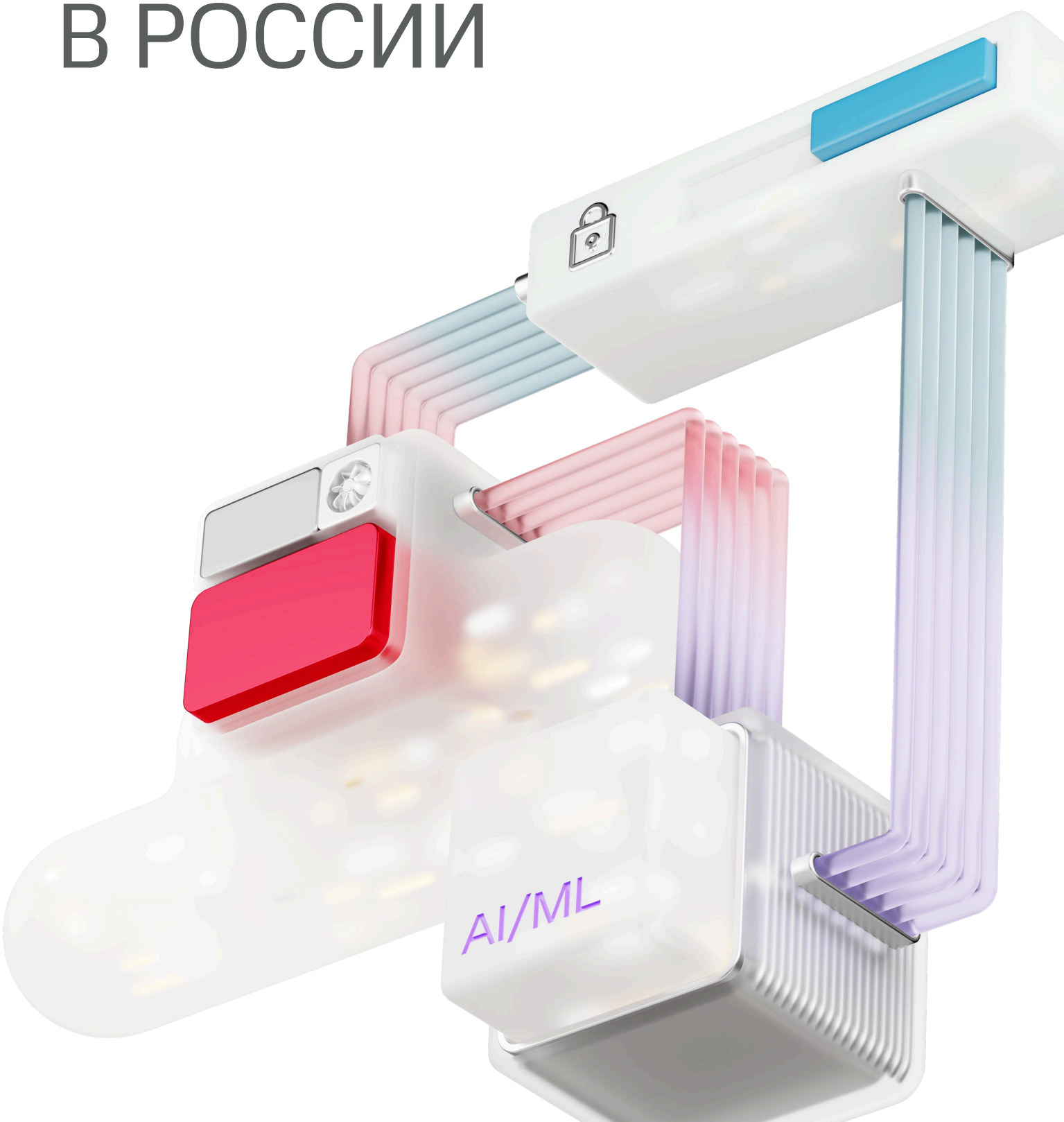
ТЕХНОЛОГИЧЕСКИЕ СТРАТЕГИИ БИЗНЕСА В РОССИИ



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

ЭКСПЕРТЫ

Павел Воронин

Генеральный директор MWS,
первый вице-президент по ИТ МТС

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, первый вице-президент по ИТ МТС

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 рынока 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

→

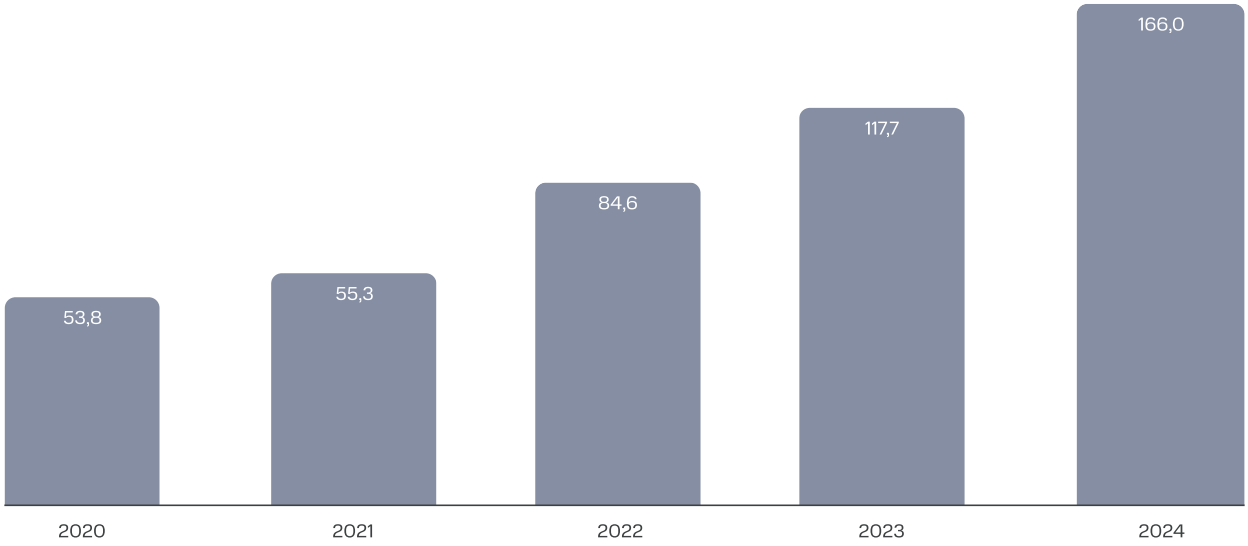
3,1%
Доля ИТ
в ВВП РФ 2030

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.

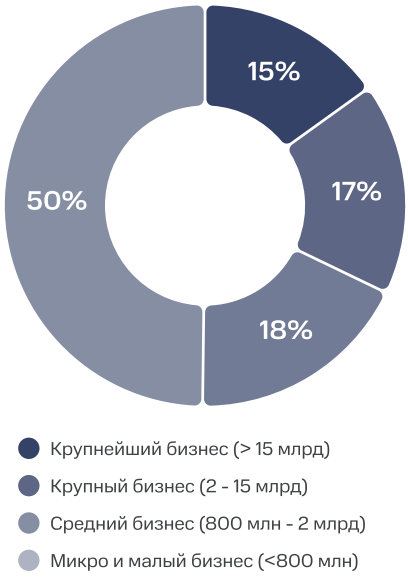
Основой исследования является анкетный опрос представителей более чем 700 российских компаний. Для расширения понимания отдельных аспектов исследования дополнительно были проведены глубинные интервью с частью респондентов.

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.

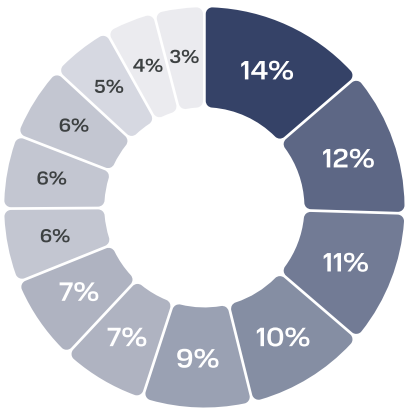
Респонденты исследования сбалансированно представляют различные сегменты бизнеса. Половину выборки составляют микро- и малые компании, оставшиеся 50% — представители среднего, крупного и крупнейшего бизнеса, причем эти доли распределены равномерно.

Структура респондентов по сегментам бизнеса

Размер выручки, руб.



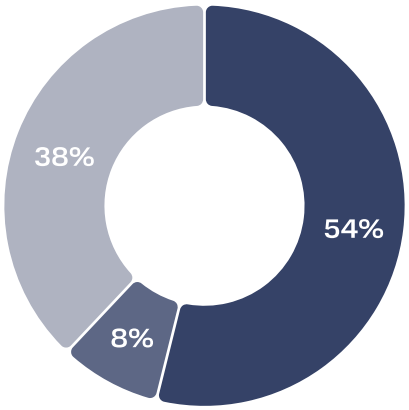
Структура респондентов по индустриям



- 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

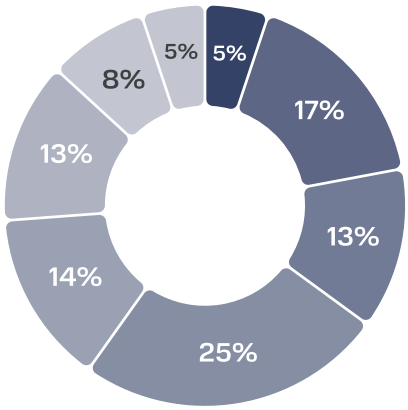
Большинство компаний-респондентов расположены в Москве и Московской области, однако свыше трети опрошенных представлены региональным бизнесом, что обеспечивает широкий географический охват. По численности персонала выборка также разнообразна: 26% компаний относятся к малому бизнесу с численностью менее 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

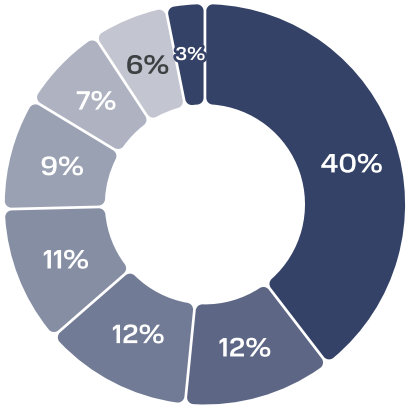


- 5 000 – 9 999
- 1 000 – 4 999
- 500 – 999
- 100 – 499
- 50 – 99
- 10 – 49
- < 10

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)

MTC 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

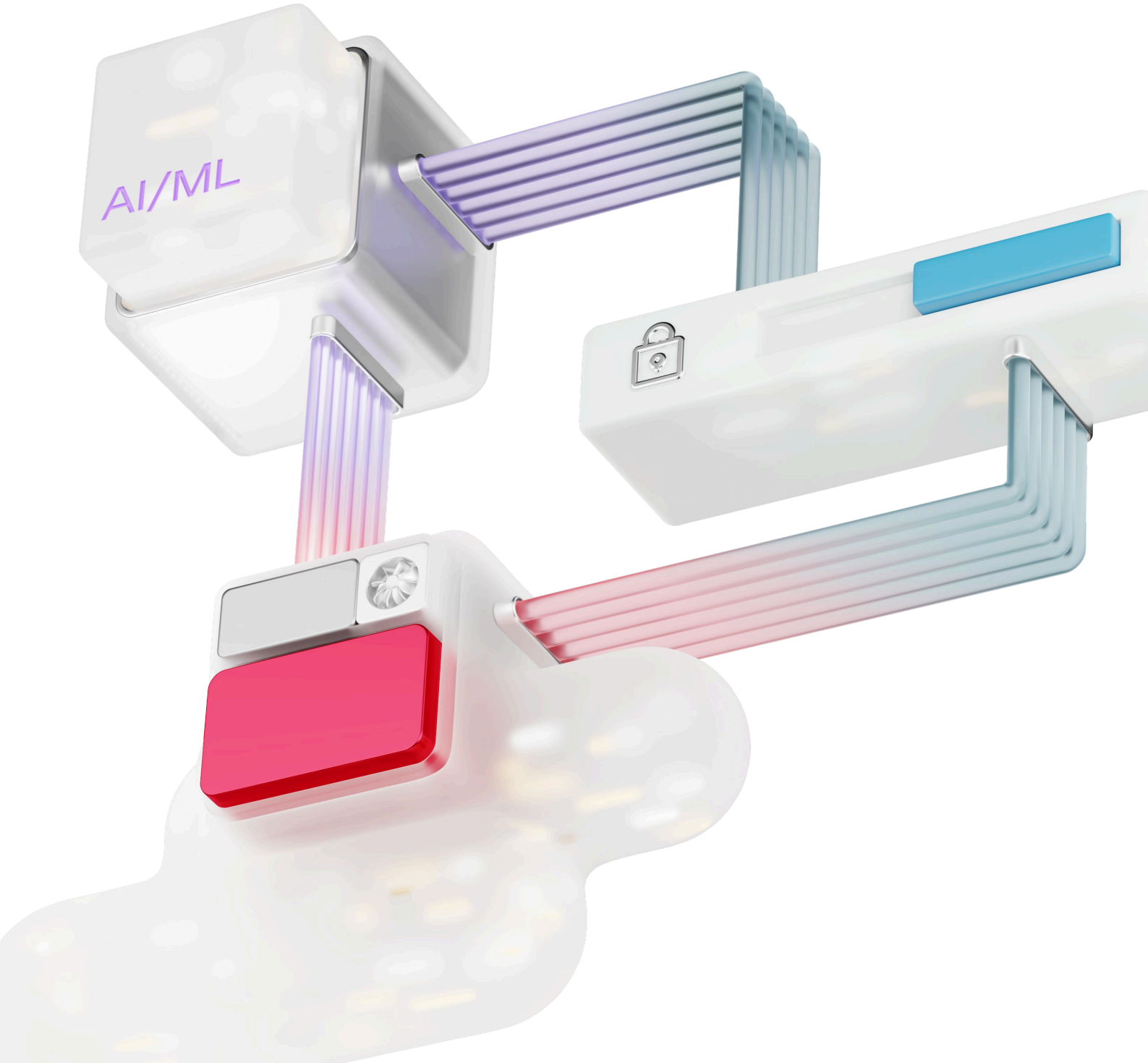
Управление данными

- 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

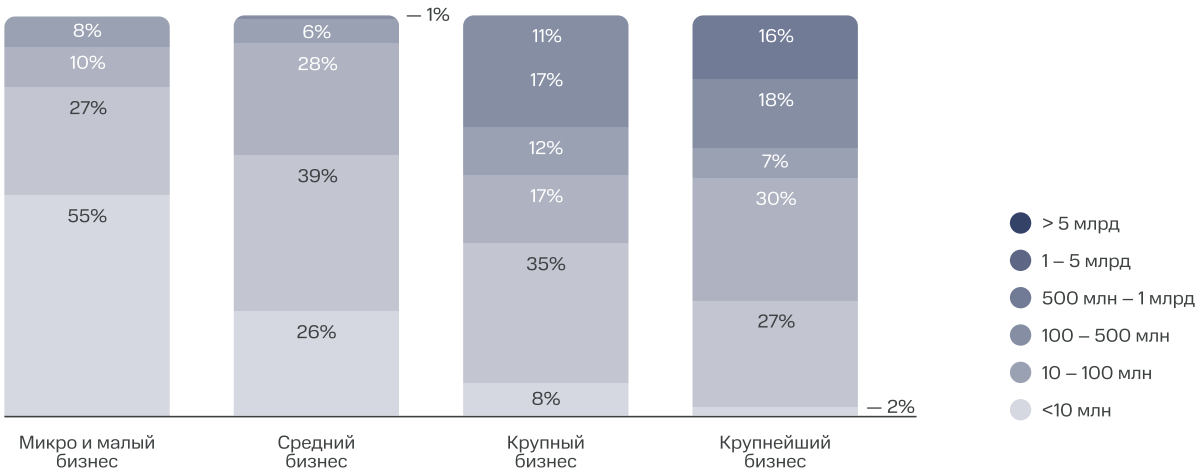
	< 10 млн	10 – 100 млн	100 – 500 млн	500 млн – 1 млрд	1 – 5 млрд	> 5 млрд
ИТ	24%	28%	13%	13%	11%	10%
Финансы и страхование	33%	19%	11%	8%	20%	9%
Добыча и переработка полезных ископаемых	33%	32%	8%	7%	11%	9%
Развлечения и медиа	22%	25%	36%	6%	3%	8%
Здравоохранение	33%	39%	15%	4%	4%	5%
Профессиональные 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.

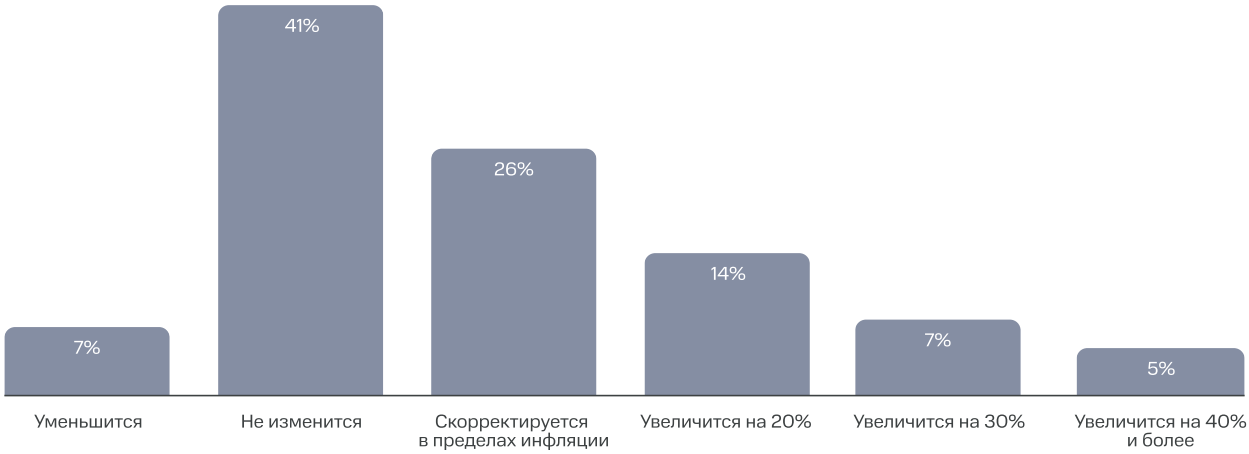
По величине расходов на данные технологические направления отечественные компании все еще отстают от международных игроков, у которых сопоставимые затраты могут достигать 50%. Кроме того, отличается и структура ИТ-бюджетов в мире и России: в международной практике лидирующие позиции занимают облачные 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.

ТОП-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: ОБЛАКО

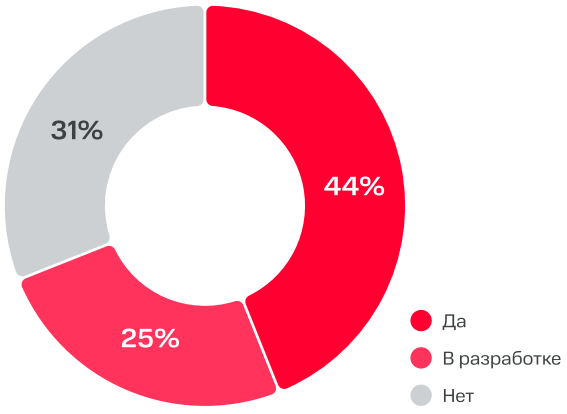
Стратегия внедрения облачных технологий служит ключевым индикатором цифровой зрелости российских компаний и их готовности к трансформации. Переход в облако — это не только технологический, но прежде всего стратегический выбор, влияющий на способность бизнеса адаптироваться, сокращать издержки и ускорять инновации.

44% компаний внедряют облачные технологии в рамках стратегического подхода, что свидетельствует о развитом, но ещё не насыщенном рынке облачных решений в России. Это демонстрирует растущее понимание ценности облаков — от гибкости и масштабируемости до оптимизации затрат. Эти компании можно отнести к «зрелым» пользователям облаков. Наличие резервов в увеличении доли системных потребителей облачных решений создает окно возможностей для поставщиков облачных услуг.

Четверть компаний всё ещё в процессе формирования стратегии, что указывает на этап осмысления и подготовки инфраструктуры. Эти компании, скорее всего, уже сталкиваются с потребностями цифровой трансформации, но пока не перешли к системной реализации. Эта категория может быть самой чувствительной к внешним стимулам — как со стороны регуляторов, так и с точки зрения рыночной конкуренции. Именно этот сегмент потенциально станет следующей волной спроса на инфраструктуру, обучение и сопровождение миграции.

Почти треть компаний не имеют облачной стратегии вообще. Это может быть связано с несколькими факторами: (1) малый или средний бизнес, у которого недостаточно ресурсов или экспертизы, (2) компании, работающие в традиционных или зарегулированных отраслях (например, промышленность), где переход в облако осложнён безопасностью и нормативами, (3) недостаточное понимание потенциала облаков или сопротивление изменениям на уровне управления.

