизнеса (с выручкой < 800 млн руб.) эта доля составляет в среднем 24%, тогда как у крупнейших предприятий — уже 35%. Однако для подавляющего большинства компаний характерна избирательная модель использования облачных КБ-сервисов: 79% респондентов разместили в облаке до 30% своих средств КБ, что подчеркивает традиционно высокое значение локальных решений для корпоративных систем безопасности.

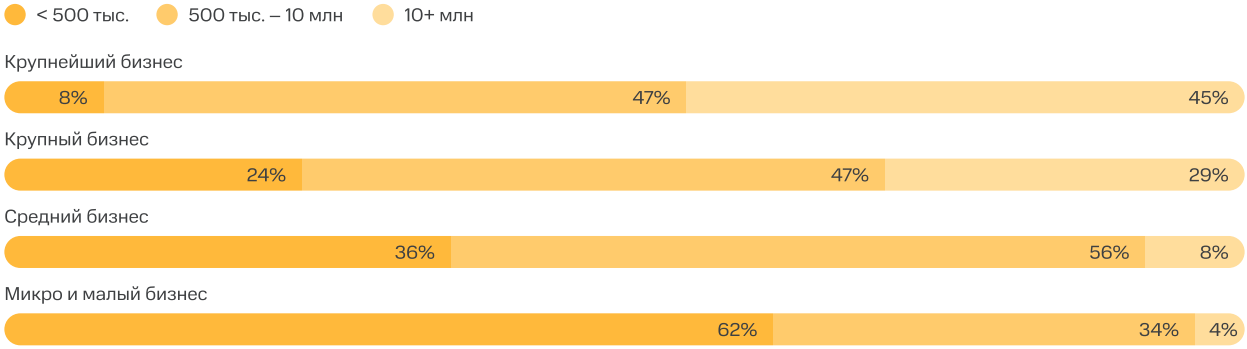
Отраслевой срез показывает, что лидерами по доле средств КБ в облаке являются ИТ, сегмент развлечений и медиа, а также наука и образование (средняя доля около 36%). Это связано с высокой цифровой зрелостью этих индустрий и значительным количеством облачных сервисов, уже встроенных в их операционные модели. При этом для транспорта и ритейла также характерны высокие значения данного показателя (24-27%), что отражает потребность в быстром масштабировании средств КБ для защиты распределенной инфраструктуры и клиентских данных.

Распределение годовых затрат на КБ среди компаний различного масштаба в полной мере отражает структуру корпоративных бюджетов. По мере уменьшения выручки заметно, как концентрация бюджетов смещается в сторону нижних диапазонов. Например, для сегмента микро и малого бизнеса основные траты сосредоточены в зоне до 500 тыс. руб., что подтверждает более сдержанные возможности таких компаний в области КБ и отражает ограниченный объем инвестиций в специализированные инструменты.

Доля от всех средств КБ, использующихся в облаке по индустриям

	Среднее значение
ИТ	36%
Ритейл	27%
Строительство и ЖКХ	19%
Транспорт и логистика	24%
Профессиональные услуги	23%

Годовой объем затрат на КБ по сегментам бизнеса



Наибольшая диверсификация диапазонов годовых облачных затрат на информационную безопасность фиксируется в индустриях ИТ и транспорта. Это демонстрирует разветленную структуру потребления КБ-решений, от типовых недорогих сервисов для защиты каналов связи и пользовательских устройств до комплексных систем мониторинга и управления инцидентами на уровне инфраструктуры.

В ТОП-5 по объему затрат вошли ИТ, финансовый сектор, развлечения и медиа, добыча и переработка, здравоохранение. Для этих отраслей характерно устойчивое смещение затрат в диапазон более 10 млн руб., что отражает зрелый спрос на облачные сервисы КБ и наличие регламентов, требующих системного подхода к обеспечению защиты данных клиентов и финансовых транзакций.

С точки зрения рисков и отраслевых драйверов, распределение расходов выглядит закономерно: ИТ-индустрия инвестирует в КБ для защиты собственных платформ и клиентских данных, финансы и ритейл — для минимизации угроз мошенничества и обеспечения регуляторного соответствия, здравоохранение — для охраны интеллектуальной собственности и клинических данных. Такое распределение отражает не только разные уровни зрелости КБ-стратегий, но и специфику угроз, с которыми сталкиваются отрасли.

> Несмотря на то, что локальные установки по-прежнему доминируют — особенно среди крупнейших компаний, где вопросы контроля и регуляторных требований стоят острее всего, — растет доля частных и гибридных облачных моделей. Это отражает стремление бизнеса сочетать надежность и управляемость с масштабируемостью и гибкостью современных КБ-решений. Мы видим, что наибольший интерес к выносу функций КБ в облако проявляют отрасли с высокой цифровой зрелостью и распределенной инфраструктурой: ИТ, медиа, образование, транспорт и ритейл. Для таких сегментов облачные инструменты кибербезопасности становятся ключевым условием поддержания бесперебойных операций и защиты сложных цепочек обработки данных. При этом структура расходов демонстрирует широкий диапазон бюджетов — от базовых сервисов защиты до комплексных платформ управления инцидентами, что подтверждает зрелый, сегментированный спрос на рынке.

Данила Егоров
Директор по бизнес стратегии MWS Cloud

Годовой объем затрат на КБ по индустриям

	< 500 тыс.	500 тыс. – 10 млн	10+ млн
ИТ	33%	41%	26%
Финансы и страхование	47%	28%	25%
Развлечения и медиа	27%	48%	25%
Добыча и переработка полезных ископаемых	43%	36%	26%
Здравоохранение	49%	40%	11%
Наука и образование	48%	44%	9%
Ритейл	56%	36%	8%
HoReCa	50%	45%	5%
Недвижимость и строительство	59%	37%	4%
Промышленность	58%	37%	4%
Транспорт и логистика	43%	53%	4%
Профессиональные услуги	62%	36%	3%

Лишь 5% опрошенных компаний не пользуются услугами внешних поставщиков решений по информационной безопасности, что указывает на высокий уровень доверия к специализированным вендорам и признание важности профессиональных решений в области защиты данных. При этом оставшиеся 95% компаний осознают необходимость интеграции внешних решений для обеспечения надежной защиты своих цифровых инфраструктур.

Однако стоит отметить, что часть компаний предпочитает разворачивать средства информационной безопасности локально. Это может быть связано с желанием сохранить максимальный контроль над данными и минимизировать риски, связанные с передачей информации третьим сторонам. Локальные решения также могут быть предпочтительнее для компаний с высокими требованиями к безопасности и конфиденциальности данных.