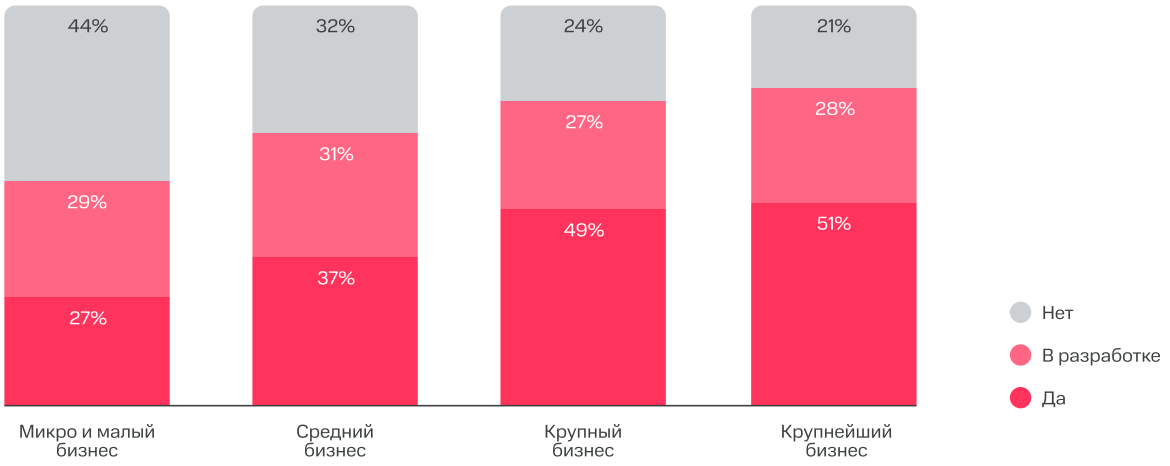
Наличие стратегии по внедрению облачных технологий



В исследовании фиксируется четкая зависимость между размером выручки компаний и наличием уже сформированной стратегии по облакам. Это напрямую отражает различия в доступе к финансовым ресурсам, уровню ИТ-компетенций и степени цифровой зрелости бизнеса.

Размер компании прямо пропорционален наличию стратегии. Наибольшую вовлеченность в стратегическое планирование облачных инициатив демонстрируют компании крупнейшего бизнеса (выручка свыше 15 млрд руб.) — здесь наличие стратегии отметили 51% респондентов. Для крупных предприятий (выручка от 2 до 15 млрд руб.) этот показатель чуть ниже и составляет 49%. Наименее подготовленным остается микро и малый бизнес с выручкой до 800 млн руб. — 44% из них вовсе не имеют облачной стратегии, что является наименьшим значением из всех рассматриваемых сегментов. Такой разрыв чаще всего связан с ограниченным доступом к специализированной ИТ-экспертизе и приоритетом решения текущих операционных задач над стратегическими инициативами.

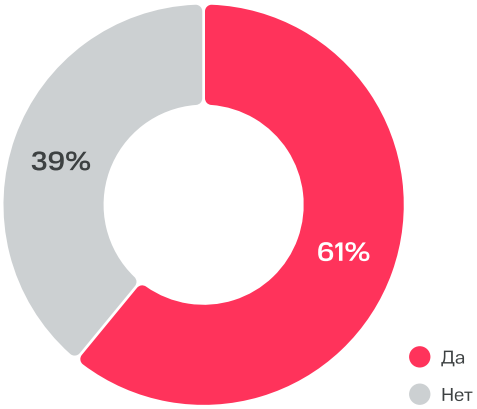
Наличие стратегии по внедрению облачных технологий



С точки зрения наличия стратегии по облачным технологиям можно выделить три ключевые группы индустрий: (1) Зрелые (более 50% компаний имеют облачную стратегию). Эти индустрии демонстрируют высокий уровень зрелости в области облачных технологий. Примечательно, что у компаний из этой группы также зафиксирован сопоставимый уровень стратегий, находящихся в разработке — около 16%, что указывает на устойчивое внимание к теме и активную работу в данном направлении. К данным индустриям относится ИТ, транспорт и логистика, промышленность, финансы и страхование. (2) Промежуточная зрелость (30–49% компаний имеют стратегию). К данной группе принадлежит большая часть индустрий из скоупа исследования. С точки зрения процесса разработки облачной стратегии или ее отсутствия складывается неоднозначная и фрагментированная картина среди данных индустрий. Такими индустриями являются развлечения и медиа, здравоохранение, профессиональные услуги, строительство и ЖКХ. (3) Низкий уровень стратегической зрелости (<30% компаний имеют стратегию): более 45–60% компаний из этих индустрий вовсе не имеют стратегии по облачным технологиям. Это может свидетельствовать как о более консервативном подходе, так и о наличии барьеров (регуляторных, технологических, организационных) для внедрения облачных решений. К данным сферам относятся HoReCa, наука и образование.

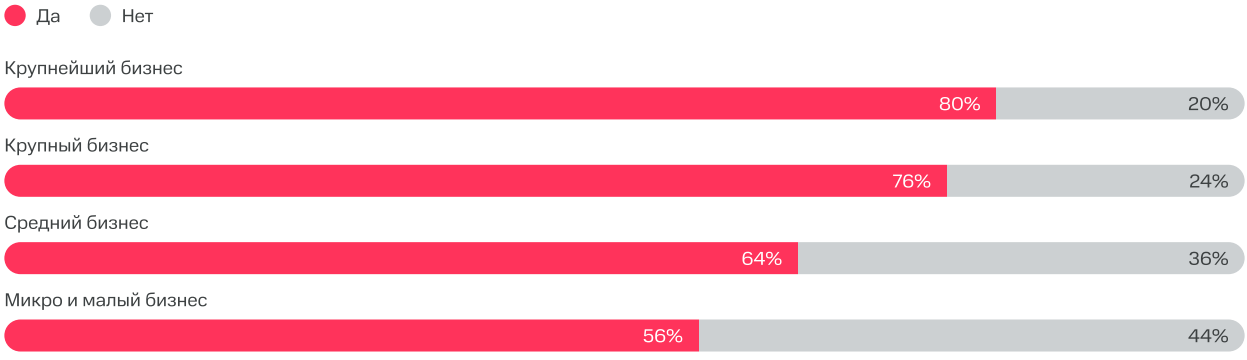
Наличие облачной экспертизы становится одним из ключевых индикаторов цифровой зрелости компании и её способности эффективно масштабировать инфраструктуру, управлять рисками и реализовывать стратегию перехода к гибридным и мультиоблачным моделям. Разница между компаниями, уже имеющими и только развивающими экспертизу в облачных решениях формирует границу между организациями, способными активно развивать облачную архитектуру, и теми, кто пока воспринимает облако скорее как потенциальный вектор развития, а не как инструмент системной трансформации. При этом, доля компаний со сформированной стратегией развития облачных сервисов меньше доли компаний, имеющих экспертизу. Это означает, что часть компаний с экспертизой всё ещё работает в рамках ограниченного сценарного поля, не выходя на уровень полноценного масштабирования или комплексной трансформации ИТ-ландшафта.

Наличие опыта и экспертизы работы с облачными технологиями



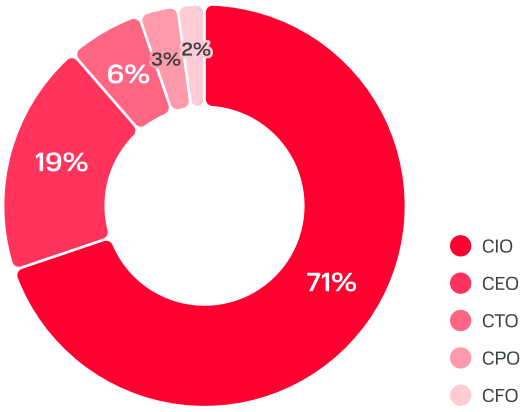
Наличие опыта не обязательно означает зрелость практик. Во многих случаях речь идёт о внедрении отдельных сервисов — резервного копирования, электронной почты — без перехода к продвинутым архитектурам с использованием CI / CD, автоматизированного управления, FinOps и средств контроля SLA. Уровень экспертизы в работе с облачными технологиями закономерно повышается с ростом размера компаний, поскольку у больших компаний больше возможностей в плане найма, обучения сотрудников. Также такое распределение отражает стратегические приоритеты. Крупный бизнес чаще запускает масштабные цифровые инициативы, инвестирует в DevOps и мультиоблачные архитектуры, имеет выделенные ИТ-департаменты и осознанную ИТ-стратегию.

Наличие опыта и экспертизы работы с облачными технологиями по сегментам бизнеса



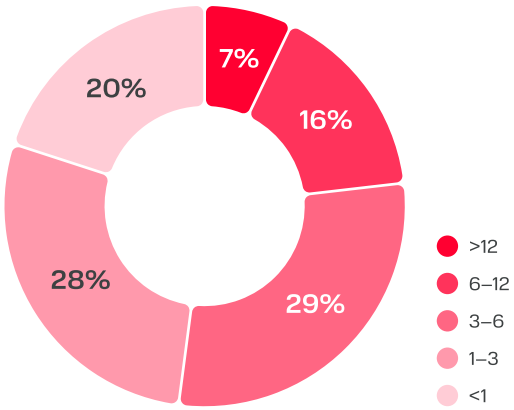
Если смотреть на отраслевой срез, то картина получается более фрагментированной. Лидерами по облачной экспертизе являются ИТ (90% имеют соответствующую экспертизу), финансы (84%), медиа и развлечения (79%),. Высокий уровень вовлечённости здесь объясняется либо самой природой отрасли (как в ИТ), либо необходимостью в высокой скорости реакции на рынок, гибкости в масштабировании или соблюдении высоких стандартов безопасности.
Таким образом, экспертиза в области облаков остаётся неоднородной.

Ключевые сотрудники (ЛПР) в процессе миграции в облако



Длительность процесса миграции в облако

Количество месяцев



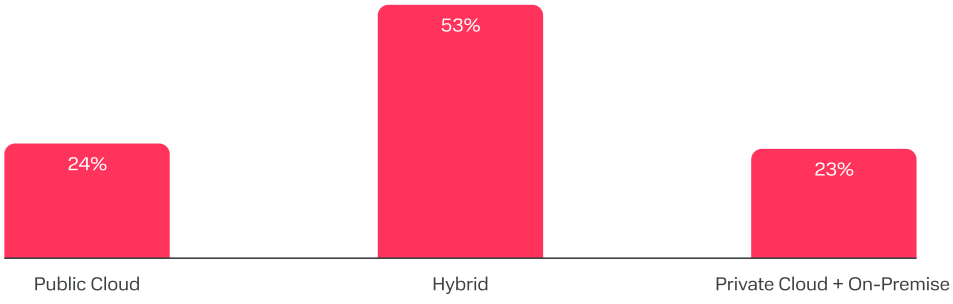
В большинстве компаний решения о переходе в облако принимаются на уровне C-Level. В каждом 5 случае, решение о миграции принимает непосредственно CEO, что отражает невысокую долю стратегической вовлечённости первого лица, хотя именно эта вовлечённость может способствовать синергии ИТ и бизнеса и ускорению трансформации.

Анализ сроков миграции демонстрирует значительную зависимость от масштабов компании и сложности ИТ-ландшафта. Для 20% компаний процесс занял менее месяца, что может свидетельствовать о компактной инфраструктуре и ограниченном объёме переноса. Наиболее распространённым оказался диапазон от 1 до 6 месяцев (57% компаний), характеризующий сценарии со средней или высокой степенью трансформации процессов компании и перестройкой архитектуры. При этом 23% затратили на миграцию более полугода, что типично для компаний с существенным объёмом legacy, сложными требованиями к безопасности или регулируемыми сегментами.

> Multicloud уже здесь, 41% компаний использует более 1 провайдера

Типы развертывания инфраструктуры

Множественный ответ



Публичные и мультиоблачные подходы востребованы (по 36% соответственно), что отражает стремление к гибкости, масштабируемости и диверсификации рисков. Поскольку опрос допускал множественный выбор, данные подтверждают тенденцию к использованию комбинированных архитектур: большинство компаний используют сразу несколько моделей для балансировки безопасности, экономической эффективности и устойчивости инфраструктуры. Это свидетельствует о зрелости ИТ-стратегий и осознанном подходе к архитектуре инфраструктуры.

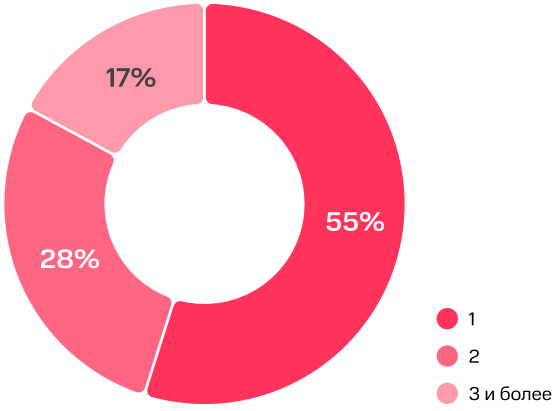
Крупные (2-15 млрд руб.) и крупнейшие (>15 млрд руб.) компании чаще отдают предпочтение частным инсталляциям и On-Premise решениям, подчеркивая важность безопасности, регуляторных требований и устойчивости к внешним рискам (например, санкциям или сбоям у внешних провайдеров). Микро и малый бизнес (до 800 млн руб.), в свою очередь, более гибок и готов к инновациям, за счёт чего охотнее использует публичные и мультиоблачные решения, минимизируя инфраструктурные издержки.

Чем крупнее бизнес, тем больше multicloud решений

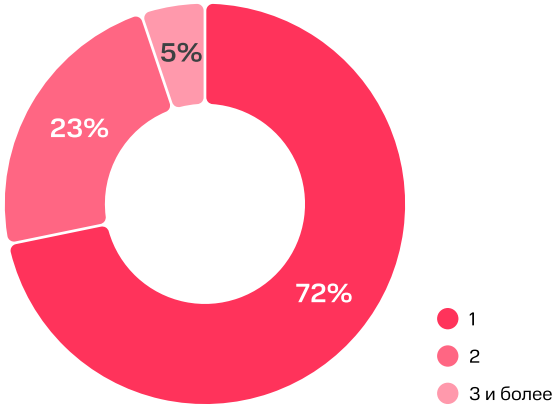
> Мультиоблачная архитектура становится стандартом для зрелых компаний. С увеличением числа провайдеров возрастает и сложность инфраструктуры. Это требует более высокой квалификации персонала, развития DevOps/FinOps практик и автоматизации управления. Компании, выбирающие одного провайдера, делают ставку на простоту и экономию. Те, кто используют нескольких — на устойчивость, гибкость и инновации, но сталкиваются с дополнительными издержками и сложностями.

Михаил Тутаев
Директор по продуктам MWS Cloud

Количество используемых провайдеров Public Cloud



Количество используемых провайдеров Private Cloud



Для Public Cloud менее характерна single-cloud стратегия: ее выбирают только 55% компаний. Преимуществами является упрощение управления, унификацией процессов и потенциальным снижением издержек за счёт концентрации сервисов у одного провайдера. Однако такая модель повышает зависимость от единственного поставщика, может ограничивать гибкость и увеличивать риски для бизнеса.

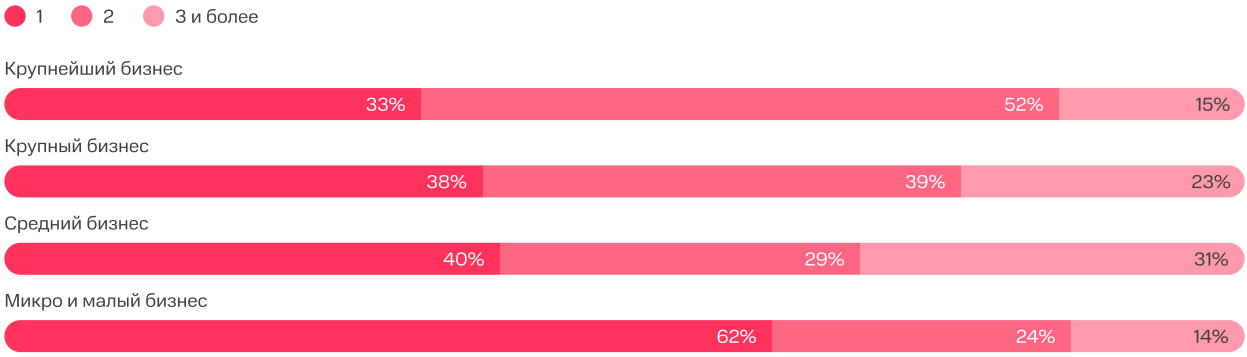
28% компаний задействуют двух провайдеров, реализуя элементы multicloud подхода для диверсификации рисков, повышения отказоустойчивости и доступа к уникальным сервисам разных платформ. 17% используют трёх провайдеров и более, что уже отражает более зрелую распределённую multicloud архитектуру, характерную для организаций с развитой ИТ-инфраструктурой. В сегмент индустрий, использующих наибольшее число провайдеров входят ИТ, финансы и страхование, ритейл, промышленность и HoReCa.

Таким образом, полученные данные фиксируют разноуровневый подход к управлению облачной средой и подтверждают, что многооблачные стратегии чаще встречаются у технологически продвинутых компаний, заинтересованных в балансе между отказоустойчивостью, доступом к разным сервисам и контролем над инфраструктурой.

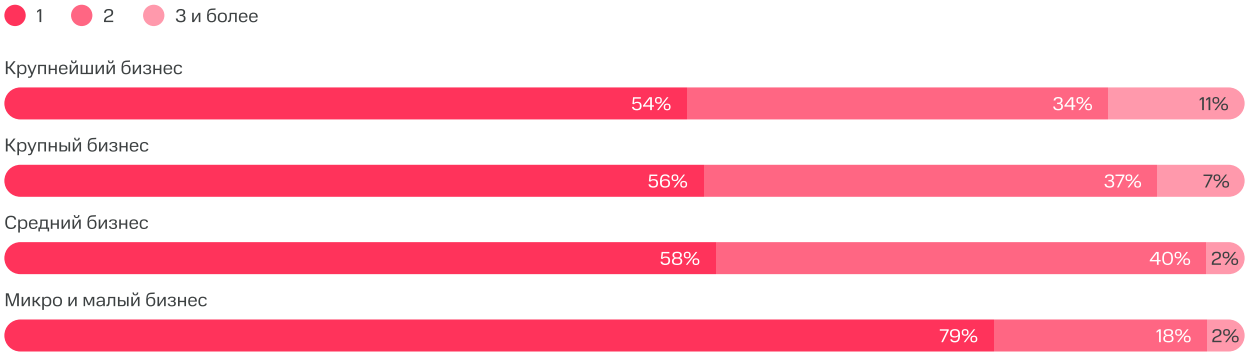
Аналогичная ситуация наблюдается в сегменте Private Cloud. Для большинства компаний (72%) характерен выбор одного провайдера, что обеспечивает единое управление инфраструктурой, унификацию SLA и упрощённое сопровождение решений. Такая стратегия позволяет сфокусироваться на согласовании требований безопасности и регуляторных аспектов с одним поставщиком, однако одновременно повышает зависимость от выбранного партнёра.

23% компаний сотрудничают с двумя провайдерами, что может свидетельствовать о желании минимизировать операционные и технические риски, а также использовать преимущества различных технологических стеков для разных задач. При этом мультиклауд в Private Cloud чаще мотивирован резервированием критичных сервисов и повышением отказоустойчивости.

Количество используемых провайдеров Public Cloud по сегментам бизнеса



Количество используемых провайдеров Private Cloud по сегментам бизнеса



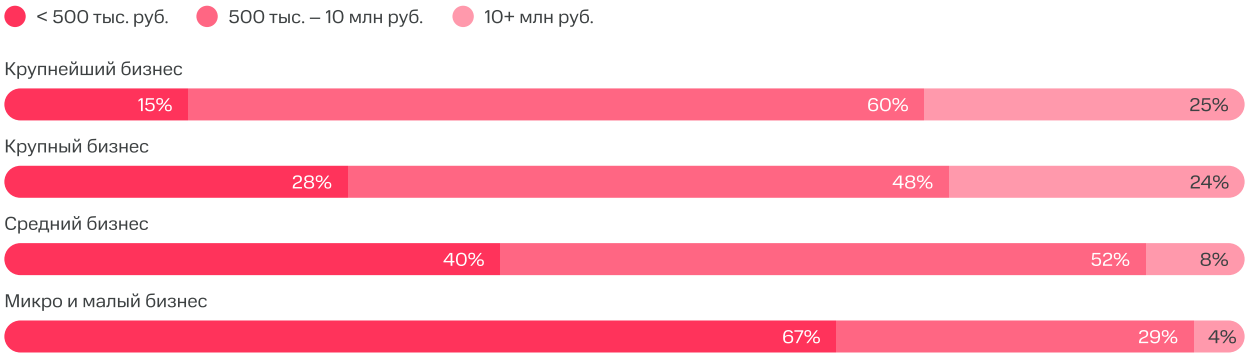
Данные ясно демонстрируют, что размер бизнеса напрямую влияет на применение multicloud-подхода. Крупные компании более склонны использовать продукты и услуги нескольких облачных провайдеров. Для всех компаний кроме микро и малого бизнеса характерно активное использование нескольких публичных облаков: в среднем 61% уже работают с двумя и более провайдерами, а около 20% среднего и крупного бизнеса задействуют инфраструктуру трех и более поставщиков. Это свидетельствует о высокой зрелости их облачных стратегий. Как правило, такие компании распределяют задачи между провайдерами по функциональным зонам: одни используются для хранения данных, другие — для аналитики и ИИ, CI/CD или резервного копирования. Такое решение обеспечивает гибкость, отказоустойчивость и поддерживает бизнес-непрерывность.

При этом бизнес осознанно снижает риски vendor lock-in, избегая зависимости от одного поставщика. Multicloud даёт возможность балансировать нагрузки, выбирать платформы по стоимости и SLA и быстрее внедрять новые технологии. Для этих компаний multicloud уже не просто элемент инфраструктуры, а инструмент управления рисками, технологической независимости и ускорения цифровых инноваций.