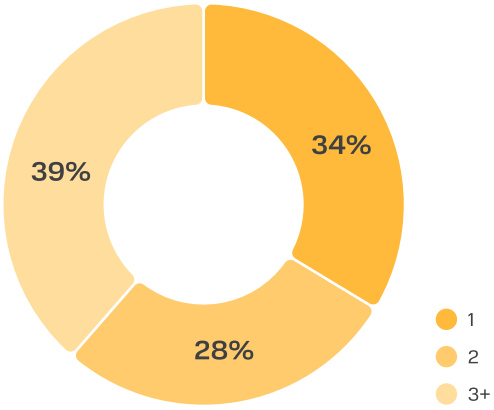
Более трети респондентов сотрудничают с одним вендором, что может свидетельствовать о стремлении к упрощению управления и интеграции решений, а также о доверии к одному проверенному партнеру, что может быть выгодно с точки зрения консолидации сервисов и получения более выгодных условий обслуживания.

В то же время, 64% опрошенных компаний используют услуги не более двух вендоров. Такой подход позволяет комбинировать лучшие практики и технологии, адаптируя их под специфические нужды компании.

В целом, данные тенденции отражают зрелый подход компаний к управлению информационной безопасностью, где баланс между использованием внешних ресурсов и локальных решений определяется стратегическими приоритетами и специфическими потребностями бизнеса.

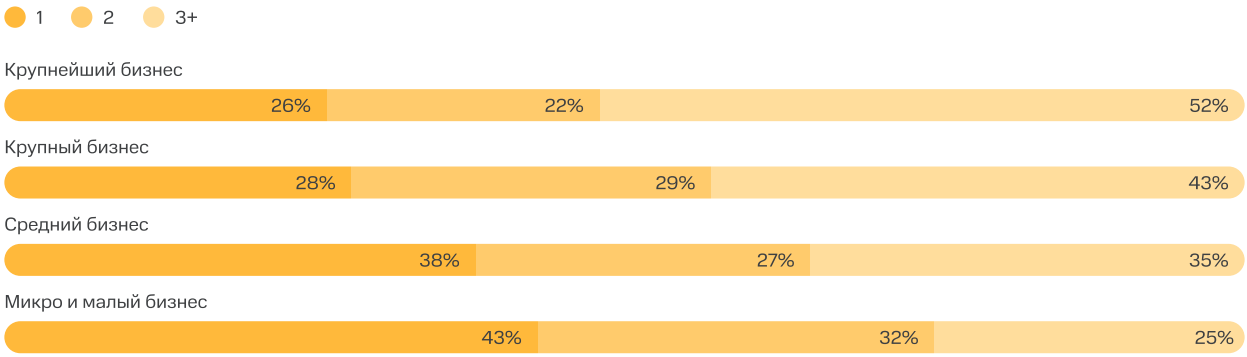
Стоит отметить, что крупный и крупнейший бизнес пользуется большим числом провайдеров, а число провайдеров увеличивается пропорционально росту размера компании.

Количество используемых вендоров КБ



Компании все чаще диверсифицируют риски в кибербезопасности, привлекая несколько вендоров

Количество используемых вендоров КБ по сегментам бизнеса



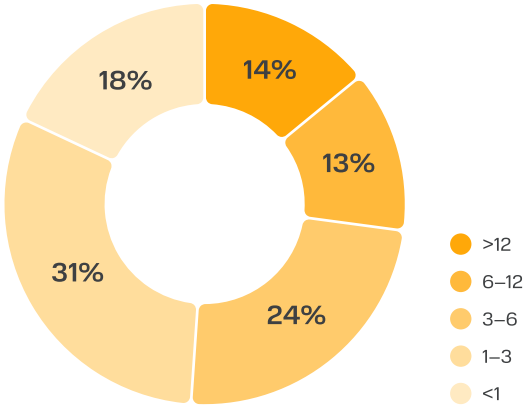
> Для российского корпоративного сектора такой паттерн выбора КБ-решений иллюстрирует доминирование подхода «compliance-driven security», где главной целью выступает соблюдение законодательства и стандартов. Вместе с тем подобная стратегия может сдерживать инвестиции в проактивные технологии киберустойчивости, что важно учитывать в условиях усложнения киберугроз и роста числа целевых атак на крупные компании.

Полина Ли
Руководитель центра аналитики и исследований MWS Cloud

У 55% респондентов процесс внедрения средств КБ длился до полугода. При этом большинство компаний отметили, что внедрение заняло от 1 до 3 месяцев. 14% респондентов заявили, что процесс внедрения средств КБ занял больше года. Длительные сроки миграции могут быть связаны с рядом факторов, таких как сложная инфраструктура, необходимость интеграции с множеством существующих систем или высокие требования к безопасности. Компании, которые сталкиваются с более длительными сроками, возможно, проводят масштабную модернизацию или переходят на более комплексные и кастомизированные решения, что требует значительных временных и ресурсных затрат.

Длительность процесса внеднения средств КБ

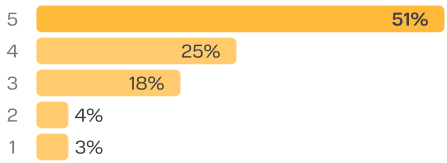
В месяцах



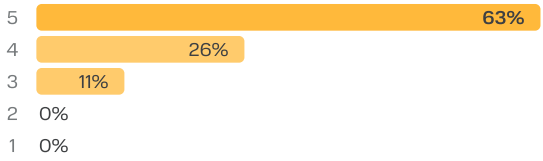
Ключевые факторы при принятии решения о внедрении средств КБ

Оценка респондента от 1 до 5 баллов, где 1 балл — минимальное влияние фактора, 5 — максимальное

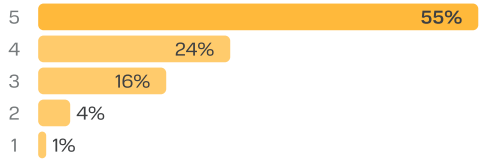
Соответствие требованиям законодательства в части информационной безопасности



Обеспечение защиты данных от внутренних и внешних угроз



Обеспечение киберустойчивости предприятия



Большинство респондентов рассматривают отсутствие нужных компетенций среди сотрудников как наиболее критичный фактор, затрудняющий процесс внедрения систем информационной безопасности. Этот барьер последовательно занимает лидирующие позиции по доле оценок 4 и 5 баллов, что указывает на значительную роль человеческого капитала в успехе проектов КБ.

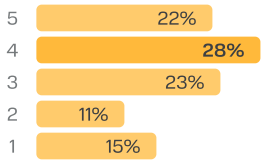
В то же время такие факторы, как отсутствие поддержки вендора в процессе внедрения, а также отсутствие у провайдеров полноценных программ технической поддержки (POC, Support и др.), оцениваются значительно мягче. Для большинства компаний эти сложности не стали критическими, что может свидетельствовать о двух тенденциях. Во-первых, часть компаний предпочитает развивать собственные компетенции, минимизируя внешнюю зависимость и риски, связанные с передачей контроля над критической инфраструктурой. Во-вторых, вероятна концентрация спроса на базовые услуги, которые не требуют глубокой кастомизации или постоянной поддержки поставщика.

Отдельно стоит отметить факторы «повышение сложности управления инфраструктурой» и «дополнительные расходы на этапе внедрения», которые для значимой доли респондентов также остаются чувствительными факторами. Их сравнительно высокая оценка важности подчеркивает необходимость сбалансированного планирования бюджета и архитектуры КБ при переходе на более зрелый уровень защищенности.

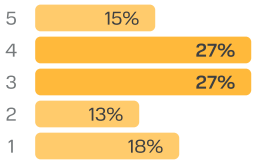
Сложности в процессе внедрения средств КБ [1/2]

Оценка респондента от 1 до 5 баллов, где 1 балл — минимальное влияние фактора, 5 — максимальное

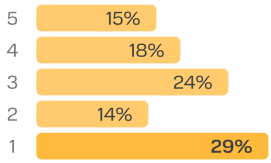
Отсутствие нужных компетенций среди сотрудников



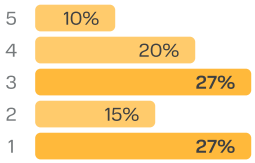
Сложность в оценке предполагаемых расходов на требуемую инфраструктуру



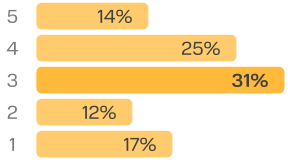
Сложность переноса большого объема данных



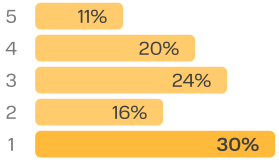
Отсутствие дорожной карты внедрения



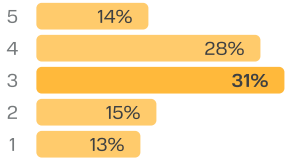
Дополнительные расходы на этапе внедрения систем информационной безопасности



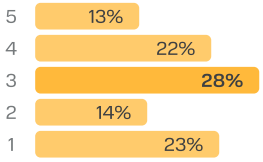
Отсутствие поддержки вендора в процессе внедрения



Повышение сложности управления инфраструктурой



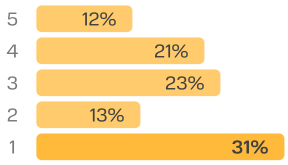
Необходимость временного дублирования инфраструктуры



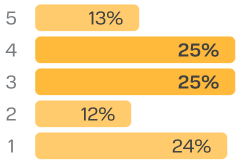
Сложности в процессе внедрения средств КБ [2/2]

Оценка респондента от 1 до 5 баллов, где 1 балл — минимальное влияние фактора, 5 — максимальное

Отсутствие программ технической поддержки у рассматриваемых провайдеров / вендоров (POC, Support, etc.)



Невозможность интеграции средств информационной безопасности в используемые локальные решения (устаревшее ПО / оборудование)



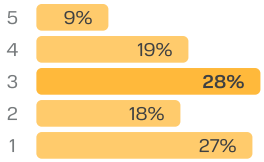
Дополнительные расходы, связанные с переобучением или наймом сотрудников для качественной работы со средствами информационной безопасности, наиболее часто упоминаются респондентами и распределены в сторону высоких оценок важности. Данная тенденция подчеркивает, что кадровый аспект продолжает оставаться одной из основных статей дополнительных затрат в рамках проектов по КБ.

Обновление локальной инфраструктуры также занимает заметное место в структуре расходов, что логично отражает необходимость технологической модернизации в условиях внедрения более сложных или ресурсозатратных систем КБ.

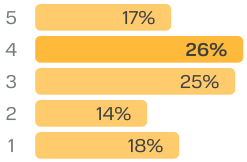
Дополнительные расходы в процессе внедрения средств КБ

Оценка респондента от 1 до 5 баллов, где 1 балл — минимальное влияние фактора, 5 — максимальное

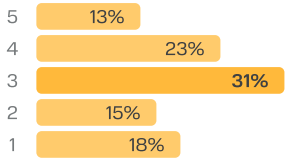
Развертывание тестового контура для проверки работоспособности рассматриваемого решения



Переобучение / найм сотрудников для качественной работы со средствами информационной безопасности



Обновление локальной инфраструктуры

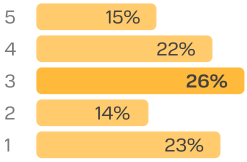


Респонденты наиболее критично воспринимают риски, связанные с утечкой данных — как персональных, так и данных коммерческой тайны. Эти две группы рисков суммарно набрали наибольшую долю оценок по наивысшему уровню критичности (5): утечки коммерческой тайны были определены как критичные 35% участников, утечки персональных данных — 34%. Это подтверждает устойчивую тенденцию повышенного внимания к защите данных клиентов, партнеров и конфиденциальной информации бизнеса. Нехватка технической экспертизы в части информационной безопасности также воспринимается как важный риск, но чаще получает умеренные оценки (3 и 4), что указывает на осознание проблемы, но без ярко выраженного кризисного характера.

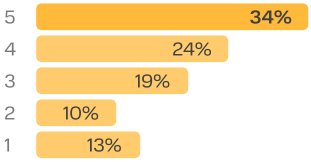
Критичность перечисленных ниже групп рисков при внедрении средств КБ

Оценка респондента от 1 до 5 баллов, где 1 балл — минимальное влияние фактора, 5 — максимальное

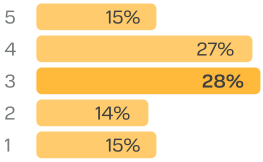
Сложность в закупке оборудования



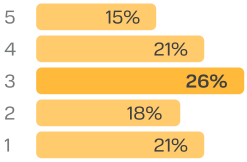
Утечки персональных данных



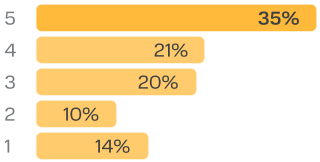
Нехватка технической экспертизы в части информационной безопасности



Неконтролируемый рост затрат на средства информационной безопасности



Утечка данных коммерческой тайны



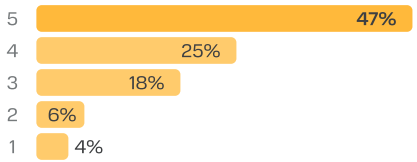
Среди факторов, влияющих на принятие решений о внедрении КБ, с небольшим опережением лидирует анализ угроз и рисков — его критически важным назвали 51% респондентов. Такое распределение ответов подчеркивает практическую ориентацию компаний на понимание уязвимостей и потенциальных сценариев атак как основы для формирования эффективной КБ-стратегии.

Соответствие нормативным требованиям также занимает значительную долю — 47% поставили этот фактор на высший уровень важности, что отражает регуляторное давление и необходимость соответствия отраслевым стандартам и законодательству в области защиты информации.