Исследование подтвердило прямую зависимость между размером бизнеса и масштабом инвестиций в облачные технологии. Для микро и малого бизнеса (выручка <800 млн руб.) характерны минимальные расходы: около 67% тратят на облака менее 100 тыс. руб. Это связано как с масштабами операций и сложностью структуры, так и с необходимостью обеспечения отказоустойчивости, безопасности и работы с большими данными. Крупные компании строят мультиоблачные архитектуры, развивают аналитику, автоматизацию и High Performance Computing, чаще создают собственные цифровые продукты, что требует значительных вложений и внедрения сервисов контейнеров и ИИ.

Малый бизнес, напротив, ограничивается базовыми ИТ-потребностями — виртуальными серверами, хранилищами и SaaS для бухгалтерии и документов, что удерживает расходы на низком уровне. В целом для рынка наиболее типичны бюджеты до 2 млн руб., что отражает умеренную зрелость и значительную дифференциацию потребностей.

Годовой объем облачных затрат по сегментам бизнеса



> Рынок облачных технологий в России демонстрирует явное смещение в сторону более крупных бюджетов, что отражает рост зрелости и стратегического значения облачных инфраструктур для бизнеса. Корпоративный рынок переходит от фазы точечных пилотных внедрений к системной трансформации, охватывающей ключевые процессы и сервисы. Это означает растущую востребованность комплексных платформ, способных поддерживать сложные мультиоблачные и гибридные сценарии, обеспечивать отказоустойчивость на уровне бизнес-критичных приложений и предлагать прозрачные механизмы управления затратами.

Полина Ли
Руководитель центра аналитики и исследований MWS

Годовой объем облачных затрат по индустриям

	< 500 тыс.	500 тыс. – 10 млн	10+ млн
ИТ	32%	44%	24%
Финансы и страхование	40%	48%	12%
Ритейл	50%	39%	11%
Развлечения и медиа	44%	46%	10%
HoReCa	53%	37%	10%
Наука и образование	44%	48%	10%
Недвижимость и строительство	59%	34%	7%
Транспорт и логистика	53%	41%	6%
Профессиональные услуги	76%	19%	5%
Здравоохранение	74%	22%	4%
Добыча и переработка полезных ископаемых	49%	48%	3%
Промышленность	69%	30%	2%

Распределение годового объёма облачных затрат по индустриям позволяет оценить зрелость внедрения облачных технологий и выявить различия в стратегическом подходе между секторами. Значительная часть компаний по-прежнему сосредоточена в сегменте минимальных расходов — до 500 тыс. руб. в год. Это характерно для таких отраслей как профессиональные услуги, здравоохранение, где облака используются точечно и не становятся ядром бизнес-модели.

Наибольшую зрелость демонстрируют индустрии, где более 10% компаний уже тратят свыше 10 млн руб. в год: ИТ, финансы и страхование, HoReCa, наука и образование. Для них характерны мультиоблачные архитектуры, DevOps и использование облаков в критически важных процессах.

Во всех отраслях уже встречаются компании с высокими бюджетами на облака, что отражает начавшуюся дифференциацию: технологические лидеры выстраивают сложные модели потребления, тогда как большинство остаётся на базовом уровне. В дальнейшем можно ожидать рост доли крупных затрат на фоне усиления доверия к облакам, развития собственной экспертизы и адаптации к требованиям регуляторов.

57% компаний планируют наращивать использование облаков, что отражает умеренные темпы углубления стратегий, частично из-за достигнутого насыщения и существующих барьеров. При этом 31% респондентов собираются развивать частные облака — это подтверждает растущий запрос на контроль над данными и соответствие требованиям локализации и безопасности. Частные решения всё чаще становятся ядром гибридных стратегий, дополняя или заменяя On-Premise инфраструктуру.

Публичные облака также сохраняют спрос: 39% компаний планируют увеличить их использование, рассматривая их как инструмент для снижения затрат, ускорения цифровых проектов и гибкого масштабирования.

Таким образом, компании выстраивают сбалансированные подходы: с приоритетом на private для управления рисками и соответствия нормативам, но с сохранением интереса к public для оптимизации и быстрого запуска инициатив, что поддерживает рост гибридных и мультиоблачных моделей.

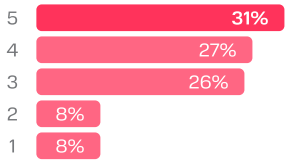
> “ Ключевыми драйверами перехода в облако остаются модернизация ИТ, операционная эффективность и стратегическая устойчивость. Облачные решения позволяют запускать инновации без крупных инвестиций, автоматизировать инфраструктуру, оптимизировать расходы и быстрее адаптироваться к внешним вызовам. В совокупности эти факторы формируют устойчивую мотивацию для миграции, при этом модернизация инфраструктуры выступает главной причиной таких проектов.

Галина Гайдаржи
Бизнес-аналитик MWS Cloud

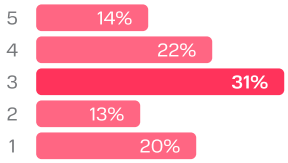
Ключевые факторы принятия решения о миграции в облако

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

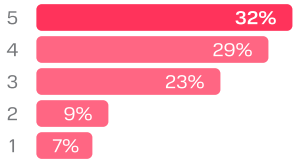
Масштабирование ресурсов



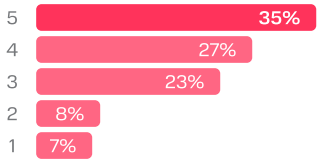
Переход от CAPEX модели к OPEX



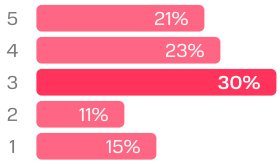
Снижение трудозатрат на обслуживание



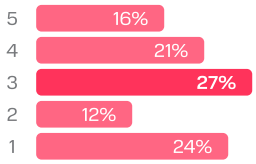
Модернизация ИТ-инфраструктуры



Снижение time-to-market новых продуктов



Невозможность приобретения оборудования



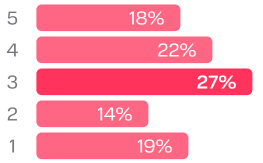
Ни один из барьеров не получил преобладающих максимальных оценок, что говорит о наличии на рынке инструментов для их смягчения. Однако ряд проблем сохраняет свою актуальность: технологические, организационные, кадровые и финансовые. Чаще всего компании отмечают сложность прогнозирования облачных расходов: почти 70% поставили этому барьеру 3 балла и выше, что указывает на нехватку прозрачности и зрелых FinOps-практик.

Существенными остаются и дополнительные затраты на миграцию — временное удвоение ресурсов, оплату услуг и лицензий, адаптацию процессов, а также необходимость поддерживать параллельно локальную и облачную инфраструктуры, что увеличивает нагрузку на бюджеты и команды.

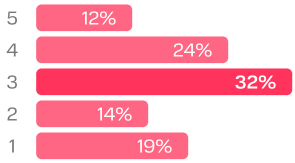
Сложности в процессе миграции в облако [1/2]

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

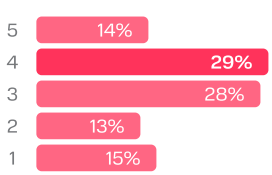
Отсутствие нужных компетенций среди сотрудников



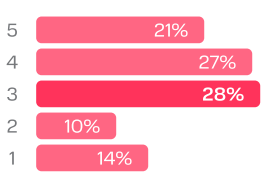
Сложность в оценке предполагаемых расходов на требуемую инфраструктуру



Необходимость временного дублирования инфраструктуры



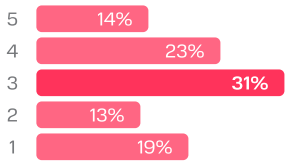
Сложность переноса большого объема данных



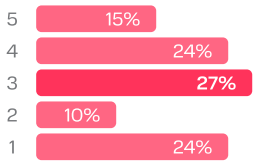
Сложности в процессе миграции в облако [2/2]

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

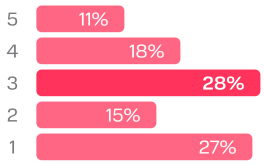
Дополнительные расходы на этапе переноса систем в Облако



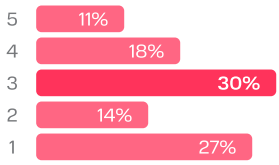
Невозможность интеграции в Облако используемых локальных решений (устаревшее ПО / Оборудование)



Отсутствие поддержки вендора в процессе миграции



Отсутствие дорожной карты миграции



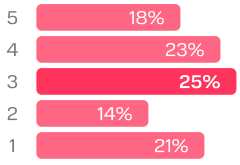
Согласно опросу, дополнительные расходы при миграции в облако не воспринимаются компаниями как критичный барьер, что свидетельствует о зрелости рынка и готовности закладывать такие затраты в бюджеты. Чаще всего упоминаются расходы на развёртывание тестовых контуров: 31% считают их средней важности, а всего более 56% — значимыми, что отражает норму пилотных запусков для снижения рисков. Сопоставимую значимость имеют траты на модернизацию локальной инфраструктуры для подготовки к интеграции с облаками.

Это подтверждает, что компании всё чаще заранее планируют бюджеты на пилоты и апгрейд On-Premise, воспринимая их как естественную часть миграции, а не внеплановые расходы.

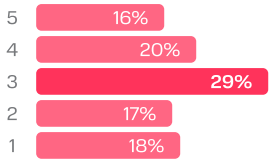
Дополнительные расходы в процессе миграции в облако

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

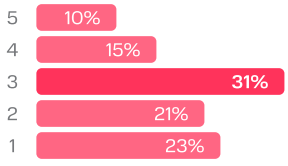
Переобучение / найм сотрудников для качественной работы с Облаком



Обновление локальной инфраструктуры



Развертывание тестового контура для проверки работоспособности рассматриваемого решения



Среди рисков наибольшую важность компании придают угрозам утечки персональных данных, коммерческой тайны, кибератакам и уходу поставщика с рынка. Особенно вопросы информационной безопасности остро стоят у пользователей мультиоблачных и гибридных моделей, что подчёркивает роль защиты данных при проектировании таких архитектур. Наибольшую чувствительность демонстрируют банки.

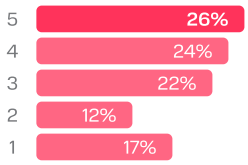
Отдельно выделяется риск невозможности обновления оборудования из-за ухода вендоров или санкций: здесь мнения разделились, но для гостинечно-ресторанного бизнеса, промышлен-ности этот риск стал критическим (40% дали максимальную оценку), что подчёркивает их уязвимость.

Перерасход бюджета на облака для российских компаний менее актуален (19%) по сравнению с мировыми 69%, что связано с меньшей распространённостью мультиоблаков. В итоге компании больше всего сосредоточены на вопросах КБ и устойчивости поставок, тогда как финансовые риски и неполнота сервисов рассматриваются скорее как управляемые барьеры.

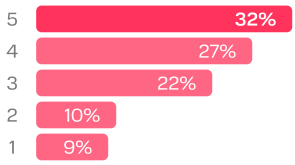
Риски при миграции в облако

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

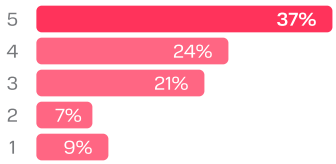
Уход поставщика с рынка



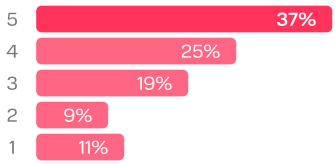
Кибератаки на облачные сервисы провайдера



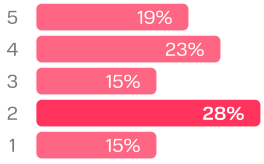
Утечки персональных данных



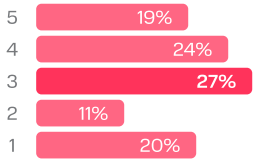
Утечка данных коммерческой тайны



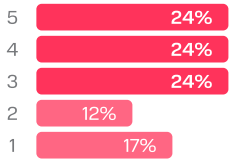
Неконтролируемый рост затрат на Облачную инфраструктуру



Отсутствие требуемого функционала у провайдера



Невозможность обновления оборудования поставщика (санкции)



Решения о масштабировании облаков всё чаще принимаются не только по техническим причинам, но и как часть стратегии роста и цифровой трансформации. Главными мотива-торами стали экономическая целесообразность и внедрение новых автоматизированных систем — оба фактора получили максимальную важность у 33% компаний. Это подтверж-дает, что облака всё чаще рассматриваются как инструмент оптимизации затрат, гибкости и ускоренной перестройки бизнес-моделей.

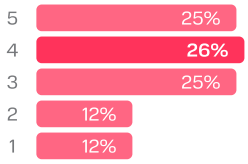
Схожая динамика наблюдается и по фактору сокращения локальной инфраструктуры: 33% оценили его на среднем уровне, а ещё 40% присвоили высокий приоритет. Это указывает на тренд ухода от On-Premise в пользу облаков для снижения CAPEX и перехода к более управляемым OPEX-моделям.

В итоге компании всё чаще используют облака как средство стратегической перестройки, что поддерживает рост их доли в ИТ-бюджетах и смещает акценты с технических на бизнес-драйверы.

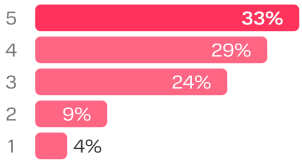
Ключевые факторы при принятии решения о масштабировании потребления облака

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

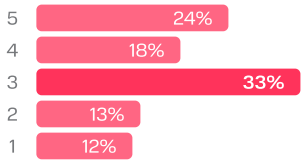
Выпуск новых продуктов



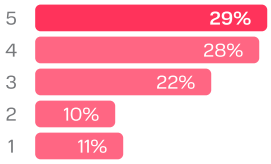
Экономическая выгода



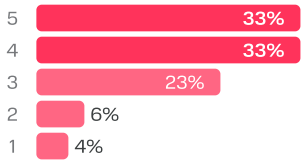
Сокращение локальной инфраструктуры (полный отказ от нее)



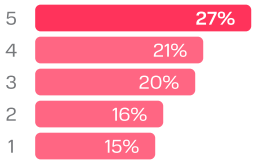
Увеличение клиентской базы или выпуска существующей продукции



Внедрение новых автоматизированных систем



Расширение географии присутствия компании

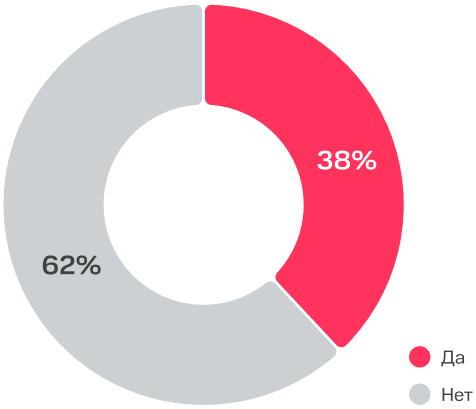


> “ Рынок облачных технологий в России демонстрирует поступательный переход от локальных ИТ-инициатив к стратегическому переосмыслению бизнес-моделей. Для большинства компаний облачные решения становятся не просто инструментом оптимизации затрат и ускорения внедрения цифровых проектов, но и ключевым элементом повышения устойчивости и адаптивности бизнеса. Заметно преобладание частных облаков, что отражает возрастающие требования к контролю над данными и соответствию отраслевым и регуляторным стандартам. При этом публичные облака продолжают играть важную роль в составе гибридных архитектур, позволяя компаниям гибко масштабировать ресурсы и оперативно запускать новые инициативы без значительных капитальных вложений.

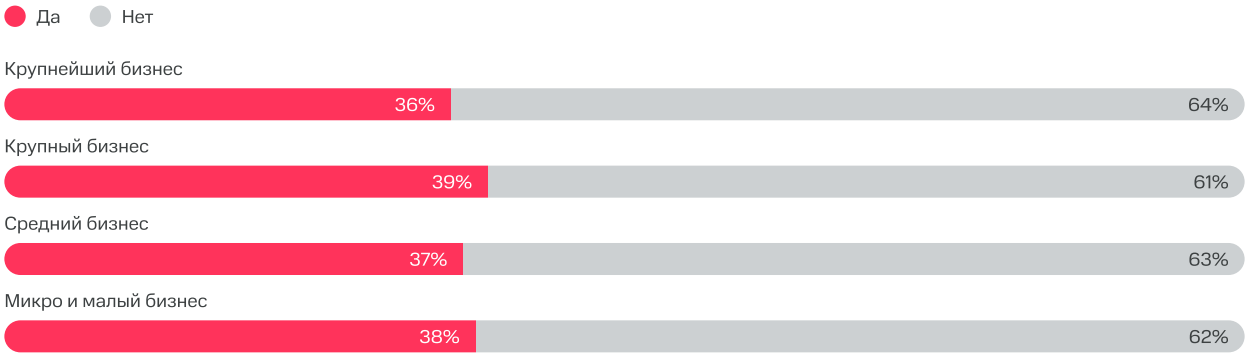
Данила Егоров
Директор по бизнес-стратегии MWS Cloud

В последние несколько лет активно обсуждается проблема нехватки квалифицированных кадров, однако в сфере облачных технологий более 62% компаний не имеют проблем в найме экспертов. Наличие проблем с наймом не зависит от размера компаний, что говорит об общей нехватке специалистов, вне зависимости от уровня компетенций и уровня заработной платы. Среди индустрий также незначительна дифференциация по данному показателю. Незначительно большие сложности отмечаются наука и образование и промышленность.

Наличие проблем в найме экспертов в сфере облачных технологий



Наличие проблем в найме экспертов в сфере облачных технологий по сегментам



Вопрос экспертизы напрямую связан с распространённостью прикладного ПО по модели SaaS. Доля потребляющих SaaS решений остаётся невысокой — на уровне 21–34% в зависимости от сегмента бизнеса. Причём в среднем и крупном бизнесе эти показатели даже ниже, чем в малом. Вероятно, это отражает настороженность к SaaS из-за безопасности, ограничений по функционалу и привязки к поставщику. Вместо этого компании предпочитают развивать собственные облачные среды или использовать IaaS / PaaS как более гибкие платформы. Таким образом, SaaS остаётся точечным решением, а не массовым стандартом. На фоне нехватки внутренней экспертизы компании активно используют профессиональные сервисы. Более половины респондентов прибегают к технической поддержке, 40% — к обучению персонала, треть — к аутсорсингу. Это подчёркивает, что рынок облачных решений развивается не только за счёт продаж ресурсов, но и за счёт сопутствующих сервисов, сопровождающих весь цикл миграции.

Профессиональные сервисы, используемые компаниями для развития облачных технологий

53%
Техническая поддержка

40%
Обучение

33%
Аутсортинг

19%
Консалтинг (стратегия)

11%
Не используем

РАСШИРИМ ВОЗМОЖНОСТИ ВАШЕЙ ИНФРАСТРУКТУРЫ

MWS CONTAINER PLATFORM

Надёжная платформа для разработки и эксплуатации контейнерных приложений. Помогает быстрее внедрять инновации, проводить цифровую трансформацию и запускать ИТ-продукты

на 40%
снижает нагрузку на ИТ-команды

на 70%
ускоряет выпуск новых приложений и упрощает их эксплуатацию

на 80%
автоматизирует ручные операции

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

ВНЕДРЕНИЕ ТЕХНОЛОГИЙ: ОБЛАКО

В данном исследовании технологий, помимо общей оценки, в которую входят бюджеты, стратегия, экспертиза, драйверы и барьеры внедрения, критически важно дополнительно оценить потребление соответствующих технологических продуктов.

Для транспарентности накопленных результатов исследования последующая аналитика носит фактический характер, без дополнительных интегральных расчетов. Выводы и инсайты, которые сопровождают полученные данные в рамках исследования, могут быть независимо проанализированы пользователем данного отчета, поскольку показатели отражают непосредственные ответы респондентов. Таким образом, данный блок является прикладным инструментом для принятия решений о потреблении исследуемых технологий.

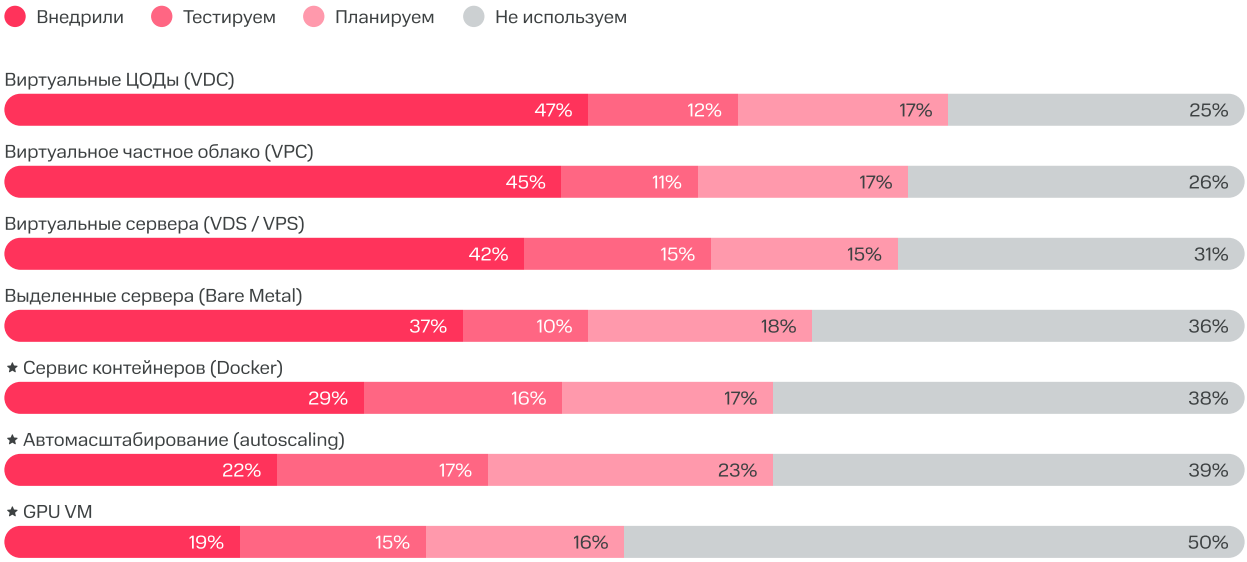
Для оценки среди полученных субкатегорий тех продуктов, которые имеют повышенный потенциал роста, введен подход, получивший название «Формула потенциала роста субкатегорий». Данная формула представляет собой сопоставление: с одной стороны параметра «внедрили», с другой стороны суммы параметров «тестируем» 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

Раздел с продуктовыми решениями демонстрирует классические продуктовые категории, которые относятся к сегментам Infrastructure as a Service(IaaS), Platform as a Service (PaaS) и Software as a Service (SaaS). Облака являются фундаментом для комплиментарных технологий, в частности для кибербезопасности и искусственного интеллекта. Следовательно, высокий уровень развития и потребления облаков упрощает процесс тестирования и интеграции более специализированных технологий.