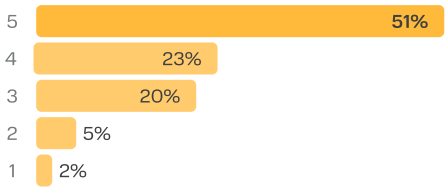
Наиболее важные факторы при принятии решений о внедрении КБ

Оценка респондента от 1 до 5 баллов, где 1 балл — минимальное влияние фактора, 5 — максимальное

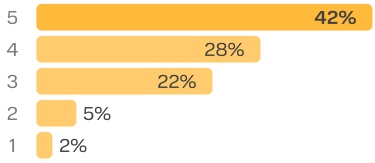
Соответствие нормативным требованиям



Анализ угроз и рисков



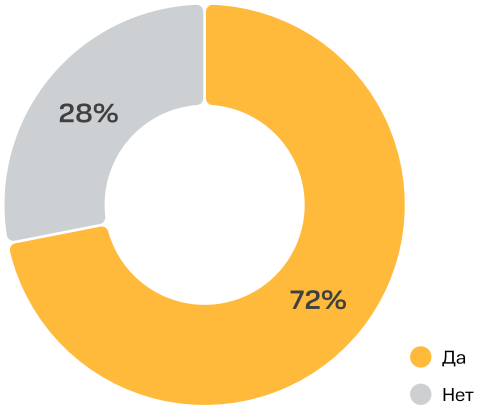
Оптимизация затрат на выявление рисков и угроз



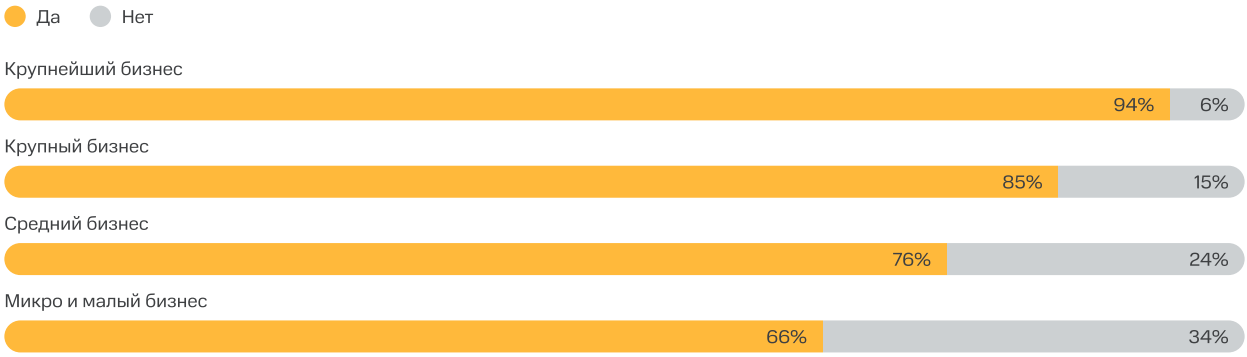
Только крупный и крупнейший бизнес имеет достаточное финансирование для найма необходимых специалистов

72% компаний уже обладают опытом и экспертизой в области кибербезопасности. Такая высокая доля подтверждает, что вопросы КБ прочно вошли в корпоративную повестку большинства участников рынка. Структура по сегментам бизнеса показывает, что чем выше выручка компании, тем выше вероятность наличия опыта и компетенций в области КБ. Среди компаний с годовой выручкой < 800 млн руб. экспертизу в КБ отметили 66%, тогда как среди компаний с большей выручкой доля растет, вплоть до 94% у крупнейшего бизнеса . Это логично объясняется возможностями крупных компаний вкладываться в специализированные команды, обучение и развитие процессов КБ.

Наличие опыта и экспертизы работы с КБ



Наличие опыта и экспертизы работы с КБ по сегментам бизнеса

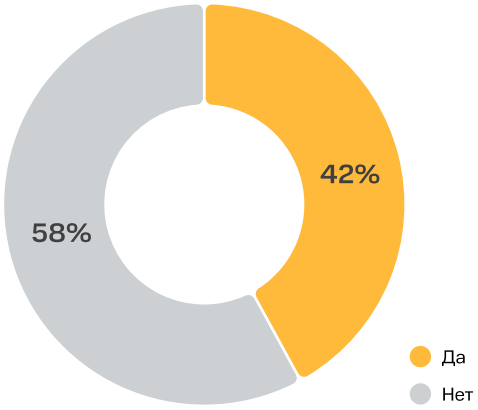


Наибольшая концентрация экспертизы по отраслям наблюдается в ИТ (88%), добыче полезных ископаемых (82%), финансах и страховании (81%), а также в здравоохранении и профессиональных услугах. Для этих индустрий характерны специфические регуляторные требования, высокие риски утечек конфиденциальных данных, а также потребность в защите интеллектуальной собственности и критической инфраструктуры. Эти факторы напрямую влияют на необходимость формирования зрелой компетенции по КБ внутри компаний. Наличие опыта и экспертизы в КБ выступает не только индикатором зрелости управления технологическими рисками, но и отражает специфику отраслевых регуляций и бизнес-моделей. Для менее капиталоемких и менее зарегулированных секторов характерна более низкая доля экспертизы, что свидетельствует о потенциале для дальнейшего развития практик КБ и консалтинговых сервисов в этих сегментах.

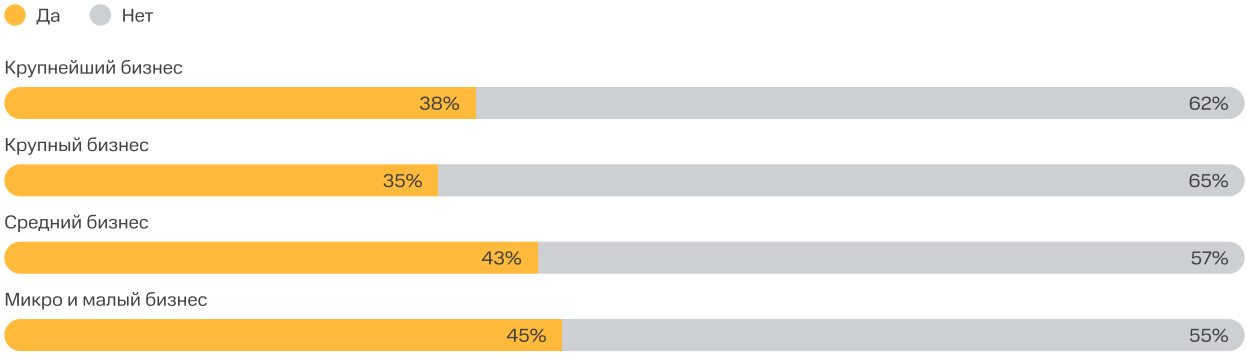
Несмотря на общее наличие опыта работы со средствами КБ, проблемы с наймом квалифицированных сотрудников все еще являются существенным фактором для отрасли. 43% респондентов указали на наличие проблем в найме экспертов в сфере КБ, что является значительным показателем. При этом наличие проблем в найме не коррелирует с размером бизнеса — компании из всех сегментов бизнеса испытывают примерно схожие проблемы в найме, что говорит о структурном характере проблемы, затрагивающей как малый бизнес, так и крупных игроков.

С технологической точки зрения, тренд подчеркивает растущую роль сервисов, позволяющих компаниям компенсировать нехватку собственных компетенций за счет готовых управляемых сервисов безопасности (Managed Security) и встроенной экспертизы провайдера. В долгосрочной перспективе такие модели становятся не просто технологической опцией, а стратегическим инструментом закрытия критического дефицита кадров и ускорения цифровой трансформации бизнеса.

Наличие проблем в найме экспертов в сфере КБ



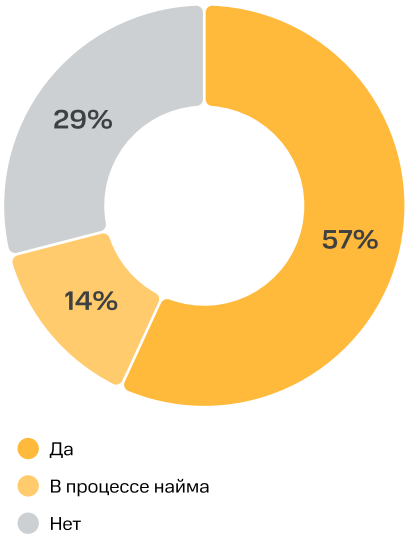
Наличие проблем в найме экспертов в сфере КБ по сегментам бизнеса



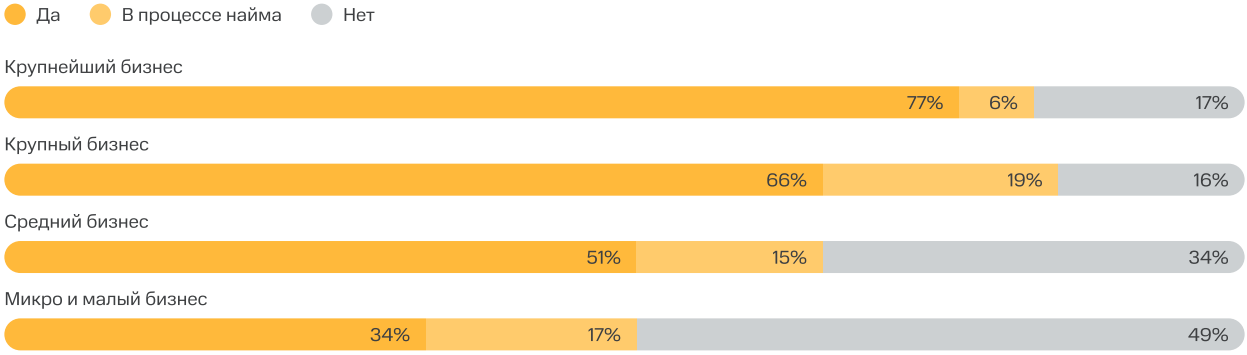
При этом, наличие полноценной собственной команды также становится все более распространенным явлением. 57% опрошенных компаний уже имеют собственную команду по кибербезопасности, в то время как 14% находятся в процессе ее формирования. Это указывает на растущее признание значимости кибербезопасности в бизнесе. Согласно результатам опроса, ожидаемо, существует прямая корреляция между размером компании и наличием у нее собственной команды по кибербезопасности. Большие компании, имеющие более сложные ИТ-структуры, чаще имеют свои команды.

Наиболее часто наличие собственной команды отмечается в компаниях сектора ИТ и фармацевтики. Это связано с тем, что они обрабатывают большое количество данных и подчиняются значительным регуляторным требованиям. При этом даже при наличии внутренних специалистов предприятия продолжают полагаться на облачные сервисы безопасности для покрытия масштабируемых задач и для соответствия растущим регуляторным стандартам. В итоге рынок движется в сторону комбинированных моделей: собственные центры компетенций в КБ дополняются продвинутыми облачными решениями, что создает спрос на более гибкие, комплексные и отраслево-ориентированные сервисы.

Наличие собственной команды по кибербезопасности



Собственная команда по кибербезопасности по сегментам бизнеса



Профессиональные сервисы для развития кибербезопасности в основном включают техническую поддержку, обучение и аудит. Эти сервисы используются более чем 40% опрошенных компаний. Техническая поддержка играет ключевую роль в обеспечении оперативного реагирования на инциденты и устранении уязвимостей. Обучение персонала кибербезопасности повышает осведомленность сотрудников о потенциальных угрозах и способах их предотвращения. КБ-аудит позволяет компаниям систематически проверять и улучшать свои защитные меры. В целом, данные свидетельствуют о том, что компании активно инвестируют в ключевые элементы кибербезопасности, что является важным шагом для снижения рисков и защиты от киберугроз.

Перечень профессиональных сервисов, используемых для развития КБ

63%
Техническая поддержка

25%
Интеграция

ПРОДУКТЫ MTC WEB SERVICES

КИБЕРЗАЩИТА ГИБРИДНОЙ ИНФРАСТРУКТУРЫ КЛИЕНТА

Инструменты для защиты от угроз информационной безопасности

На 80% снизить риски кибератак

за счёт систем кибербезопасности

На 50% сократить убытки от любых кибератак

24/7

мониторинг
и защита периметра

500

активных правил для анализа
и сопоставления событий ИБ

>1500

источников широкого спектра
информации для обработки данных

300 Гбит/сек

активной полосы пропускания
для AntiDDoS

SOC

Комплексное решение для повышения уровня кибербезопасности предприятия. Объединяя квалифицированных специалистов, инновационные технологии и выстроенные процессы, обеспечивает всестороннюю защиту организации от киберугроз в режиме реального времени. SOC круглосуточно мониторит состояние ИТ-инфраструктуры компании и снижает риски взломов, похищения данных сотрудников/клиентов/пользователей и других киберугроз, которые могут привести к остановке бизнеса

ANTI-DDOS

Комплексное решение, обеспечивающее блокировку DDoS-атак на инфраструктуру и web-ресурсы заказчика. Защита от DDoS-атак необходима организациям, чья деятельность напрямую или косвенно связана с доступностью систем в сети интернет, чьи производственные процессы увязаны с удаленным доступом к собственным и сторонним ресурсам

WAF

Сервис защиты от атак и уязвимостей в веб-приложениях. С помощью личного кабинета можно самостоятельно настраивать политики и правила защиты своих ресурсов

ВНЕДРЕНИЕ ТЕХНОЛОГИЙ: КИБЕРБЕЗОПАСНОСТЬ

Раздел демонстрирует продуктовые категории, которые относятся к технологии информационной безопасности. В силу специфики исследования, в части КБ фокус сконцентрирован на вертикалях Software и IT-Services в ИТ-рынке, поскольку данные вертикали составляют большую часть рынка кибербезопасности в России с точки зрения объема. Аппаратная часть решений в сфере кибербезопасности не находится в фокусе нашего исследования, поскольку состоит из узкоспециализированных продуктов, в том числе аналоговых решений, и не всегда связанных с digital-продуктами. По аналогии с облаком, продукты в сфере КБ можно разделить на широко распространенные, в том числе, необходимые для соответствия требованиям законодательства, и на узкоспециализированные, востребованные компаниями для решения задач повышенной сложности.