Вычисления



Наиболее часто используемыми продуктовыми субкатегориями ожидаемо являются виртуальные ЦОДы (VDC) и виртуальные частные облака (VPC), 47% и 45% внедрений соответственно. Данные решения являются commodity для существенного количества компаний из скоупа респондентов, что коррелирует с рыночными открытыми данными по потреблению. В структуре выручки облачных провайдеров вычисления, наряду с другими продуктовыми категориями сегмента IaaS, традиционно занимают наибольшую долю.

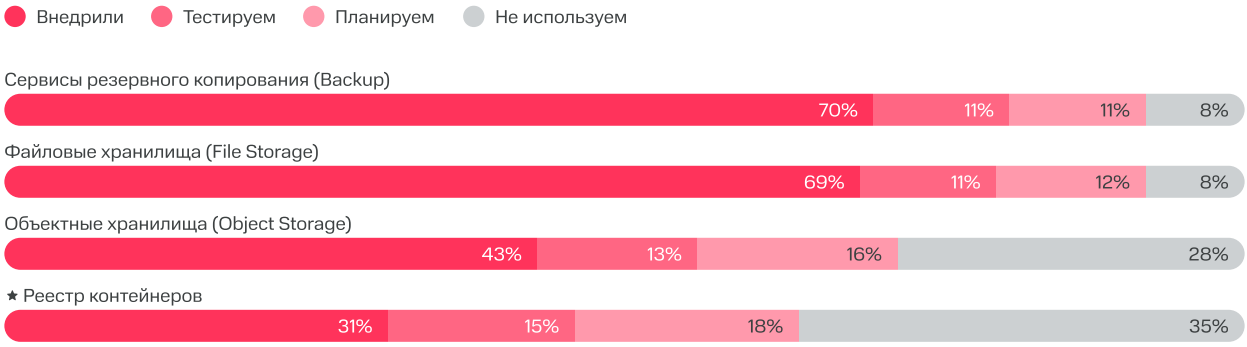
Также полученная аналитика поддерживает актуальный на рынке тезис о наличии высокого спроса и на публичные, и на частные инсталляции. Крупнейшие облачные провайдеры активно реагируют на данный тренд, развивая гибридные решения.

Отдельно обращаем внимание на продуктовую субкатегорию сервисы контейнеров (Docker), которые полноценно внедрены только у трети опрошенных компаний, однако также треть пользователей в сумме уже тестируют (16%), либо запланировали (17%) интеграцию.

Несмотря на высокую актуальность и повсеместное упоминание технологий ИИ, продуктовая субкатегория, относящаяся к вычислениям для работы с ИИ (GPU VM) фактически используется сравнительно небольшим числом компаний из опрошенных. Это связывается с тем, что большинство корпоративных пользователей работают с инструментами ИИ на уровне ассистентов и бизнес-приложений. Виден высокий спрос на GPU, однако этот спрос поддерживается ограниченным кругом клиентов, заинтересованных в высокопроизводительных вычислениях и зачастую обладающих собственной командой разработки ИИ. Наличие такой команды отмечается только у 31% опрошенных компаний. Активное потребление инфраструктурных решений для задач ИИ не является одинаково значимым для различных индустрий и сегментов рынка.

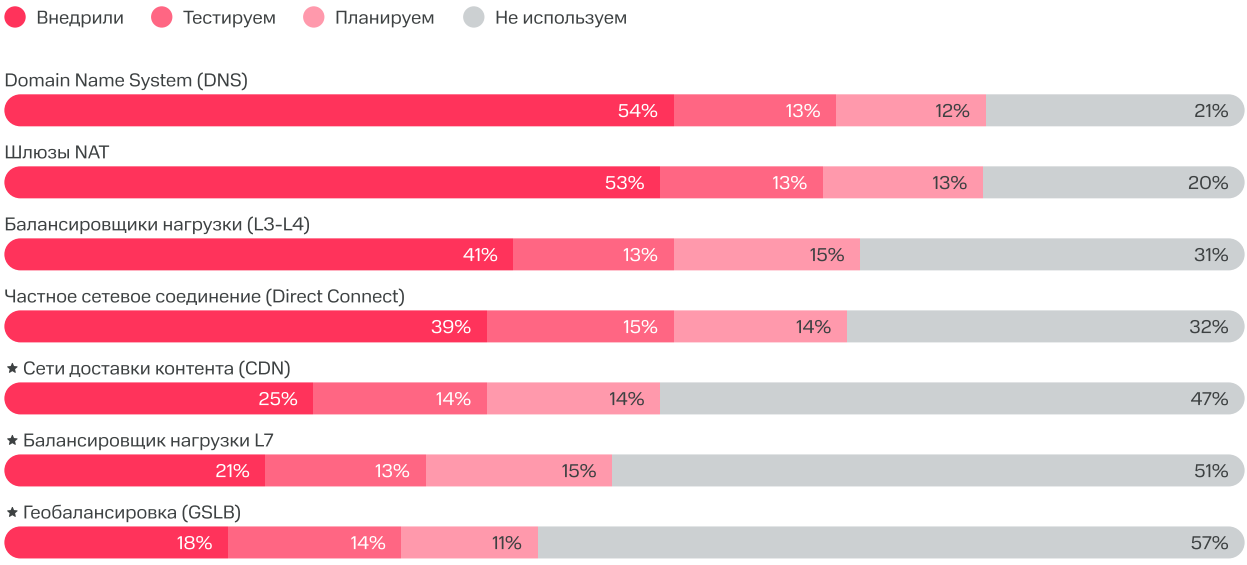
★ — высокий потенциал

Хранилище



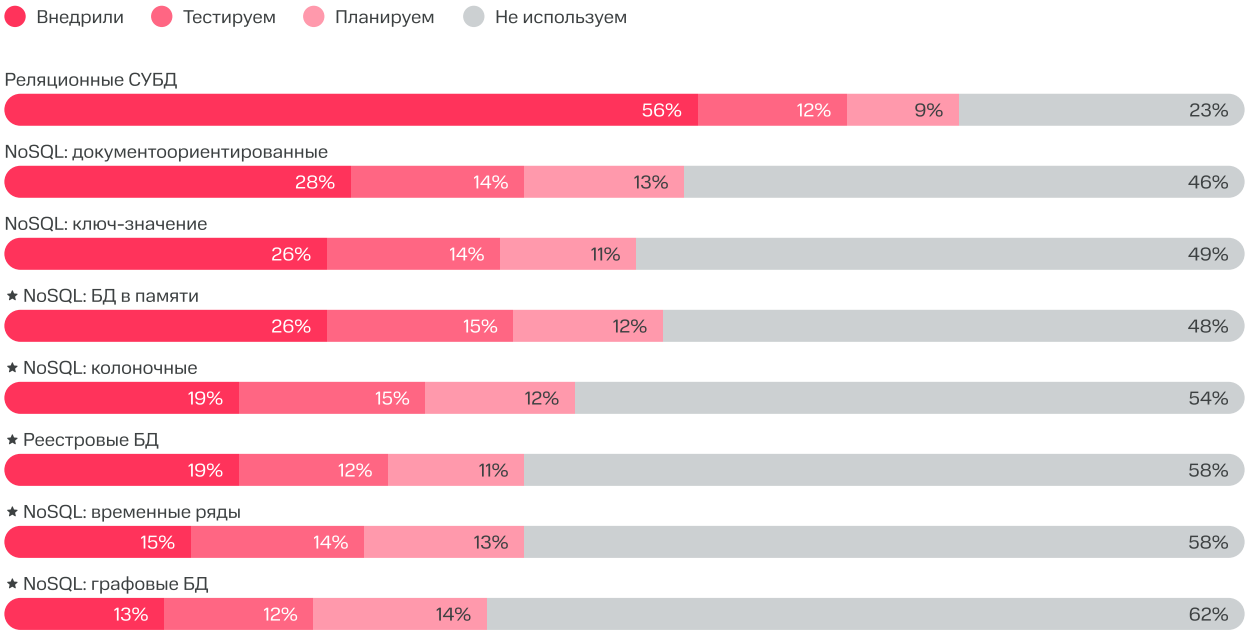
Хранилище является базовой продуктовой категорией для подавляющего большинства компаний на рынке. Можно однозначно оценить, что продукты резервного копирования, файловые хранилища, а также диски виртуальных машин стали commodity для подавляющего большинства корпоративных клиентов в России. Наблюдается существенный разрыв в уровне потребления между решениями, обеспечивающими выполнение повседневных задач и специализированными продуктовыми субкатегориями – уровень потребления может отличаться более, чем в 2 раза. Но при этом у объектных хранилищ и реестров контейнеров отмечаются высокие резервы роста: компании часто отмечают, что планируют использовать либо тестируют данные продукты.

Сеть и доставка контента



Зачастую компании, которые переходят в облака не кастомизируют отдельные сетевые параметры, а пользуются комплексным решением со стандартными настройками. Частная настройка с использованием отдельных продуктов в данной категории, требуется для территориально-распределенных компаний, например, с широкой филиальной сетью. Такие компании зачастую являются представителями крупного и крупнейшего бизнеса, для которых использование сетевых продуктов с тонкой настройкой является стандартным сценарием потребления облаков. Наиболее характерно использование данных продуктов для секторов ИТ и транспорта.

Базы данных



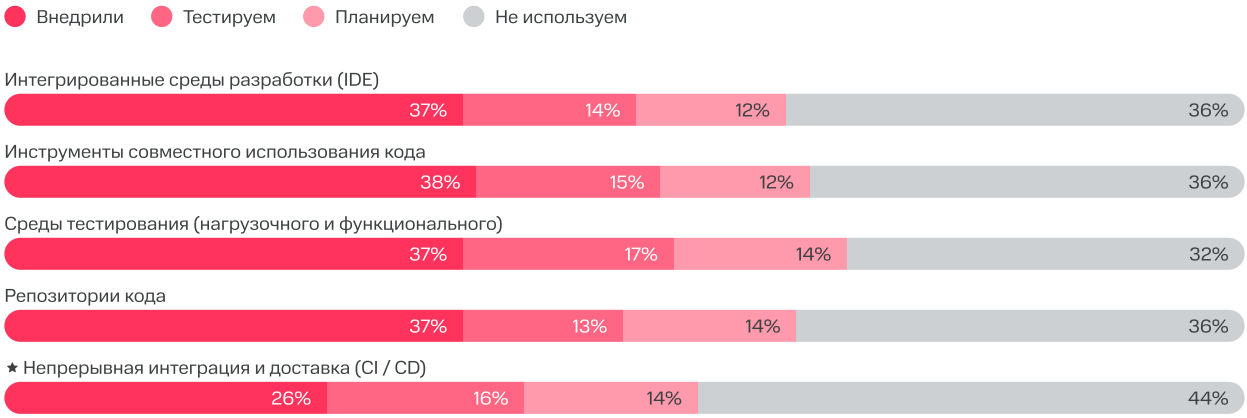
Базы данных являются наиболее популярной продуктовой категорией в сегменте PaaS. Реляционные базы данных ожидаемо являются наиболее внедряемым классом продуктов среди анализируемых, что объясняется нативным применением для большинства сценариев разработки бизнес-приложений. Второй субкатегорией по частоте использования являются NoSQL базы данных (28% внедрений или 55% положительных ответов совокупно), что отражает рост интереса к гибким, горизонтально масштабируемым решениям. При этом, SQL остается типом баз, который внедрило или рассматривает к внедрению подавляющее большинство компаний. Это может отражать сложность поддержки новых форматов баз данных и недостаток кейсов использования альтернативных решений.

> “ Рынок облаков в России демонстрирует высокую зрелость в базовых инфраструктурных решениях — виртуальные ЦОДы, VPC и хранилища стали фактически стандартом для большинства компаний. Вместе с тем, сервисы контейнеров и инфраструктура для ИИ пока охватывают меньшую часть рынка, но обладают заметным потенциалом роста: треть компаний уже их внедрила, а сопоставимая доля тестирует или планирует интеграцию. Существенные перспективы также видны у объектных хранилищ и сервисов вокруг управления контейнеризированными приложениями. Это задает двойной фокус для дальнейшего развития: укрепление позиций в массовых IaaS-решениях и параллельное наращивание предложений для более продвинутых архитектур и специфических отраслевых кейсов.

Михаил Тутаев
Директор по продуктам MWS Cloud

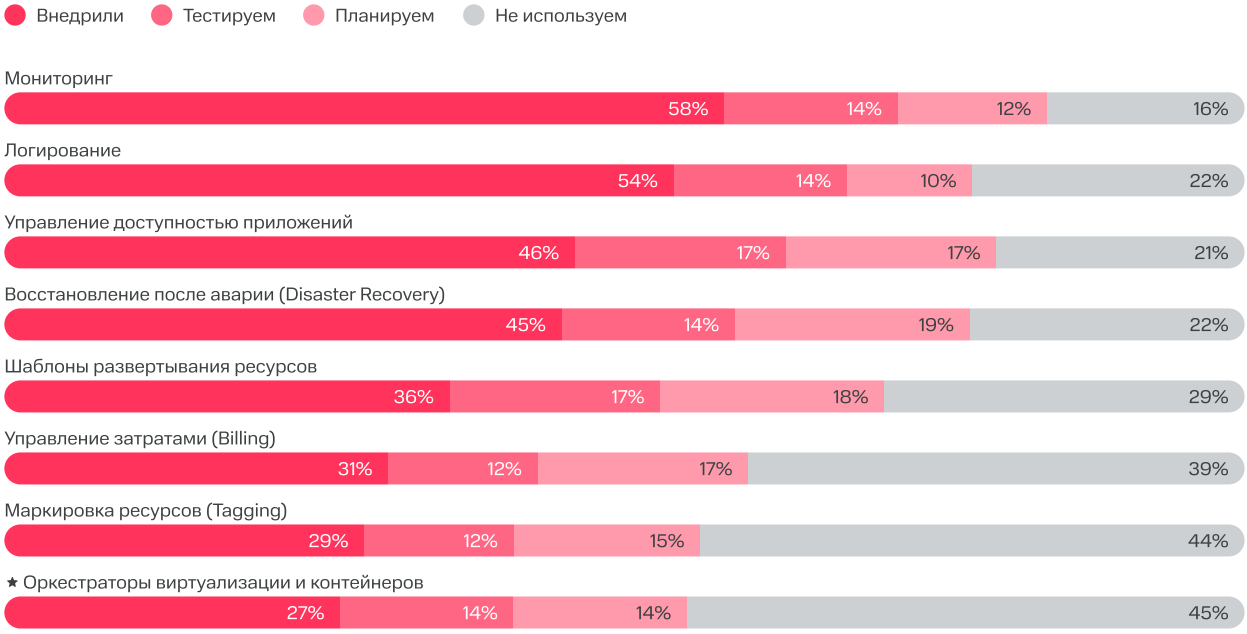
★ — высокий потенциал

Средства разработки



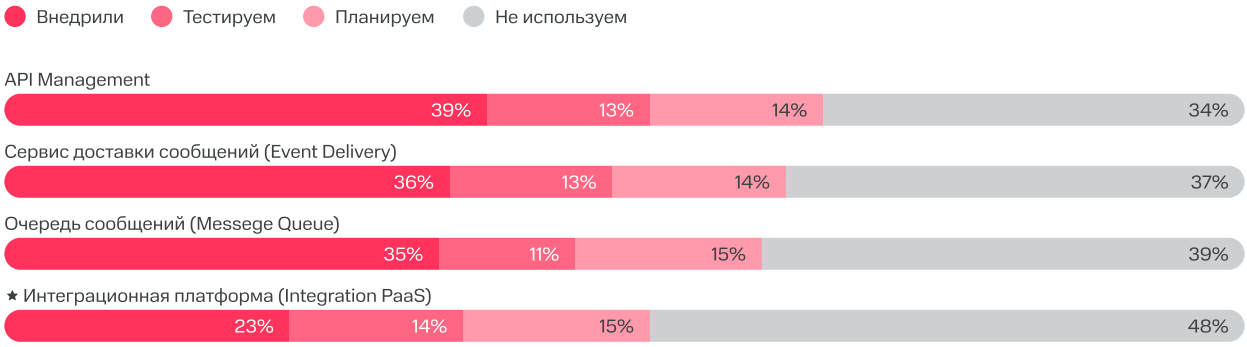
Средства разработки являются одной из базовых субкатегорий сегмента PaaS. Средние значения по исследуемым параметрам связываются с тем, что данные продукты зачастую являются неотъемлемыми компонентами платформы и не выделяются в отдельные продукты. Потенциал роста, который отражается в высоких значениях тестирования и планирования внедрения (в сумме порядка 28% для рассматриваемых продуктов) коррелирует с темпами роста рынка платформенных решений в России. Непрерывная интеграция и доставка контента (CI / CD) требует высокого уровня зрелости команд разработки. Респондентами из скоупа исследуемых компаний данная категория отмечалась реже остальных.

Инструменты управления



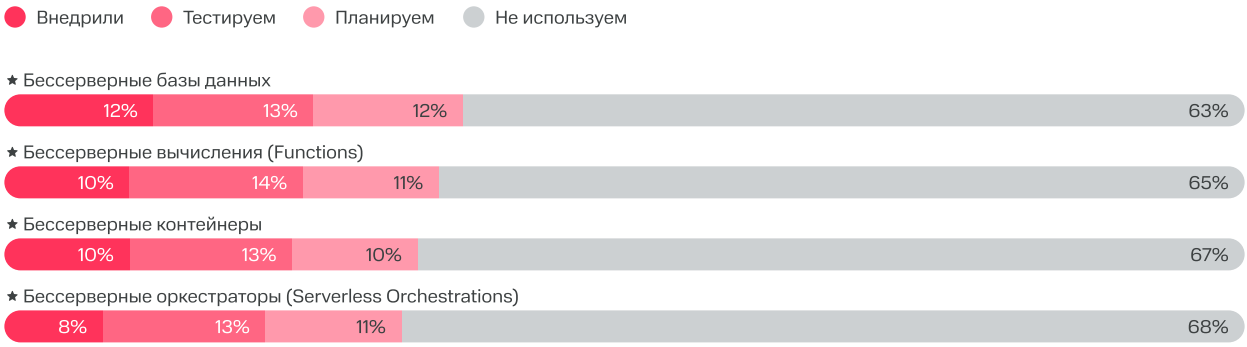
Продуктовые субкатегории, относящиеся к инструментам управления, также в значительной доле случаев являются неотъемлемым свойством или функционалом платформы облачного провайдера. Но в отличии от категории Средства разработки, респонденты исследования существенно чаще отметили положительным ответом данные продуктовые субкатегории. Это иллюстрирует базовый характер перечисленных решений для облачных клиентов. Особенную важность применения данных компонентов можно наблюдать в компаниях крупного и крупнейшего бизнеса, устойчивость инфраструктуры для которых имеет критическое значение. Применение решений Disaster Recovery дополнительно характеризует зрелость управления ИТ-рисками компаний.

Интеграция



Данные решения, как правило являются базовыми компонентами платформ. Комплексные решения для интеграции необходимы для крупных компаний с многоуровневой корпоративной архитектурой, в которой реализуются сложные сценарии интеграции и внесения изменений в бизнес-архитектуру, архитектуру данных, архитектуру приложений и технологический стек. Развитые интеграционные платформенные решения, в том числе поддерживают переход от монолитной к компонентной и микросервисной архитектурам. Многообразие и зрелость интеграционных продуктов напрямую влияет на технологический контракт между поставщиком и потребителем, что в конечном итоге сказывается на доступности, времени ответа, пропускной способности и ограничениях связанных с безопасностью.