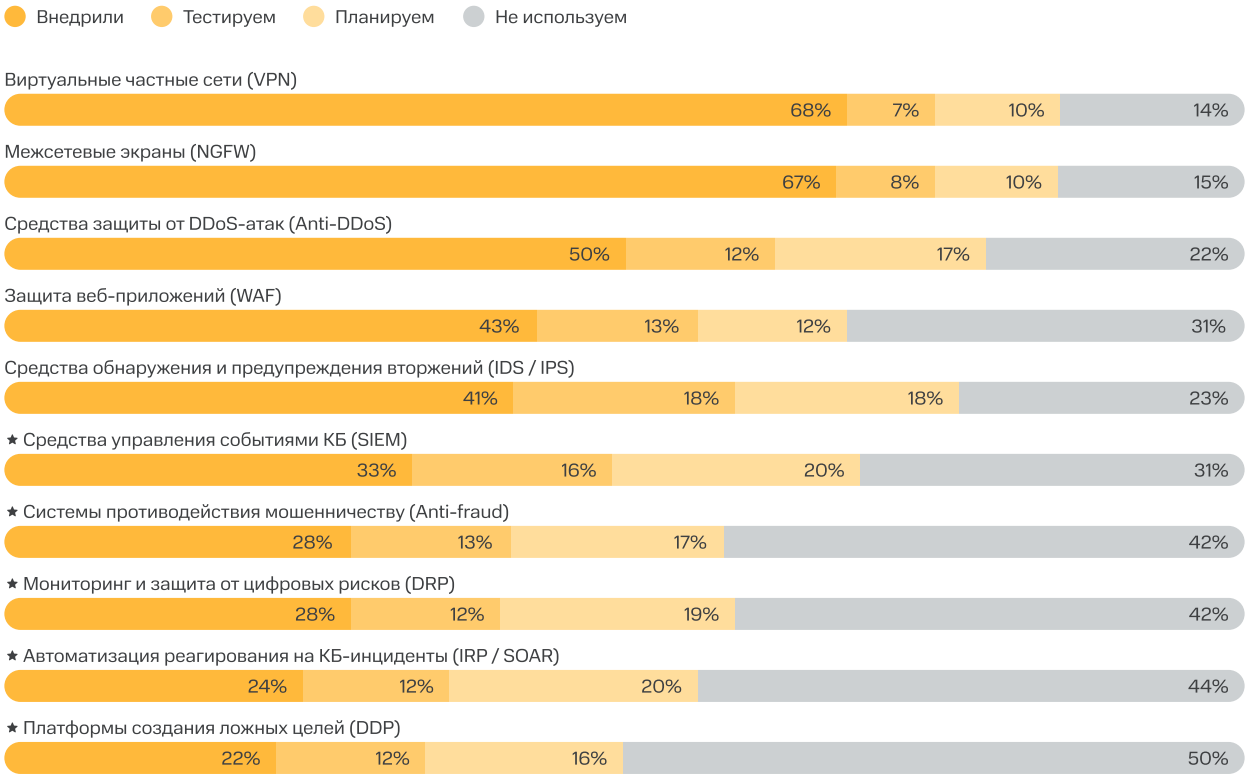
Для оценки среди полученных субкатегорий тех продуктов, которые имеют повышенный потенциал роста, введен подход, получивший название «Формула потенциала роста субкатегорий». Данная формула представляет собой сопоставление: с одной стороны параметра «внедрили», с другой стороны суммы параметров «тестируем» и «планируем». В отличии от параметра «не используем», данные значения положительно характеризуют планы респондентов, что можно интерпретировать, как вероятный переход в статус «внедрели» в ближайшей перспективе.

Внедрили < Тестируем + Планируем = есть потенциал

Внедрили > Тестируем + Планируем = потенциал исчерпан

По этим данным, наиболее перспективной являются продуктовая субкатегория Средства защиты инфраструктуры (5 перспективных технологий из 10). Высокий потенциал дальнейшего развития данных направлений обуславливается одновременно и технологическими трендами (миграция в облака, микросервисы, remote / hybrid work, переход от традиционной периметровой модели к модели Zero Trust), и экономическими факторами (рост убытков от инцидентов, страхование киберрисков, нехватка КБ-специалистов). Дополнительные угрозы несет не только общее повышение числа киберугроз, но и такие факторы, как ускорение разработки и поставки программных продуктов, ужесточение регуляторных требований, общая трансформация ИТ-ланшафта. В этих условиях инвестиции в передовые средства защиты приложений и инфраструктуры становятся ключевым драйвером снижения киберрисков и обеспечения непрерывности бизнеса.

Средства защиты инфраструктуры



Решения в сфере информационной безопасности являются сегментом с наибольшим бюджетом среди анализируемых технологий. Важно подчеркнуть, что это связано не просто с формальным соответствием требованиям законодательства, а с реальной угрозой защищенности инфраструктуры (среди крупнейшего бизнеса более 60% из опрошенных компаний сталкивались с DDoS-атаками в течение года). Также для усиления защиты от внешних угроз компании отметили частое внедрение VPN сервисов корпоративного класса. Межсетевые экраны (NGFW) продолжают отмечаться компаниями как один из наиболее частых продуктов на рынке (параметр внедрения отметили 67%). Закономерно, что высокий спрос на модель поставки программно-аппаратных комплексов в большей степени зафиксировали компании крупного и крупнейшего бизнеса.

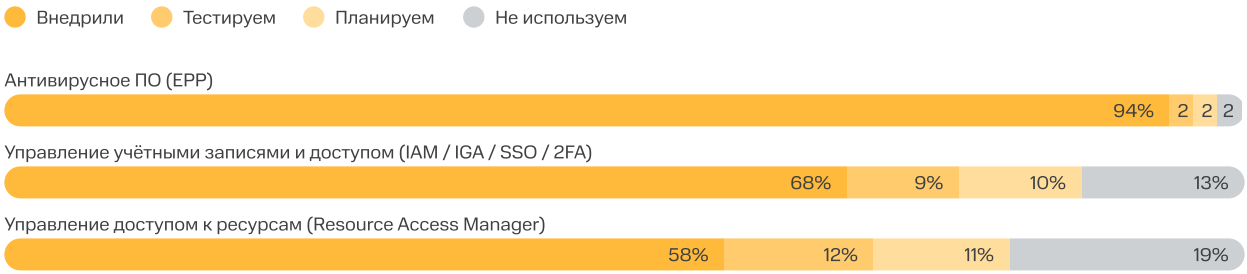
Базовой практикой в холдинговых компаниях является наличие собственной команды по КБ (отметили 76% опрошенных представителей крупнейшего бизнеса), однако найм экспертов, в том числе по защите базовой инфраструктуры предприятия, все еще остается значимой проблемой (отметили 43% опрошенных). Что может являться одной из причин высокой доли планирующих, но не внедривших решения по многим из продуктовых субкатегорий.

★ — высокий потенциал

Средства защиты данных

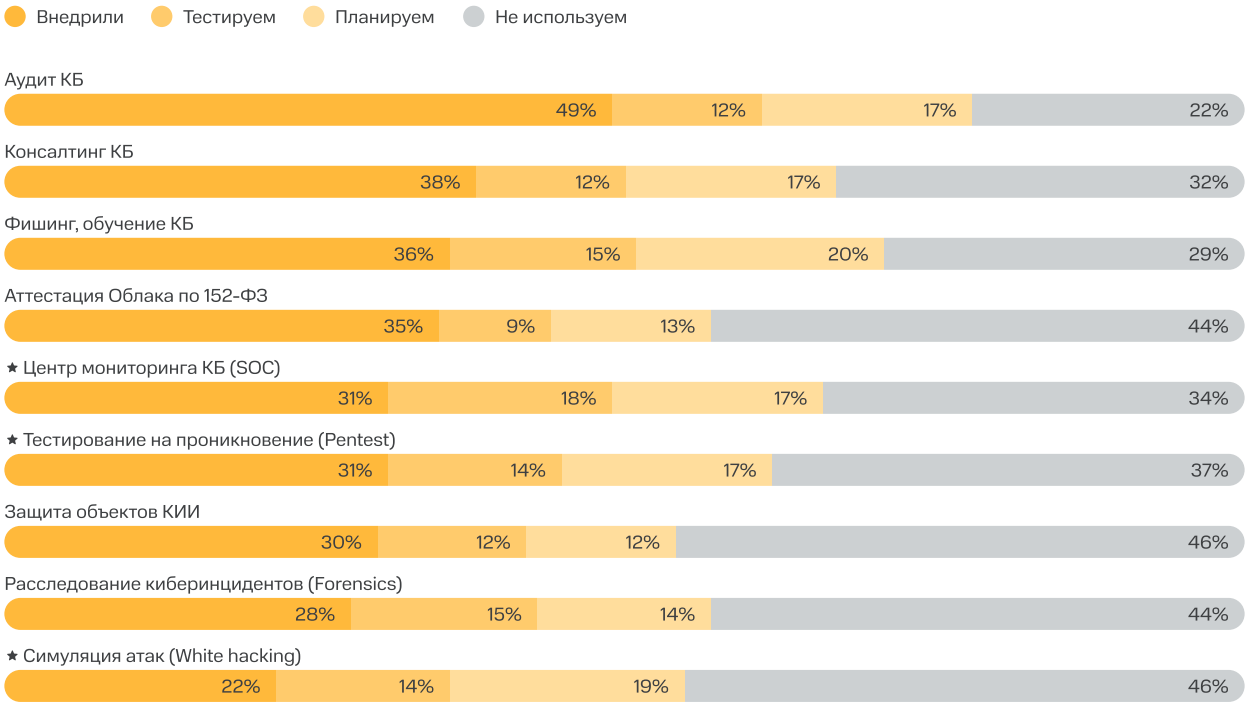
Защита данных от внешних и внутренних угроз является фундаментальным атрибутом деятельности любой корпорации. Крупнейшие экосистемные российские организации, а также органы государственной власти регулярно подвергаются соответствующим рискам, что несет не только угрозу для внутренних операционных процессов, но и акционерные, и репутационные потери. Шифрование данных отмечалось респондентами как наиболее распространенный инструмент по работе с данными, наряду с сертификацией, управлением правами доступа и другими инструментами реагирования на внешние угрозы. Отдельно многие респонденты подсвечивают DLP в качестве планируемого для внедрения класса решений, который в большей степени востребован крупными компаниями.

Средства защиты пользователей и конечных точек



Антивирусное ПО имеет самый высокий процент внедрения из всех рассматриваемых продуктов КБ - 94%, что говорит о высоком уровне информированности о потенциальных киберугрозах. Данный класс решений стал commodity на российском рынке. По мере нарастания сложности и количества кибератак, пользователи реагируют на данные риски увеличением потребления продуктов, связанных с управлением доступами.