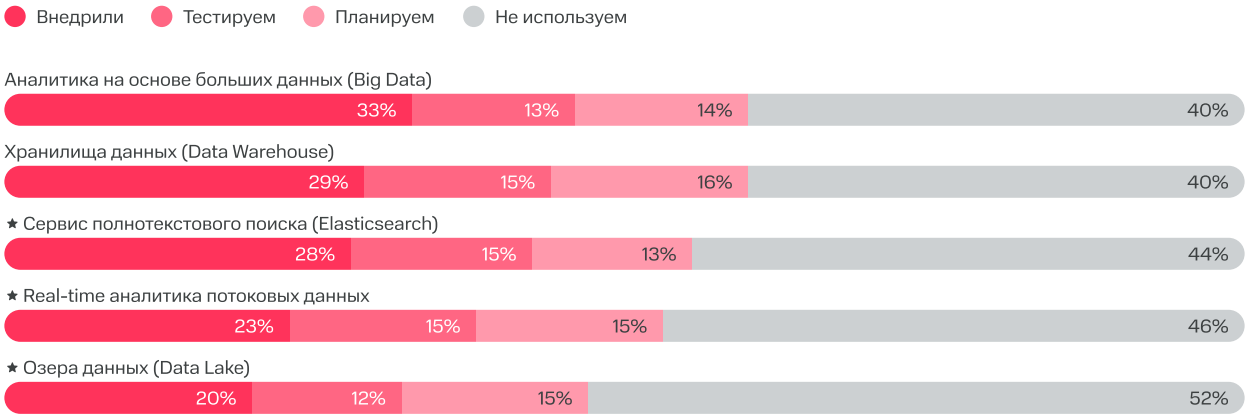
Serverless



Внедрение serverless решений остается на начальном уровне, что указывает на большую долю legacy-архитектур в технологическом стеке компаний, а также на нехватку DevOps / cloud native-практик, особенно в сравнении с зарубежными компаниями. Большинство опрошенных компаний не только не используют, но и не планируют внедрять соответствующие решения. Малая активность остается даже на уровне тестирования, что может говорить о низком уровне осведомленности пользователей о преимуществах serverless, а также о недостаточных компетенциях сотрудников для внедрения решений данного класса. Дополнительной причиной низкого уровня востребованности может выступать отсутствие соответствующих предложений у большого количества провайдеров.

★ — высокий потенциал

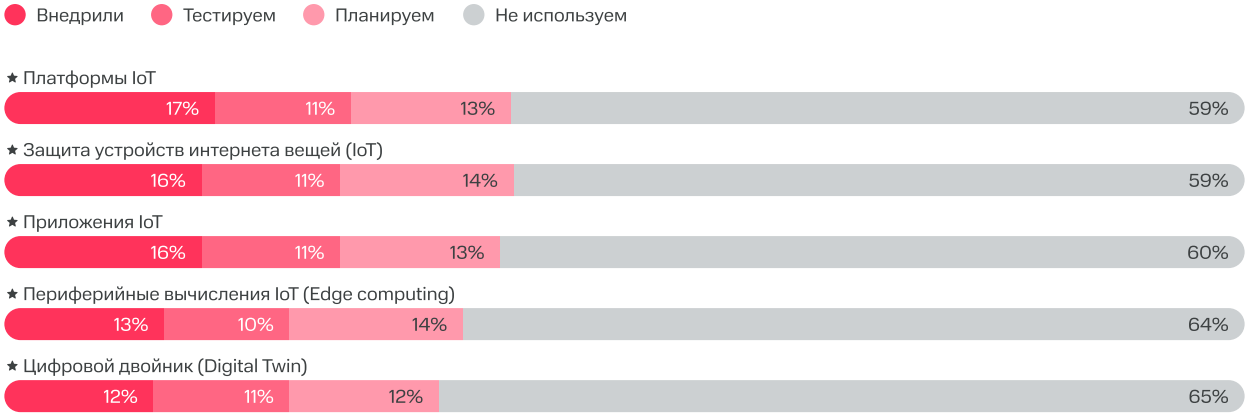
Аналитика



Зрелые компании стремятся развивать data-driven подход в своей стратегической и операционной деятельности. Сложности с внедрением данного подхода зачастую связаны с внутренними процессами в компаниях и методологией управления данными (Data Governance). Однако если организационные и процессные барьеры преодолены, то с технологической точки зрения реализация data-driven подхода требует наличия внедренных базовых IaaS и PaaS продуктов, в том числе рассмотренных ранее.

Data Warehouse является распространенным классом решений, с которого, как правило начинается построение развитой автоматизированной аналитики. Для решений в сфере real-time аналитики и создания DataLake характерно преобладание компаний, тестирующих и планирующих использовать данные продукты над реально внедряющими. Эти продуктовые субкатегории являются примерами интеграций в компаниях с развитым подходом к построению аналитики.

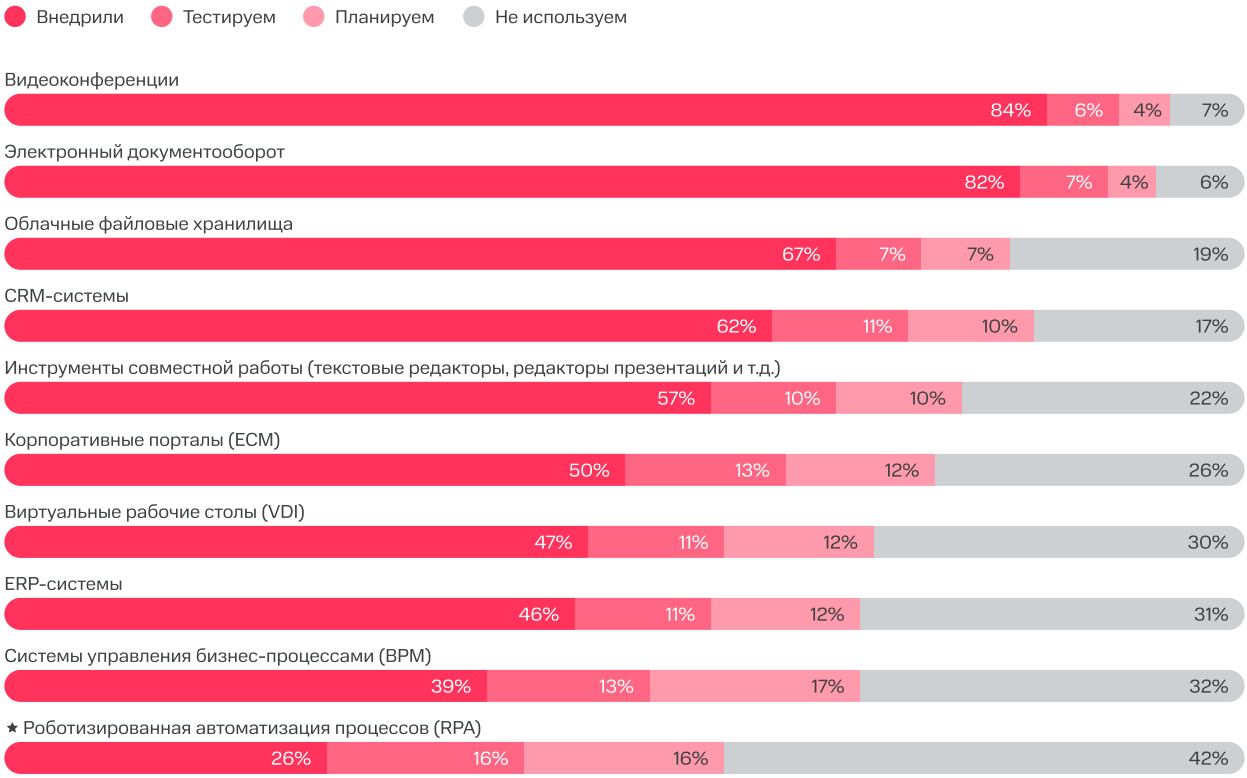
Интернет вещей (IoT)



Интернет вещей является сквозной технологией, включающей программные, аппаратные компоненты и компоненты связи. Реализация решений невозможна хотя бы без частичного использования облачной инфраструктуры. Согласно ответам респондентов широкое данные практики не имеют широкого распространения: практически по всем направлениям более половины компаний вообще не используют IoT-решения, а по цифровым двойникам решение не используют две трети компаний. Интернет вещей остается популярным преимущественно в индустриальных и логистических компаниях, в других отраслях его зрелость крайне низка.

Несмотря на то, что атаки на IoT системы – один из быстрорастущих векторов угроз, технологии защиты конечных устройств используют не более 70% компаний, внедривших платформы и приложения интернета вещей. Подобная тенденция может свидетельствовать об отсутствии в компаниях стратегий управления жизненным циклом устройств.

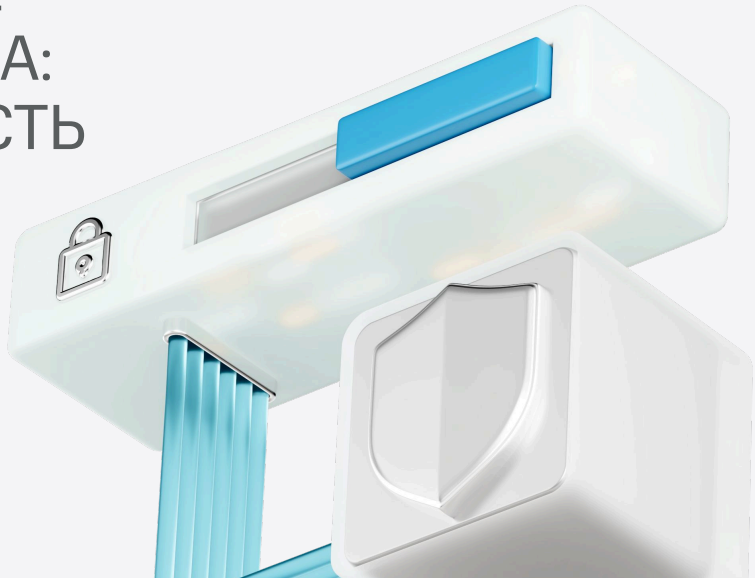
Приложения для бизнеса



Приложения для бизнеса, которые относятся к сегменту SaaS, широко распространены, пользуются повышенным спросом и во многом для компаний начали носить нативный характер. Так, подавляющее большинство респондентов в скоупе нашего исследования уже отметили внедрение видеоконференций, ЭДО, файловых хранилищ, CRM-систем и комплексных инструментов совместной работы, которые включают в себя, как правило широкий набор функционала. Отдельно обращаем внимание на 2 продуктовые субкатегории, которые имеют высокий наблюдаемый потенциал для дальнейшего роста: Системы управления бизнес-процессами (BPM) и Роботизированная автоматизация бизнес-процессов (RPA). Высокая статистика положительных ответов в рамках данных сегментов говорит об универсальности использования вне зависимости от индустрии и сегмента бизнеса.

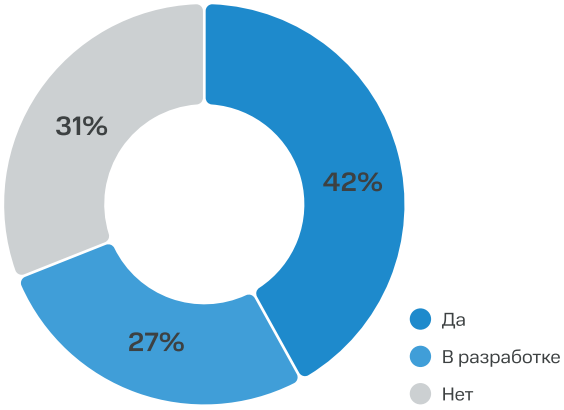
★ — высокий потенциал

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

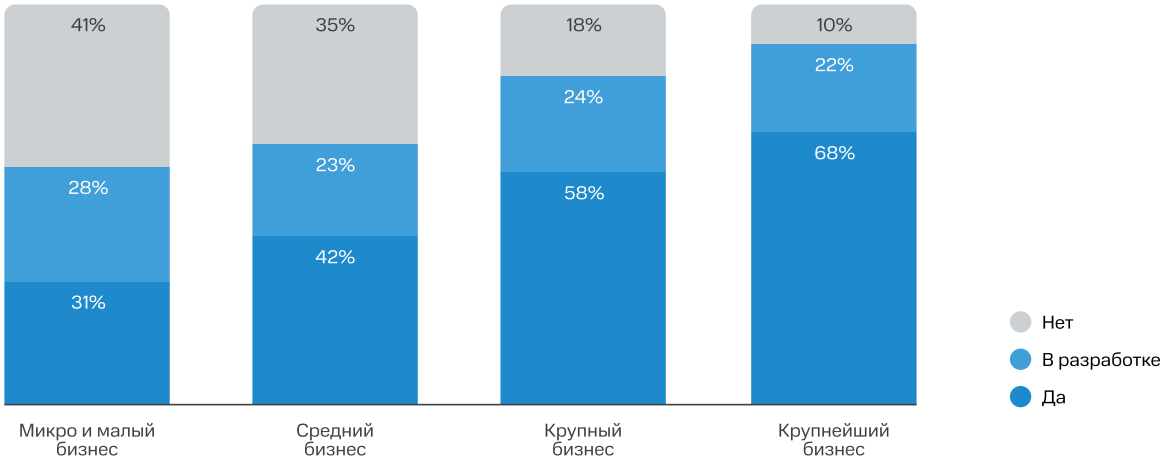


> Сегодня рынок облачных решений для кибербезопасности демонстрирует качественный сдвиг — защита информации перестает быть локальной задачей отдельных подразделений и становится фундаментом устойчивой цифровой экосистемы компаний. Все больше организаций подходят к вопросам КБ стратегически, выстраивая 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

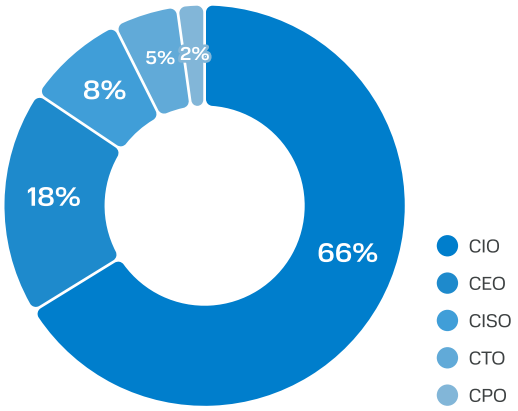
Зависимость уровня зрелости стратегий КБ от масштаба бизнеса прослеживается достаточно чётко. Среди крупнейших компаний (с выручкой >15 млрд руб.) стратегия КБ сформирована только в 68% случаев, тогда как у предприятий с выручкой <800 млн руб. этот показатель составляет лишь 31%. При этом, разработка 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



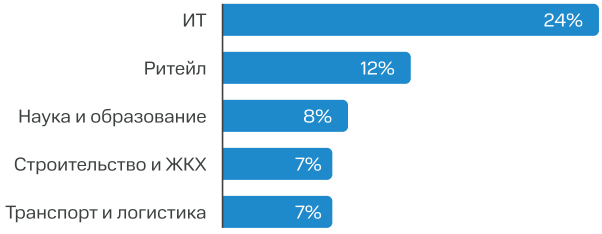
Для большинства компаний процесс внедрения средств информационной безопасности оказывается достаточно быстрым: у 73% он занимает не более полугода. Наиболее распространённый срок — от одного до трёх месяцев (31%), за ним следует период в 3–6 месяцев (24%).

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%.

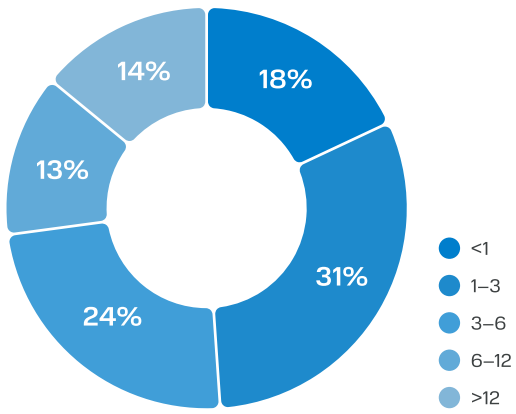
DDoS-атаки в 2024 году по индустриям



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.

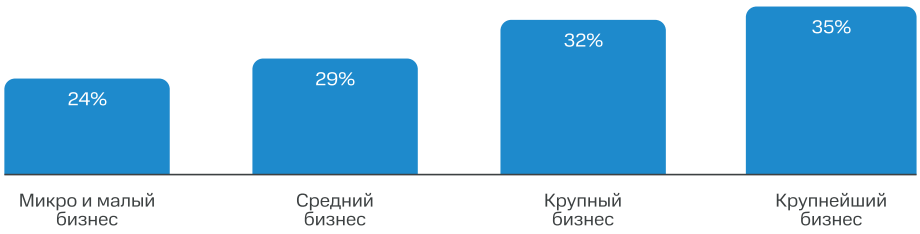
Длительность процесса внедрения средств КБ в месяцах



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.

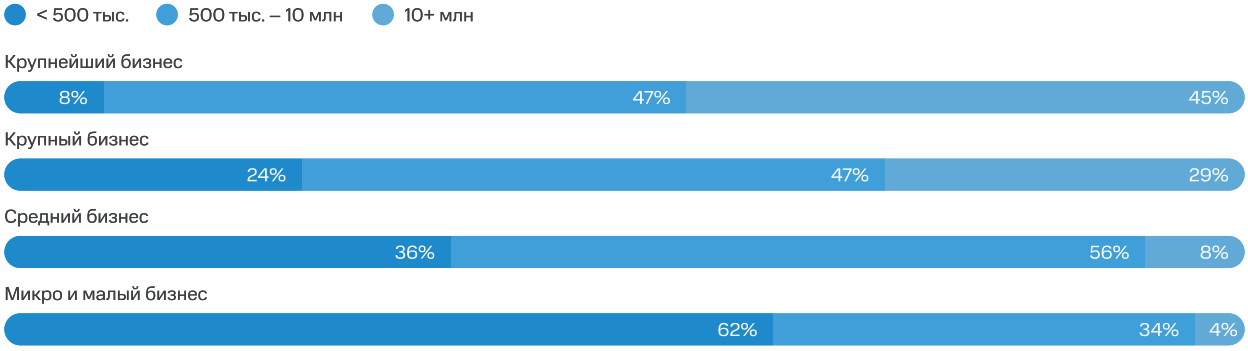
Отраслевой срез показывает, что лидерами по доле средств КБ в облаке являются ИТ, сегмент развлечений и медиа, а также наука и образование (средняя доля около 36%). Это связано с высокой цифровой зрелостью этих индустрий и значительным количеством облачных сервисов, уже встроенных в их операционные модели. 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.

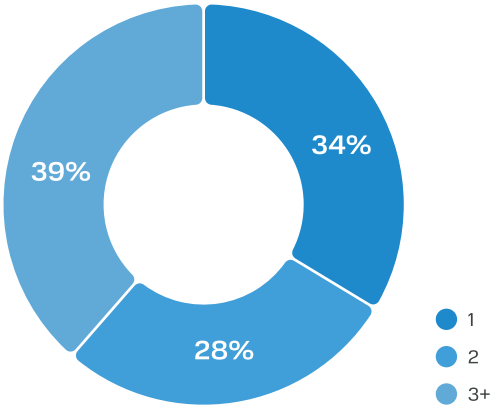
Более трети респондентов сотрудничают с одним вендором, что может свидетельствовать о стремлении к упрощению управления и интеграции решений, а также о доверии к одному проверенному партнеру, что может быть выгодно с точки зрения консолидации сервисов и получения более выгодных условий обслуживания.

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.

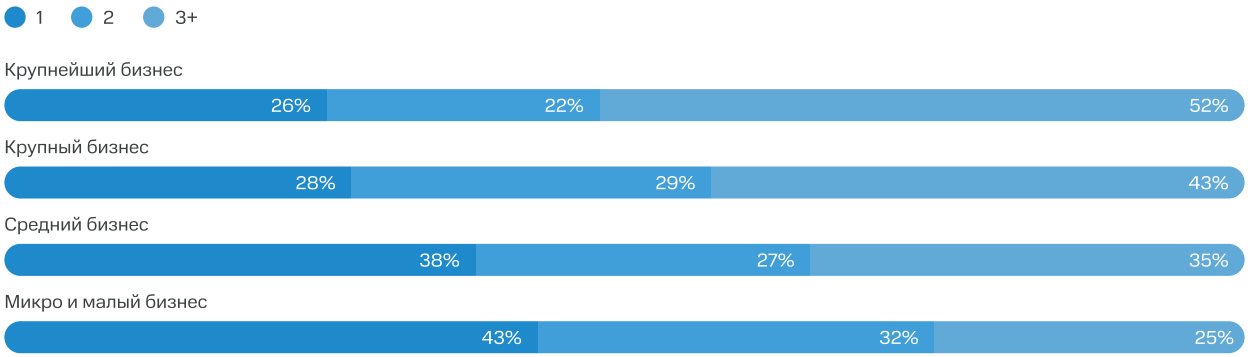
Стоит отметить, что крупный и крупнейший бизнес пользуется большим числом провайдеров, а число провайдеров увеличивается пропорционально росту размера компании.

Количество используемых вендоров КБ



Компании все чаще диверсифицируют риски в кибербезопасности, привлекая несколько вендоров

Количество используемых вендоров КБ по сегментам бизнеса



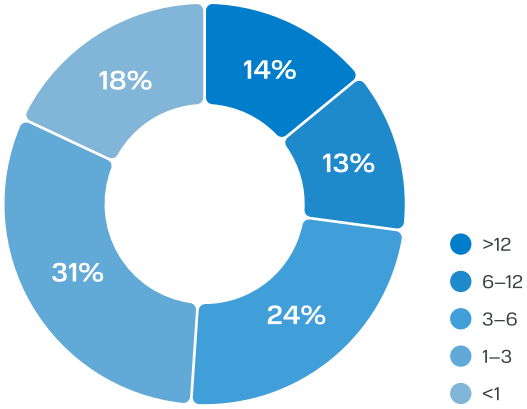
> Для российского корпоративного сектора такой паттерн выбора КБ-решений иллюстрирует доминирование подхода «compliance-driven security», где главной целью выступает соблюдение законодательства и стандартов. Вместе с тем подобная стратегия может сдерживать инвестиции в проактивные технологии киберустойчивости, 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

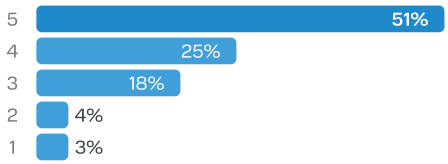
В месяцах



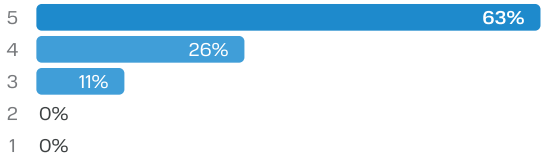
Ключевые факторы при принятии решения о внедрении средств КБ

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

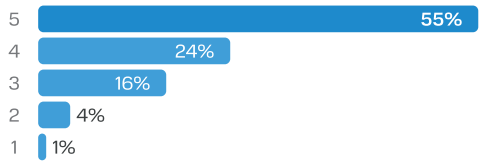
Соответствие требованиям законодательства в части информационной безопасности



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.

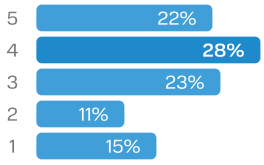
В то же время такие факторы, как отсутствие поддержки вендора в процессе внедрения, а также отсутствие у провайдеров полноценных программ технической поддержки (POC, Support и др.), оцениваются значительно мягче. Для большинства компаний эти сложности не стали критическими, что может свидетельствовать 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.

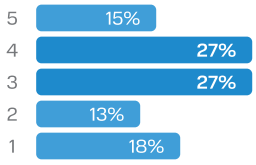
Сложности в процессе внедрения средств КБ [1/2]

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

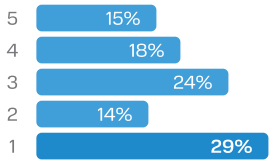
Отсутствие нужных компетенций среди сотрудников



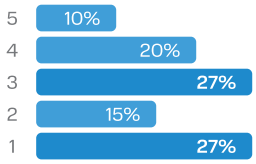
Сложность в оценке предполагаемых расходов на требуемую инфраструктуру



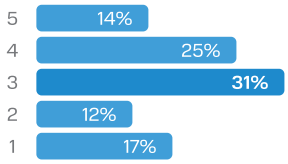
Сложность переноса большого объема данных



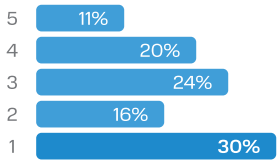
Отсутствие дорожной карты внедрения



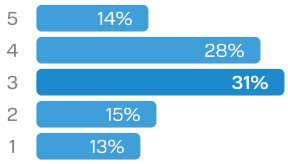
Дополнительные расходы на этапе внедрения систем информационной безопасности



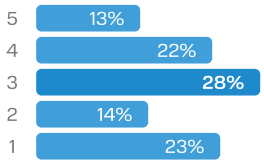
Отсутствие поддержки вендора в процессе внедрения



Повышение сложности управления инфраструктурой



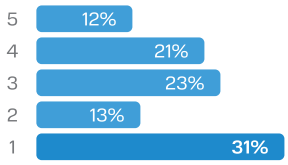
Необходимость временного дублирования инфраструктуры



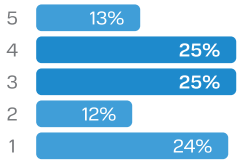
Сложности в процессе внедрения средств КБ [2/2]

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)



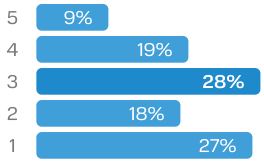
Дополнительные расходы, связанные с переобучением или наймом сотрудников для качественной работы со средствами информационной безопасности, наиболее часто упоминаются респондентами и распределены в сторону высоких оценок важности. Данная тенденция подчеркивает, что кадровый аспект продолжает оставаться 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.

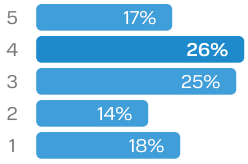
Дополнительные расходы в процессе внедрения средств КБ

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

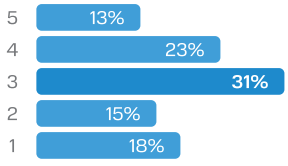
Развертывание тестового контура для проверки работоспособности рассматриваемого решения



Переобучение / найм сотрудников для качественной работы со средствами информационной безопасности



Обновление локальной инфраструктуры

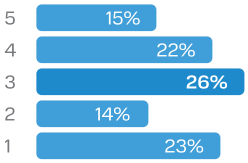


Респонденты наиболее критично воспринимают риски, связанные с утечкой данных — как персональных, так и данных коммерческой тайны. Эти две группы рисков суммарно набрали наибольшую долю оценок по наивысшему уровню критичности (5): утечки коммерческой тайны были определены как критичные 35% участников, 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.

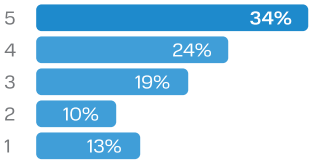
Критичность перечисленных ниже групп рисков при внедрении средств КБ

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

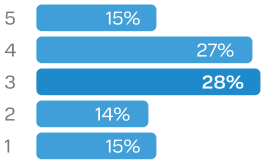
Сложность в закупке оборудования



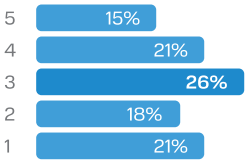
Утечки персональных данных



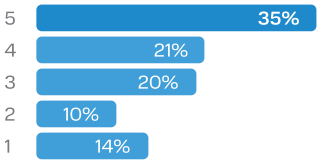
Нехватка технической экспертизы в части информационной безопасности



Неконтролируемый рост затрат на средства информационной безопасности



Утечка данных коммерческой тайны



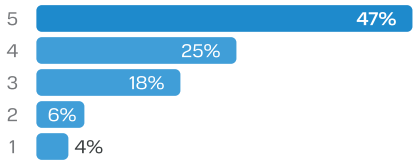
Среди факторов, влияющих на принятие решений о внедрении КБ, с небольшим опережением лидирует анализ угроз и рисков — его критически важным назвали 51% респондентов. Такое распределение ответов подчеркивает практическую ориентацию компаний на понимание уязвимостей и потенциальных сценариев атак как основы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

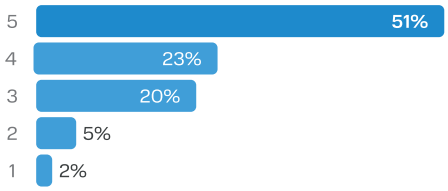
Наиболее важные факторы при принятии решений о внедрении КБ

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

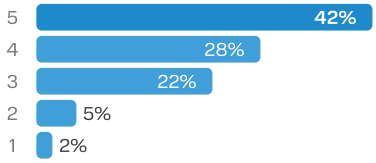
Соответствие нормативным требованиям



Анализ угроз и рисков



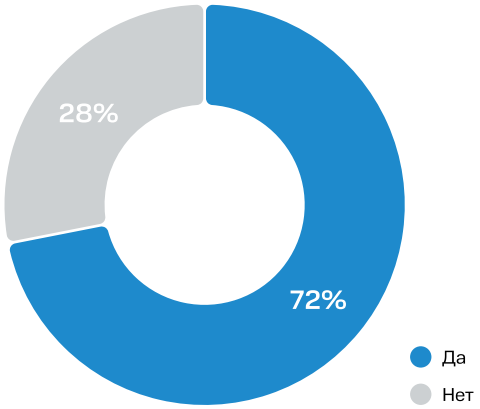
Оптимизация затрат на выявление рисков и угроз



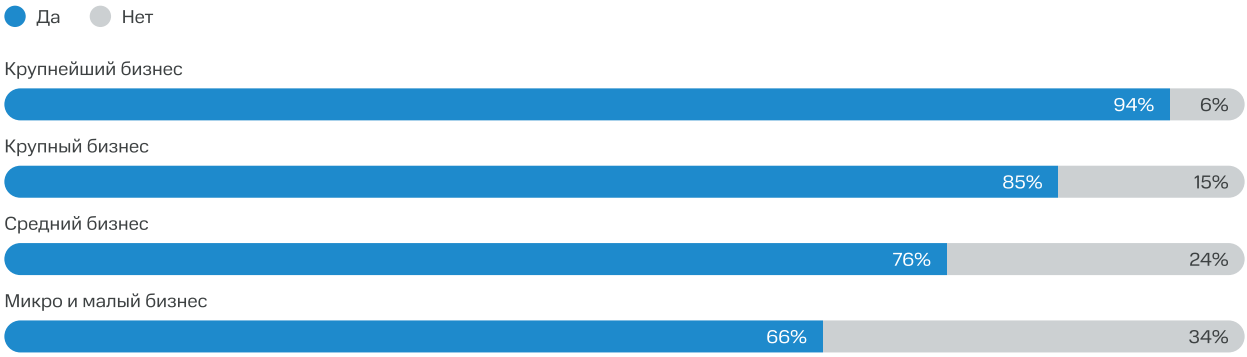
Только крупный и крупнейший бизнес имеет достаточное финансирование для найма необходимых специалистов

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

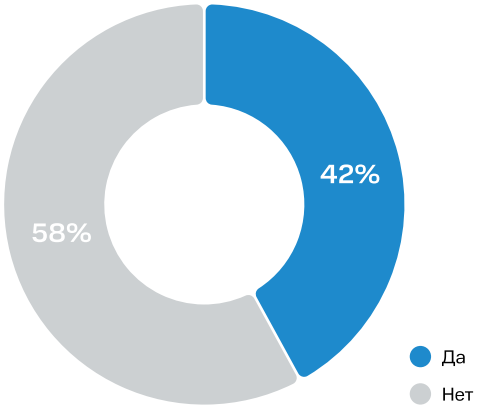


Наибольшая концентрация экспертизы по отраслям наблюдается в ИТ (88%), добыче полезных ископаемых (82%), финансах и страховании (81%), а также в здравоохранении и профессиональных услугах. Для этих индустрий характерны специфические регуляторные требования, высокие риски утечек конфиденциальных данных, 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.

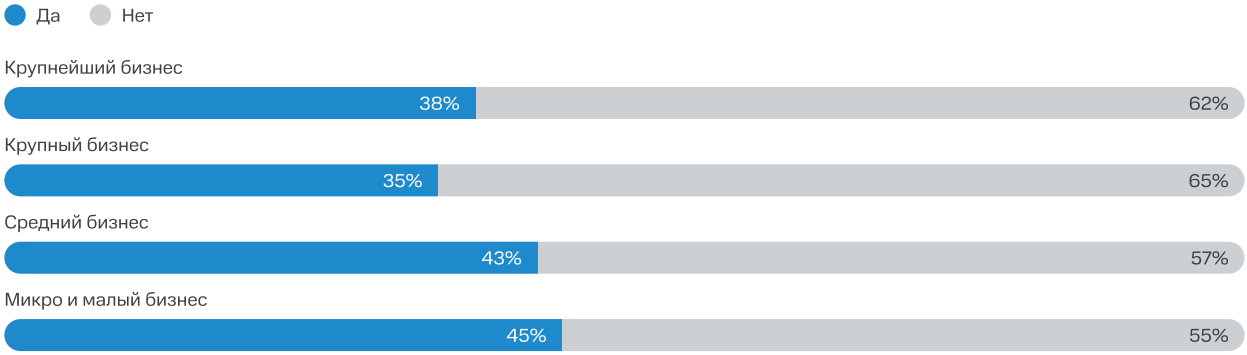
Несмотря на общее наличие опыта работы со средствами КБ, проблемы с наймом квалифицированных сотрудников все еще являются существенным фактором для отрасли. 43% респондентов указали на наличие проблем в найме экспертов в сфере КБ, что является значительным показателем. При этом наличие проблем в найме 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



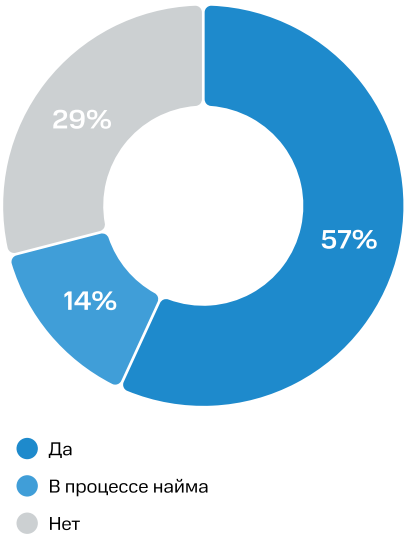
Наличие проблем в найме экспертов в сфере КБ по сегментам бизнеса



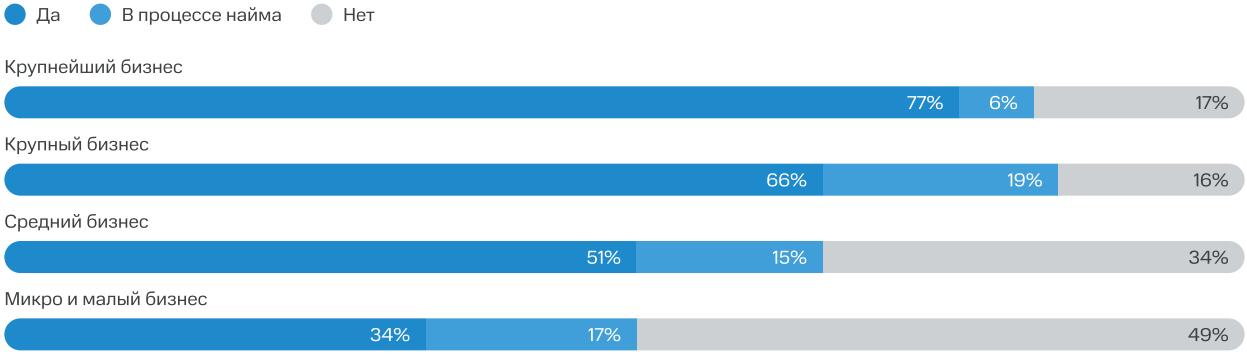
При этом, наличие полноценной собственной команды также становится все более распространенным явлением. 57% опрошенных компаний уже имеют собственную команду по кибербезопасности, в то время как 14% находятся в процессе ее формирования. Это указывает на растущее признание значимости кибербезопасности 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.

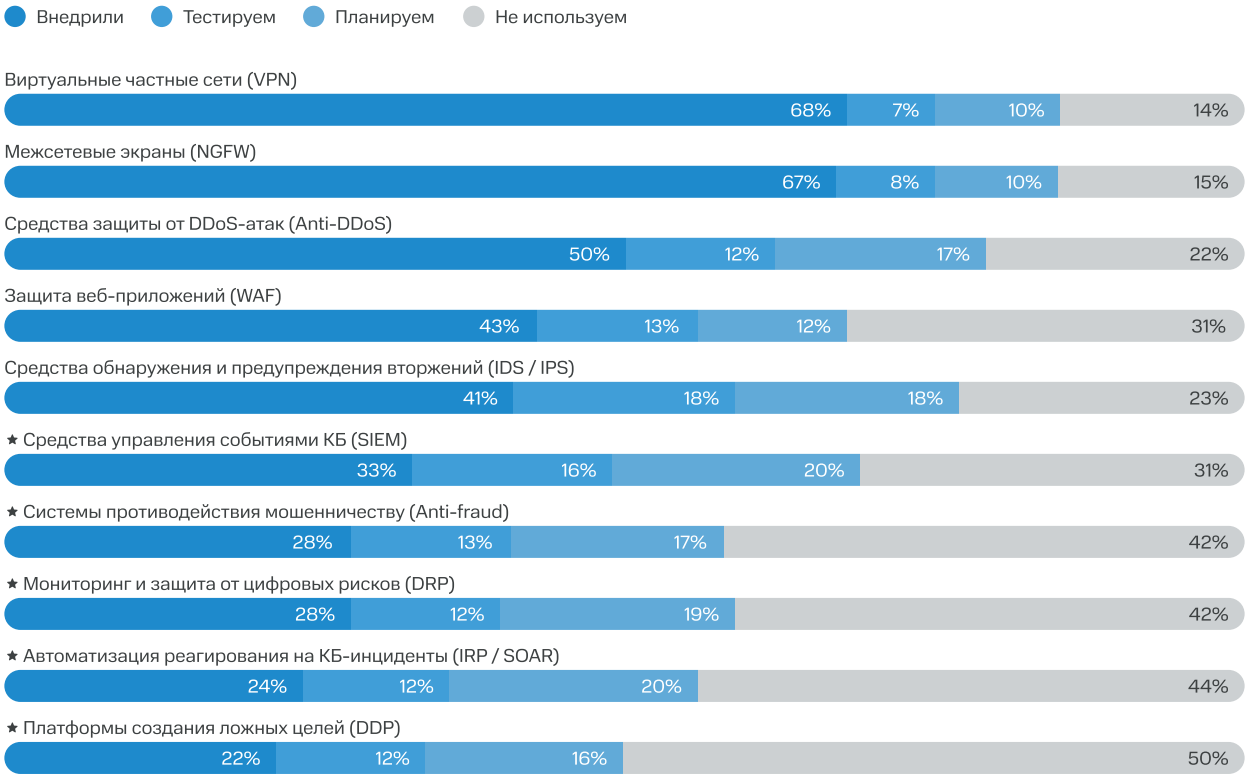
Для оценки среди полученных субкатегорий тех продуктов, которые имеют повышенный потенциал роста, введен подход, получивший название «Формула потенциала роста субкатегорий». Данная формула представляет собой сопоставление: с одной стороны параметра «внедрили», с другой стороны суммы параметров «тестируем» 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.

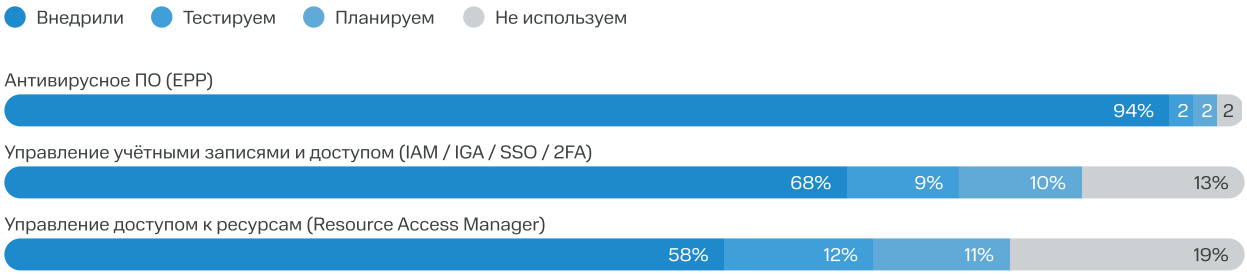
Базовой практикой в холдинговых компаниях является наличие собственной команды по КБ (отметили 76% опрошенных представителей крупнейшего бизнеса), однако найм экспертов, в том числе по защите базовой инфраструктуры предприятия, все еще остается значимой проблемой (отметили 43% опрошенных). Что может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

★ — высокий потенциал

Средства защиты данных

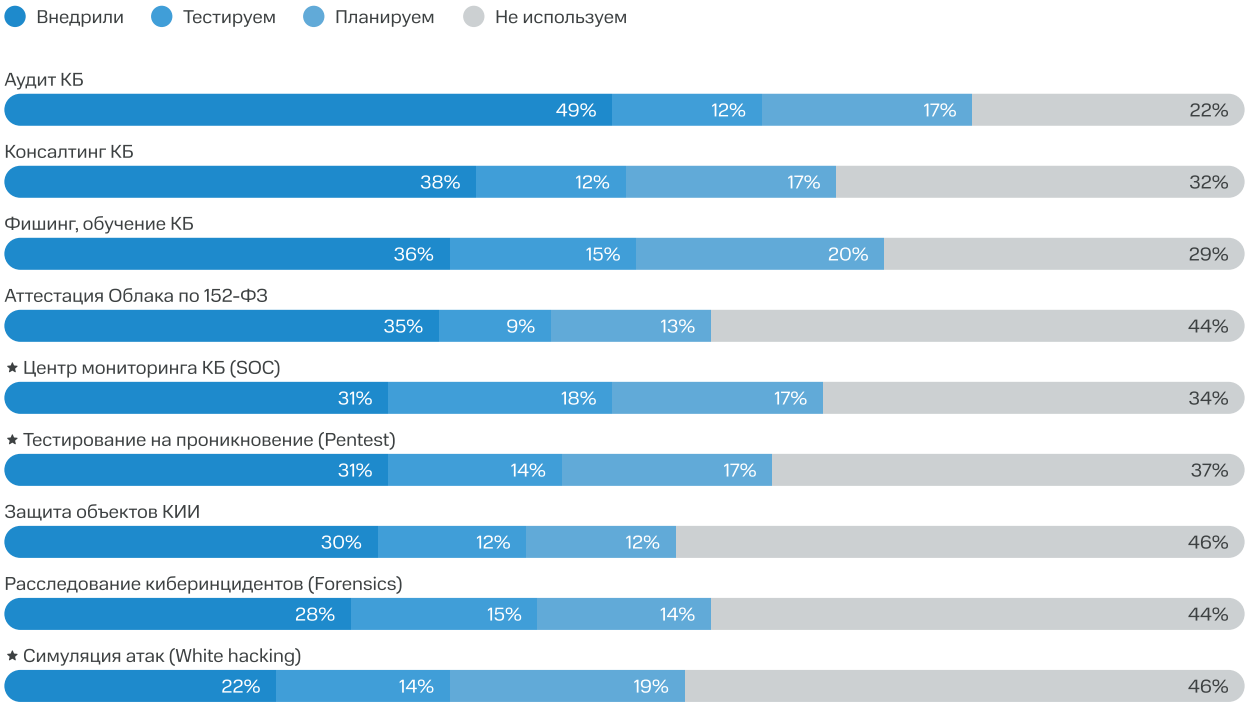
Защита данных от внешних и внутренних угроз является фундаментальным атрибутом деятельности любой корпорации. Крупнейшие экосистемные российские организации, а также органы государственной власти регулярно подвергаются соответствующим рискам, что несет не только угрозу для внутренних операционных процессов, 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