Услуги в сфере КБ

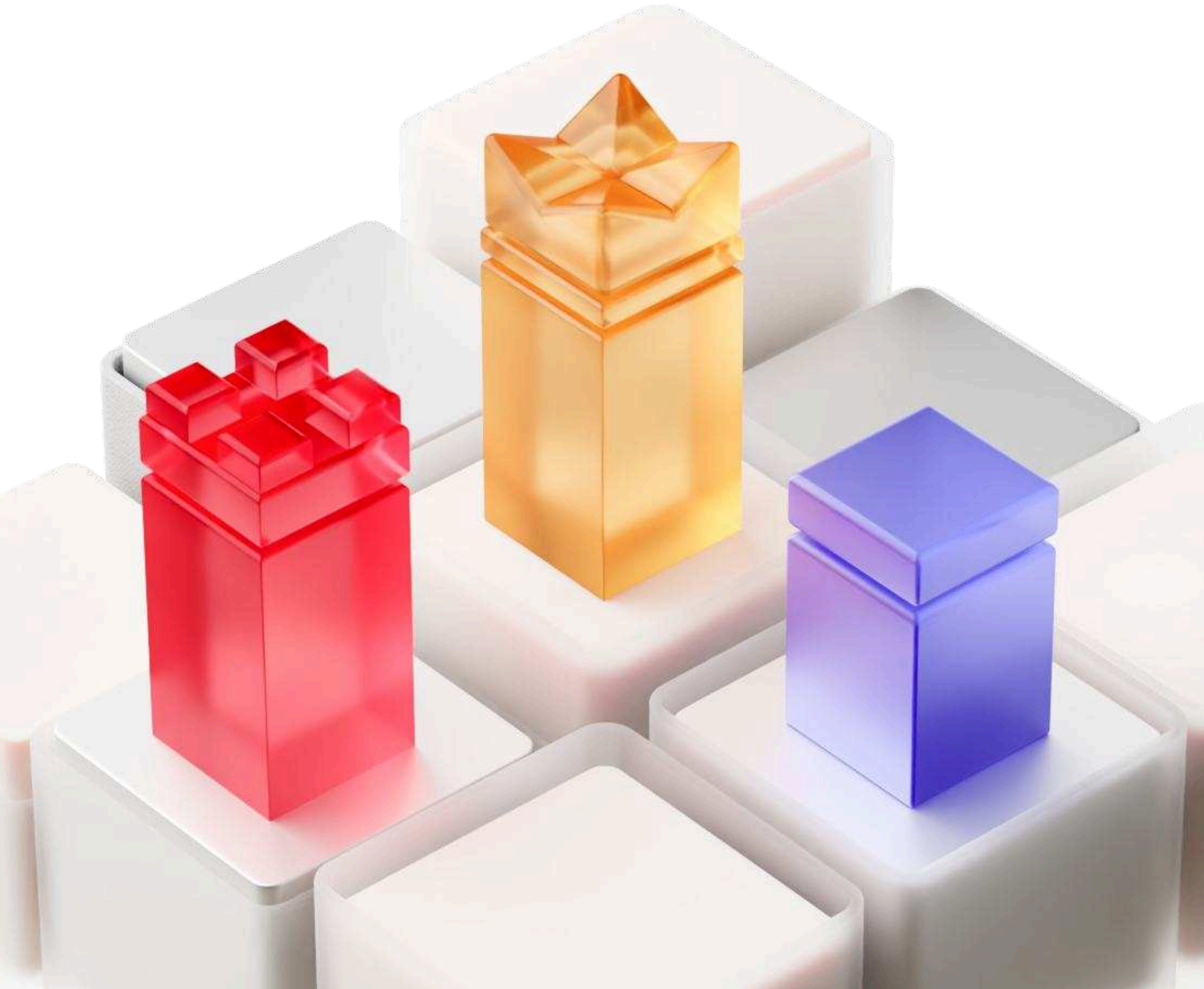


В объеме рынка кибербезопасности в России вертикали Software и IT-Services совокупно занимают порядка 80%. Вертикаль IT-Services растет с темпом годового прироста более 30%. Эти значения коррелируют с данными ожиданий объемов потребления соответствующих решений КБ в выборке данного исследования. Услуги в сфере кибербезопасности не менее развиты, чем программное обеспечение, что связано с рядом факторов: сложности с поиском специалистов, дефицит внутренней экспертизы и высокая стоимость создания собственной функции кибербезопасности в компании.

Абсолютным лидером по доле потребления услуг является Аудит КБ, что в том числе обусловлено нормативными требованиями и распоряжениями со стороны акционеров компаний. Применяя ранее сформулированный подход к выделению продуктовых субкатегорий со значимыми категориями (сумма ответов по параметрам «тестируем» и «планируем» сопоставима со значением по параметру «внедрили»), можно отметить в части IT-Services следующие категории: Фишинг, Обучение КБ, Центр мониторинга КБ (SOC), а также Pentest и White hacking.

★ — высокий потенциал

ЗАКЛЮЧЕНИЕ



“ Технологии кибербезопасности демонстрируют высокую зрелость и высокий уровень насыщения рынка. По результатам исследования, лишь около 30% направлений в ИБ сохраняют заметный потенциал дальнейшего роста, что существенно ниже, чем в облаках и ИИ. Это означает, что подавляющая часть ключевых решений по информационной безопасности уже широко внедрена в корпоративных инфраструктурах и воспринимается как обязательная часть базовой ИТ-архитектуры.

Полученные результаты напрямую связаны с высокой актуальностью киберрисков для российских компаний. Участившиеся инциденты (количество кибератак в 2025 году выросло на 30%) и ужесточение регуляторных требований стимулировали организации к ускоренному внедрению систем защиты: от антивирусных и сетевых решений до комплексных платформ класса SGRC, SIEM и CNAPP. Таким образом, рынок демонстрирует высокую степень реакции на внешние вызовы и переход от фазы активного освоения к фазе операционной консолидации и оптимизации существующих систем.

При этом сохраняется интерес к развитию управляемых сервисов безопасности (MSS / SOC), а также к решениям, обеспечивающим интеграцию защиты на уровне инфраструктуры и приложений. Эти направления становятся ключевыми точками роста, особенно в условиях дефицита квалифицированных кадров (который отмечают более 40% опрошенных) и растущей сложности ИТ-ландшафтов.

С точки зрения предложения, отечественный рынок уже располагает широкой линейкой решений собственной разработки, охватывающей большинство критичных направлений. Это позволяет компаниям обеспечивать соответствие требованиям регуляторов и одновременно снижать зависимость от иностранных поставщиков. В целом, можно отметить, что сектор кибербезопасности в России находится на этапе технологической стабилизации, но сохраняет потенциал для эволюционного роста — прежде всего за счёт расширения функциональности, автоматизации и внедрения интеллектуальных механизмов защиты

Игорь Зарубинский
Исполнительный директор MWS, CEO MWS Cloud

APPENDIX

КЛЮЧЕВЫЕ ТЕРМИНЫ

ПУБЛИЧНОЕ ОБЛАКО

Модель облачных вычислений, в которой ИТ-инфраструктура (серверы, хранилища данных, сети) принадлежит стороннему поставщику и управляется им, а ресурсы предоставляются через интернет. Пользователи (компании или частные лица) совместно используют эту инфраструктуру.

ЧАСТНОЕ ОБЛАКО

Облачная инфраструктура, развернутая и используемая исключительно одной организацией. Она может физически находиться в собственном дата-центре компании (on-premise) или у стороннего провайдера, но при этом все ресурсы полностью изолированы и предназначены только для одного клиента.

ГИБРИДНОЕ ОБЛАКО

ИТ-среда, которая объединяет частное облако с одним или несколькими публичными облаками.

ON-PREMISE

Модель, при которой ИТ-инфраструктура (серверы, программное обеспечение, сети) развертывается и управляется непосредственно на территории компании, в ее собственном дата-центре.

MULTICLOUD

Стратегия использования услуг от двух и более провайдеров облаков одновременно.

AI CLOUD

Инфраструктура и сервисы для внедрения технологий ИИ в бизнес. ИИ-облако эффективно ускоряет цифровую трансформацию и оптимизирует бизнес-процессы

на 20% растёт прибыль за счёт более точных стратегических решений благодаря использованию ИИ при анализе данных	**20-45%** повышение производительности отдела разработки при использовании систем генерации кода	**на 60%** меньше времени на обработку обращений клиентов	

ОБЛАЧНАЯ ПЛАТФОРМА MWS

Сократите Time-to-Market и улучшите возможности гибридной инфраструктуры

на 40% Сокращение расходов на инфраструктуру	**на 50%** Ускорение Time-to-Market	**на 80%** снижение вероятности успешных атак за счет систем кибербезопасности	

МТС Web Services (MWS)

Облачные сервисы и продукты Enterprise-уровня для ИИ-экспериментов и цифровой трансформации бизнеса. Компания предлагает передовые технологии, глубокую экспертизу, комплексную поддержку и надёжную инфраструктуру для достижения заказчиками новых высот. Среди решений MWS: сервисы по вычислению и хранению, инфраструктура для обучения AI- и ML-моделей, базы данных, бизнес-приложения, сетевые сервисы и решения для разработчиков

MWS Intelligence Team

Команда отвечает за лидерство в аналитике и исследованиях на ИТ-рынке России.
Мы агрегируем лучшие глобальные и российские практики в области облаков, искусственного интеллекта, кибербезопасности и информационных технологий в целом