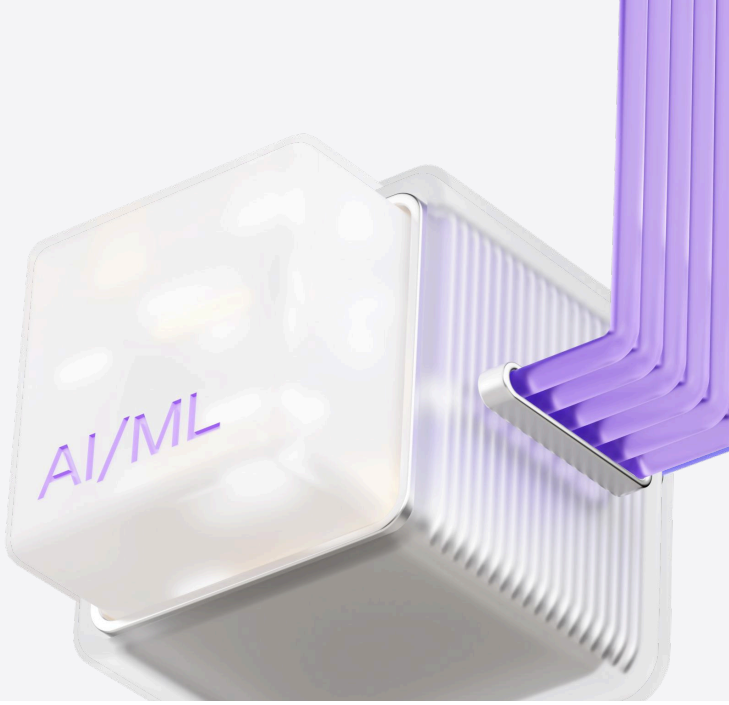


В объеме рынка кибербезопасности в России вертикали Software и IT-Services совокупно занимают порядка 80%. Вертикаль IT-Services растет с темпом годового прироста более 30%. Эти значения коррелируют с данными ожиданий объемов потребления соответствующих решений КБ в выборке данного исследования. Услуги 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

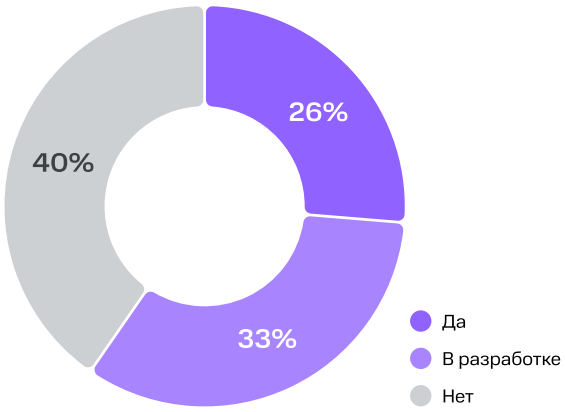
ТЕХНОЛОГИЧЕСКИЕ СТРАТЕГИИ БИЗНЕСА: ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ



Наличие стратегии по внедрению ИИ позволяет компаниям системно подходить к развитию данного направления, интегрируя ИИ в общую архитектуру бизнеса и обеспечивая согласованное распределение ресурсов.

Согласно полученным данным, стратегия по ИИ сформирована только у 26% респондентов, что меньше доли внедрения стратегий по облачным решениям (44%) и кибербезопасности (42%). При этом, планы по разработке стратегии ИИ выделяются у большего числа компаний, чем планы разработки иных стратегий. Разница обусловлена динамичностью развития технологий и новизной многих решений ИИ для значительного перечня компаний.

Наличие стратегии по внедрению ИИ



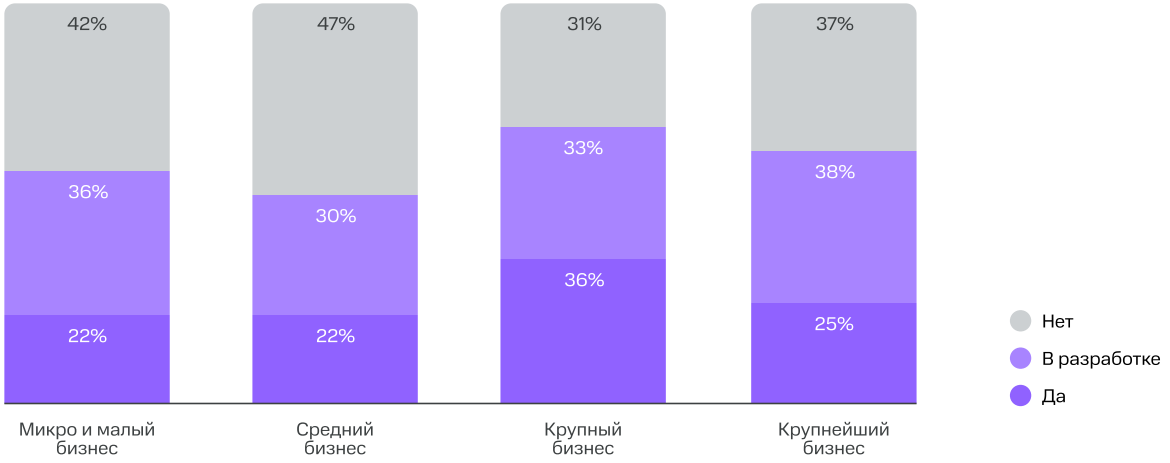
Лидерами по доле разработанной стратегии по ИИ являются крупные игроки, обладающие большими ресурсами и возможностями для инвестиций в развитие собственных ИИ-продуктов. При этом, доля крупнейших игроков с разработанной стратегией меньше, что может быть обусловлено продолжительностью цикла стратегического планирования. Среди индустриальных лидеров по наличию стратегии можно выделить ИТ-сектор, транспорт и логистику, а также научные организации, для которых использование ИИ является прикладной необходимостью в рамках процессов обработки больших объемов данных.

Готовые стратегии в сфере ИИ не распространены широко, однако активно разрабатываются игроками всех сегментов

> Мы видим сдвиг парадигмы: от универсального генеративного интеллекта, который умеет всё и ничего по-настоящему, к специализированным решениям, дающим измеримый результат. Наступает эпоха прикладных моделей, созданных под конкретные задачи и отрасли. Компании всё яснее понимают: простая интеграция занимает слишком много времени и ресурсов, а экономический эффект не сходится. Отсюда новый тренд — платформы для создания и управления ИИ-помощниками. Формируется класс решений, который позволяет бизнесу не просто использовать модели, а выстроить конвейер по созданию собственных ИИ-продуктов. Сегодня компании переходят к следующему этапу — собственной ИИ-трансформации, к бизнесу, построенному на искусственном интеллекте.

Денис Филиппов
Генеральный директор
ООО «МВС ИИ»

Наличие стратегии по внедрению ИИ по сегментам бизнеса



В 67% компаний основная роль в процессе принятия решений относительно ИИ принадлежит CIO (руководителю ИТ), что логично объясняется их экспертизой в области информационных технологий, а также глубоким пониманием инфраструктурных и архитектурных аспектов внедрения ИИ-решений. На втором месте по вовлеченности находится CEO (генеральный директор) с показателем 23%, что отражает стратегическую важность тематики ИИ на уровне высшего управленческого звена.

Остальные роли, включая CISO, CTO и CPO, совокупно составляют менее 11%, что демонстрирует относительно ограниченное участие специализированных руководителей по безопасности, техническому развитию и продуктам в непосредственном процессе утверждения инициатив по ИИ. Эти данные подчеркивают, что внедрение ИИ в большинстве случаев остается в зоне ответственности ИТ-дирекции, при поддержке первых лиц компаний в части стратегического одобрения. Данная структура ЛПР может служить ориентиром для построения клиентских стратегий и таргетированных коммуникаций при продвижении ИИ-решений на корпоративном рынке.

У большинства респондентов (55%) процесс внедрения занимает от одного до шести месяцев. Наиболее часто встречающийся диапазон составляет от 1 до 3 месяцев (29%), что указывает на стремление компаний минимизировать сроки внедрения ИИ-решений и как можно быстрее получить эффект от их использования.

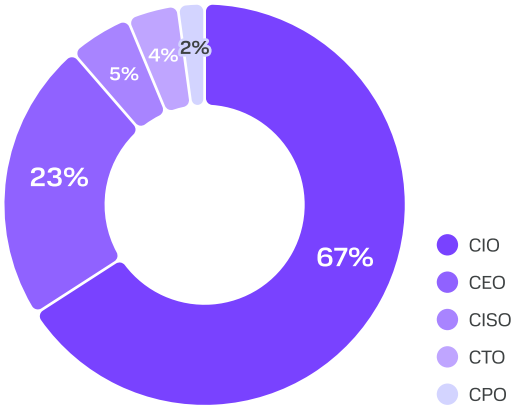
При этом у значительной доли организаций процесс растягивается на более длительные сроки. Эти показатели могут отражать либо высокую сложность внедряемых решений, либо организационные барьеры и необходимость согласования на нескольких уровнях управления.

Таким образом, полученная аналитика демонстрирует, что большинство компаний ориентированы на относительно оперативное внедрение средств ИИ, однако существенная часть проектов по-прежнему характеризуется длительными циклами более полугода, что важно учитывать при планировании ресурсов и построении проектных дорожных карт для подобных решений.

Наиболее популярными типами развертывания ИИ среди опрошенных компаний стали частное и публичное облако, которые используют по 23% респондентов. Локальные установки ИИ-нагрузок задействуют 20% компаний, тогда как гибридные сценарии пока встречаются реже — их выбирают 13%.

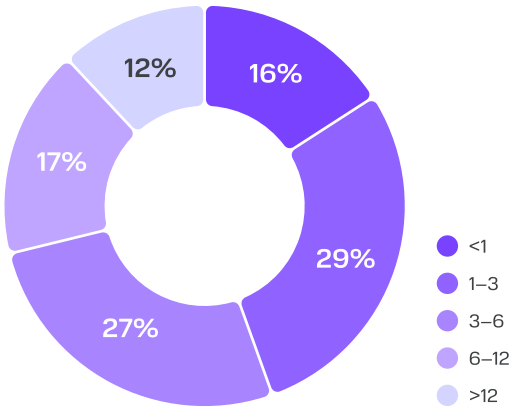
Такой выбор отражает стремление бизнеса использовать облачные модели для обеспечения гибкости, масштабируемости и снижения капитальных затрат, сохраняя при этом контроль над критичными процессами и данными в частных инфраструктурах. Публичные облака позволяют быстрее адаптироваться и масштабировать операции, что делает их привлекательными для задач с переменной или быстрорастущей нагрузкой. Эти данные подтверждают общий тренд на активное использование облачных технологий для повышения эффективности и безопасности ИИ-систем.

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



Длительность процесса внедрения средств ИИ

В месяцах

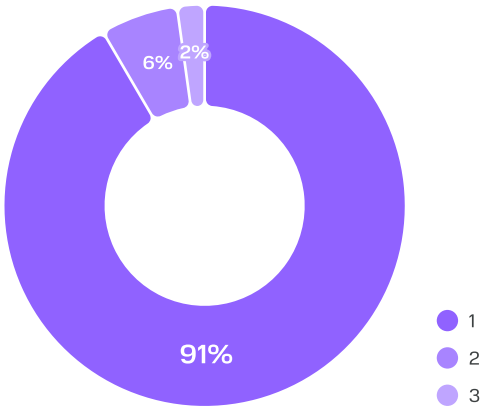


Количество используемых вендоров ИИ по сегментам бизнеса

Большинство опрошенных компаний (91%) сотрудничают только с одним вендором ИИ. Такая модель позволяет сфокусироваться на адаптации выбранных решений под специфические задачи бизнеса, а также упрощает управление инфраструктурой и снижает риски, связанные с совместимостью разных платформ. Доля компаний, которые сотрудничают сразу с несколькими вендорами (2 и более), остаётся сравнительно низкой и суммарно составляет около 9%, что указывает на пока еще ограниченное распространение мультивендорных стратегий на рынке ИИ.

Отчетливо прослеживается тенденция: по мере снижения размера бизнеса доля компаний, которые совсем не используют ИИ, увеличивается. Для крупнейших компаний (>15 млрд руб.) показатель отказа от ИИ всего 15%, тогда как в сегменте с выручкой 2–15 млрд руб. уже 21%, а среди компаний с выручкой менее 800 млн руб. — около 11%, но почти все они ограничиваются единственным поставщиком. Использование двух и более вендоров ИИ характерно для наиболее зрелых сегментов бизнеса: крупных и крупнейших компаний с выручкой свыше 2 млрд руб.

Количество используемых вендоров ИИ



Годовой объем затрат на ИИ по индустриям

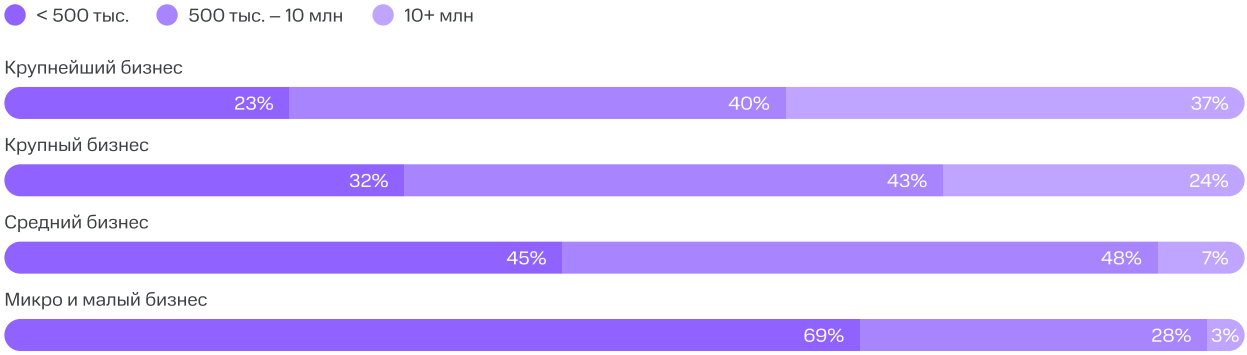
	< 500 тыс.	500 тыс. – 10 млн	10+ млн
ИТ	42%	30%	28%
Финансы и страхование	46%	34%	20%
Добыча и переработка полезных ископаемых	54%	27%	20%
Наука и образование	45%	41%	14%
Развлечения и медиа	33%	58%	8%
Ритейл	56%	36%	8%
Провессиональные услуги	82%	13%	6%
HoReCa	60%	35%	5%
Промышленность	67%	28%	5%
Транспорт и логистика	55%	40%	5%
Здравоохранение	54%	42%	4%
Недвижимость и строительство	66%	33%	1%

Для ИИ на текущем этапе характерен моновендорный подход: компании только осваивают рынок

Затраты на ИИ пропорциональны размеру бизнеса. Если доля средних затрат примерно равна для всех сегментов, кроме микро и малого бизнеса, то доля затрат более 10 млн резко возрастает для крупного и крупнейшего бизнеса. Данное разделение обусловлено наличием собственной команды разработки и созданием кастомных решений у данного сегмента бизнеса. Именно лидеры рынка формируют основную часть спроса на масштабные ИИ-инициативы и могут позволить себе развивать более капиталоемкие проекты.

Годовой объем затрат на ИИ по сегментам бизнеса

Шкалы означают сегмент бизнеса согласно выручке, цветом обозначен объем затрат



ИИ — дело крупного бизнеса, именно он инвестирует в разработку и адаптацию решений

Наибольший объем инвестиций в ИИ отмечается в отраслях ИТ, финансы и страхование, добыча и переработка, ритейл, транспорт и логистика, а также наука и образование. Эти индустрии демонстрируют более распределённую структуру затрат с заметной долей компаний, выходящих за пределы минимальных бюджетов. Особенно выделяется ИТ-сектор, где 29% компаний тратят на ИИ свыше 10 млн руб. в год, что значительно выше аналогичных показателей других отраслей. Это объясняется высокой зрелостью цифровых процессов и прямой зависимостью бизнеса от технологий.

Для ритейла и транспорта характерны более умеренные бюджеты, сконцентрированные в диапа-зоне до 20 млн руб. в год, что связано с активным использованием ИИ для прогнозирования, управления цепочками поставок и персонализации сервисов. Сектор науки и образования также демонстрирует склонность к инвестициям в среднем диапазоне, что отражает задачи обработки больших массивов данных и развития аналитических платформ.

Для большинства компаний ключевыми факторами при принятии решения о внедрении ИИ выступают повышение эффективности бизнеса (49% отметили этот фактор как максимально важный), автоматизация бизнес-процессов (46%) и быстрое принятие решений (39%). Эти три направления формируют основу бизнес-мотивации для инвестиций в ИИ, отражая стремление компаний сократить издержки, повысить операционную скорость и гибкость.

Ключевые факторы при принятии решения о внедрении ИИ

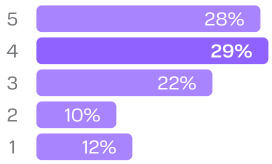
Оценка респондента от 1 до 5 баллов, где 1 балл — минимальное влияние фактора, 5 — максимальное

> Компании ожидают существенного сокращения издержек от внедрения ИИ, однако опасаются рисков, связанных с утечками данных

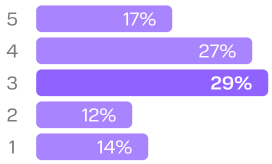
Сложности в процессе внедрения ИИ [1/2]

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

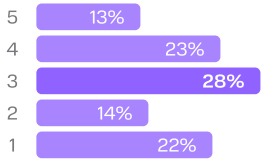
Отсутствие нужных компетенций среди сотрудников



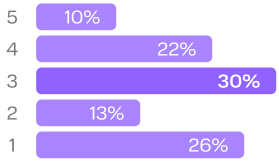
Сложность в оценке предполагаемых расходов на требуемую инфраструктуру



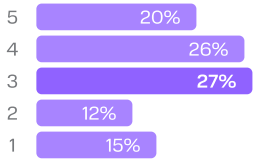
Необходимость временного дублирования инфраструктуры



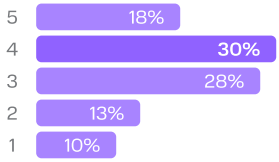
Отсутствие поддержки вендора в процессе внедрения



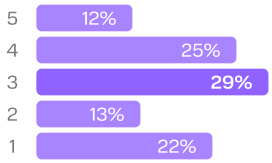
Дополнительные расходы на этапе внедрения искусственного интеллекта



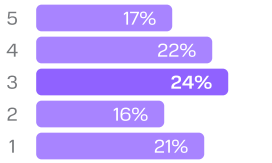
Поиск решений / инструментов на основе ИИ на рынке или их разработка



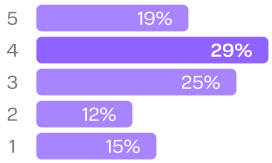
Отсутствие дорожной карты внедрения



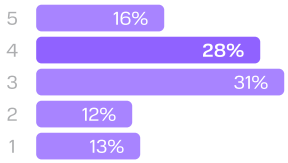
Сложность переноса большого объема данных



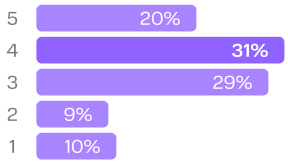
Большие финансовые затраты



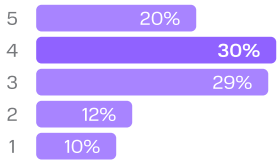
Масштабирование внутри организации



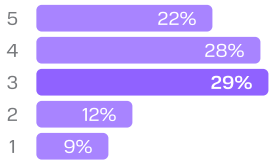
Создание необходимой платформы данных для работы с ИИ



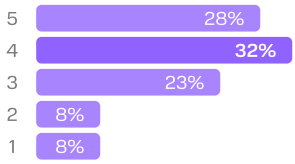
Изменение привычных бизнес-процессов для эффективного использования ИИ



Информирование и обучение сотрудников по вопросам ИИ



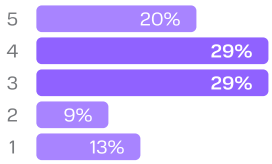
Достижение необходимого уровня качества моделей на основе ИИ



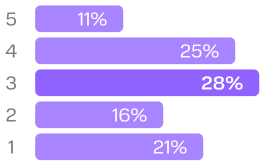
Сложности в процессе внедрения ИИ [2/2]

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

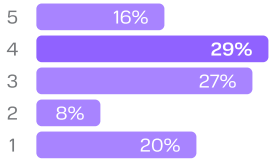
Формирование единого видения ключевых областей использования ИИ в компании



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



Невозможность интеграции средств искусственного интеллекта в используемые локальные решения (устаревшее ПО / оборудование)



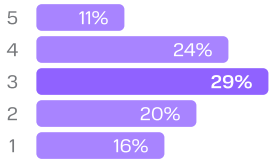
Сложности, сопровождающие процесс внедрения ИИ, в целом оцениваются респондентами на среднем уровне значимости, что подтверждает готовность большинства компаний двигаться в сторону интеграции ИИ, несмотря на существующие барьеры. Компании в основном готовы закладывать ресурсы на преодоление организационных и технологических барьеров ради получения долгосрочных выгод от использования ИИ, однако вопрос подготовки персонала остаётся ключевым фактором, требующим первоочередного внимания при планировании таких проектов.

Дополнительные расходы, возникающие в процессе внедрения ИИ, в целом оцениваются респондентами на среднем уровне значимости, что свидетельствует о готовности большинства компаний учитывать эти затраты в своих инвестиционных планах. Наиболее часто упоминаемым фактором выступает переобучение или найм сотрудников для обеспечения качественной работы с ИИ: 29% оценили этот пункт как максимально важный (4 из 5), а ещё 19% присвоили наивысший балл. Ключевым вызовом для компаний остаются кадровые вопросы, требующие инвестиций в компетенции для успешной эксплуатации ИИ-решений. Это перекликается с ранее зафиксированными барьерами — недостатком технической экспертизы и рисками, связанными с управлением данными, включая угрозу утечки информации и персональных данных.

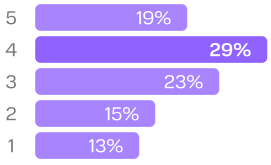
Дополнительные расходы в процессе внедрения ИИ

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

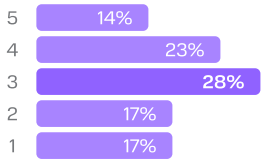
Развертывание тестового контура для проверки работоспособности рассматриваемого решения



Переобучение / найм сотрудников для качественной работы с искусственным интеллектом



Обновление локальной инфраструктуры



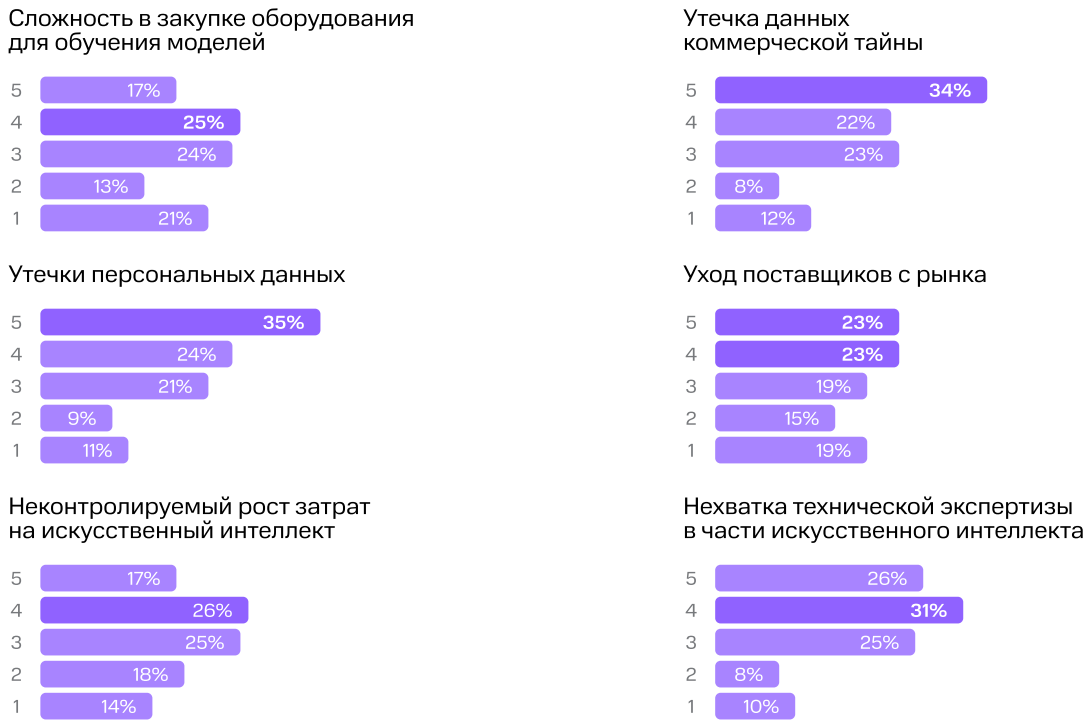
Среди критичных рисков, связанных с внедрением ИИ, компании в первую очередь выделяют угрозу утечек данных — как персональных (35% оценок наивысшей критичности), так и коммерческой тайны (34%). Это подчеркивает высокую чувствительность бизнеса к вопросам безопасности и конфиденциальности при реализации ИИ-проектов.

Значимым барьером остается также нехватка технической экспертизы в части искусственного интеллекта: 26% респондентов оценивают её как наиболее критичный риск, а ещё 31% присвоили уровень важности 4 из 5. Отдельно фиксируется обеспокоенность неконтролируемым ростом затрат на ИИ, что подтверждает необходимость выстраивания практик бюджетного планирования и FinOps для таких проектов.

Менее выраженными, но всё же актуальными остаются риски ухода поставщиков с рынка, сложности в закупке оборудования для обучения моделей и общие инфраструктурные ограничения. Эти данные свидетельствуют о том, что для компаний вопросы защиты данных, наличие компетенций и прозрачность затрат по-прежнему являются определяющими при принятии решений о масштабном развитии ИИ-инициатив, несмотря на декларируемые ранее выгоды в части оптимизации рутинных задач и повышения эффективности бизнес-процессов.

Критичность перечисленных ниже групп рисков при внедрении ИИ

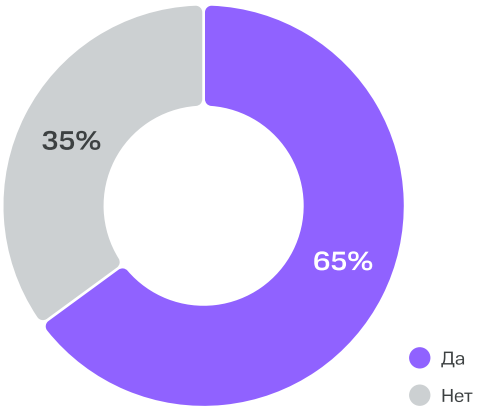
Оценка респондента от 1 до 5 баллов, где 1 балл — минимальное влияние фактора, 5 — максимальное



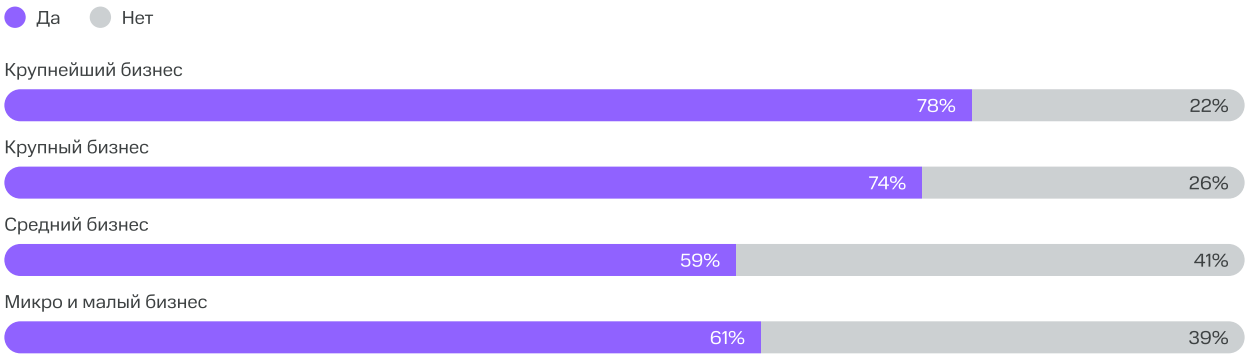
Опыт и экспертиза в работе с ИИ зафиксированы у 65% опрошенных компаний, что подчеркивает общее продвижение рынка в направлении освоения технологий искусственного интеллекта. При этом данные показывают прямую зависимость уровня накопленных компетенций от масштаба бизнеса: крупные компании чаще обладают специализированными командами и экспертизой в ИИ, что связано с их возможностями инвестировать в развитие таких компетенций и поддерживать собственные R&D-центры.

В отраслевом разрезе лидируют наука, ИТ, а также сегмент развлечений и медиа — в этих индустриях доля компаний, имеющих специалистов по ИИ, превышает 80%. Это во многом объясняется спецификой данных отраслей, где работа с большими данными, алгоритмами прогнозирования и автоматизацией процессов уже стала частью операционной модели. Такие результаты подтверждают высокую значимость накопления внутренней экспертизы для успешного внедрения и масштабирования ИИ-решений.

Наличие опыта и экспертизы работы с ИИ



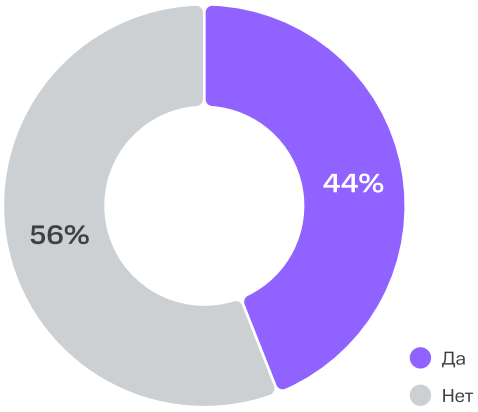
Наличие опыта и экспертизы работы с ИИ по сегментам бизнеса



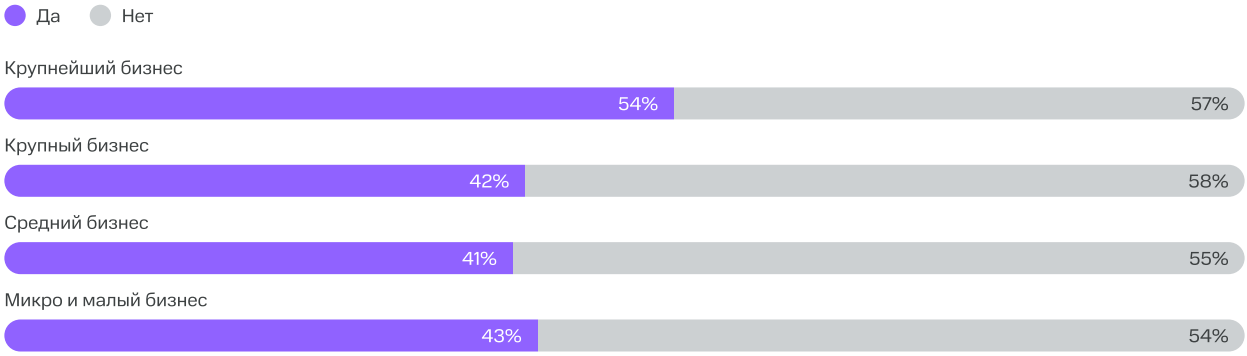
Несмотря на то, что существенная часть компаний уже обладает опытом и экспертизой в области ИИ, проблемы с наймом квалифицированных специалистов сохраняются для значительной части рынка: 43% респондентов отметили сложности в привлечении экспертов по ИИ. Этот показатель примерно одинаков для всех сегментов бизнеса по размеру выручки, что указывает на системный характер дефицита компетенций в данной области.

Наиболее остро проблема нехватки кадров проявляется в таких индустриях, как тяжелая промышленность (69%), строительство и ЖКХ (61%), промышленность (по 60%), а также наука и образование (59%). Для этих отраслей характерны специфические требования к ИИ-решениям, высокие регуляторные барьеры и необходимость глубокого понимания отраслевых процессов, что усложняет поиск и интеграцию новых специалистов.

Наличие проблем в найме экспертов в сфере ИИ



Наличие проблем в найме экспертов в сфере ИИ по сегментам бизнеса

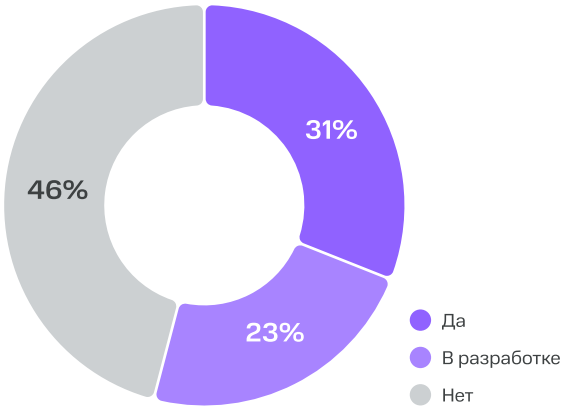


Собственная команда разработчиков и специалистов по данным (Data Scientists) имеется примерно у трети респондентов. Наличие таких команд прямо коррелирует с уровнем зрелости подходов к искусственному интеллекту в компании и чаще всего встречается у организаций, где уже сформирована стратегия по ИИ и которые находятся в фазе активного или продолжительного внедрения подобных решений.

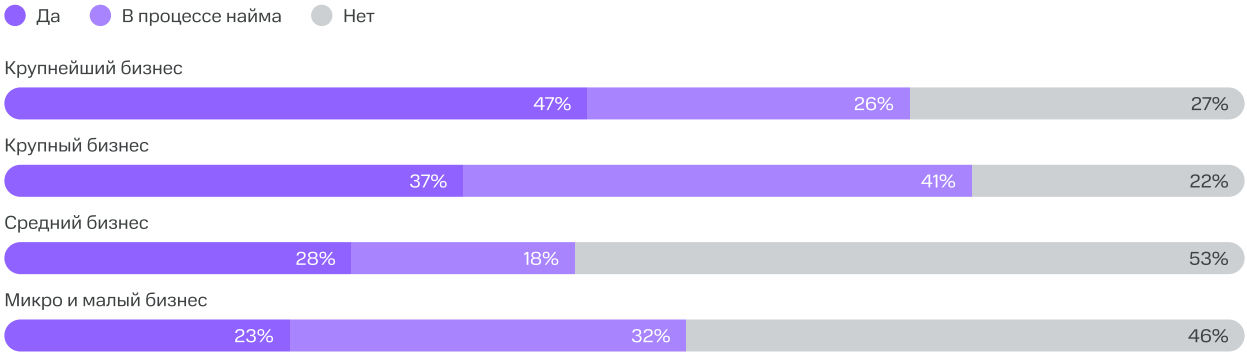
Анализ в зависимости от длительности работы с ИИ демонстрирует отчетливую тенденцию: чем дольше компания занимается внедрением ИИ, тем выше вероятность наличия собственной команды. Так, среди компаний, которые используют ИИ менее одного года, команды разработчиков есть только у 29%, тогда как среди компаний с опытом внедрения более 12 месяцев эта доля возрастает до 44%. Это подтверждает, что внутренние компетенции по ИИ в большинстве случаев формируются по мере накопления практического опыта работы с данными технологиями и усложнения проектов.

Интересно также, что большая часть компаний, находящихся в процессе создания таких команд (через найм или переобучение сотрудников), реализует проекты по ИИ в течение 3–6 месяцев. Это может свидетельствовать о том, что на этом этапе компании начинают сталкиваться с необходимостью перехода от пилотных инициатив и использования готовых решений к более сложным сценариям, требующим привлечения собственных специалистов для настройки и доработки моделей под специфику бизнеса.

Собственная команда разработки и Data Scientists



Собственная команда разработки и Data Scientists по сегментам бизнеса



Преодоление нехватки внутренних компетенций осуществляется, в том числе, с помощью использования профессиональных сервисов. Наиболее популярными сервисами для развития искусственного интеллекта среди респондентов являются обучение и техническая поддержка, используемые более чем 30% компаний. В то время как консалтинг по ИИ менее распространен, его используют только 17% респондентов. Это может свидетельствовать о предпочтении компаний самостоятельного внедрения ИИ, однако использование консалтинговых услуг может помочь оптимизировать и ускорить процесс внедрения ИИ, предоставляя ценные рекомендации и лучшие практики.

Перечень профессиональных сервисов, используемых для развития ИИ

33%
Обучение

31%
Техническая поддержка

22%
Тренинг моделей

18%
Интеграция

18%
Заказная разработка ИИ приложений

17%
Консалтинг (стратегия)

12%
Инференс моделей

ПРОДУКТЫ MTC WEB SERVICES

ЗАКРОЕМ ПОТРЕБНОСТЬ В СЕРВИСАХ И ЭКСПЕРТИЗЕ ПО ИИ

Проработанные решения на базе AI с подтверждёнными результатами

Рост прибыли на 20%

за счёт более точных стратегических решений благодаря использованию ИИ при анализе данных

20–45% повышение производительности отдела разработки

на обработку обращений клиентов

На 60% снижение времени

на обработку обращений клиентов

MWS GPT

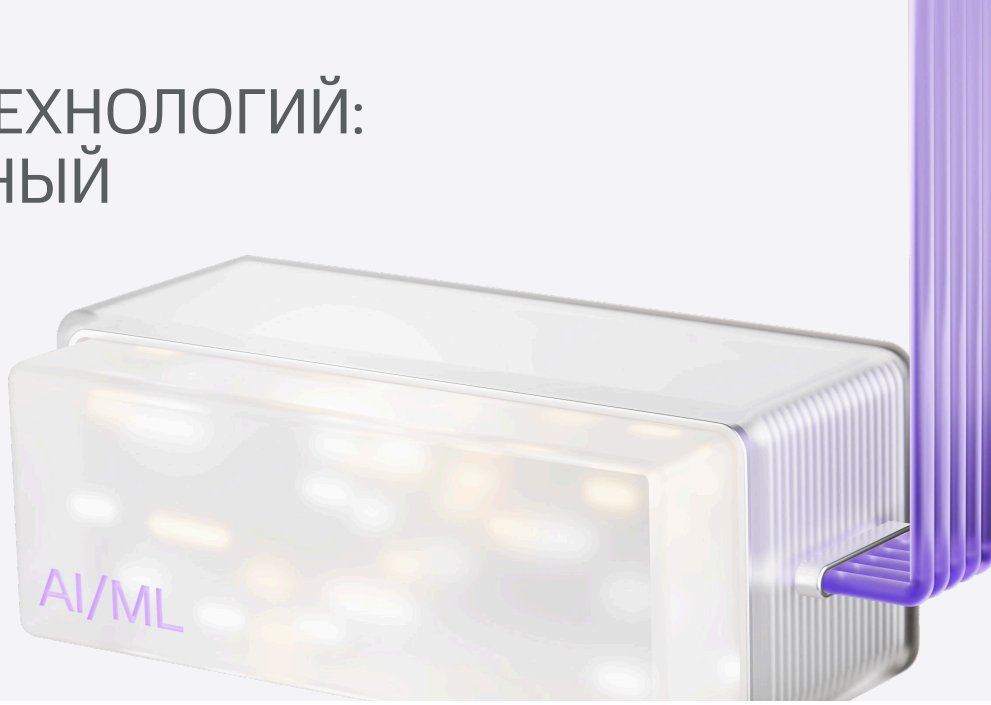
Платформа для работы с большими языковыми моделями (LLM) для бизнеса

24 часа Период от запроса модели до её работы в проде	2 года Экономия трудозатрат на создание подобного платформенного решения	Все существующие модели доступны на платформе с возможностью дообучения	

MWS COSTUME AI

Индивидуальная разработка AI-решений под нужды конкретного клиента

ВНЕДРЕНИЕ ТЕХНОЛОГИЙ: ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ



Раздел искусственного интеллекта охватывает широкий спектр технологий. Структура рынка искусственного интеллекта в данном исследовании строится, опираясь на общий подход к декомпозиции ИТ-рынка. В данной части фокус сконцентрирован на вертикалях Hardware и Software, которые, в свою очередь, разделяются на три группы: (1) Вычислительную технику, (2) AI-агенты и приложения, (3) AI-платформы. Технологии ИИ менее развиты у корпоративных клиентов относительно облаков и кибербезопасности. Принимая во внимание размер бюджета, наличие стратегии и аналитики потребления продуктов, можно сделать вывод, что для многих компаний данные решения остаются экспериментальной технологией и не интегрированы массово в корпоративные процессы. Несмотря на драматическое внимание со стороны профессионального сообщества и широкую распространенность на уровне потребления конечными пользователями, решения в B2B сегменте все еще имеют большой нереализованный потенциал.

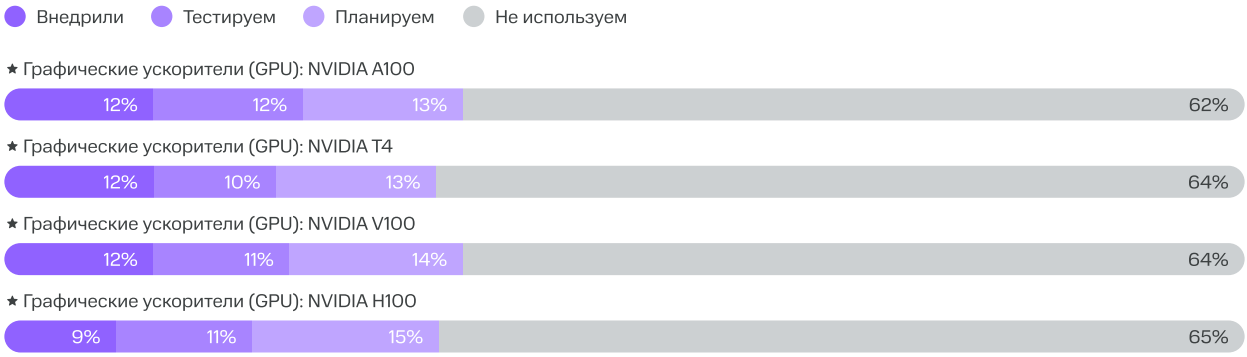
Для оценки среди полученных субкатегорий тех продуктов, которые имеют повышенный потенциал роста, введен подход, получивший название «Формула потенциала роста субкатегорий». Данная формула представляет собой сопоставление: с одной стороны параметра «внедрили», с другой стороны суммы параметров «тестируем» 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

Оценка потенциала роста субкатегорий, оценка согласно приведенной выше «Формуле потенциала роста субкатегорий» демонстрирует высокую перспективность развития всех групп решений, включая как прикладные программные продукты, так и отраслевые решения. Высокий потенциал развития ИИ-продуктов объясняется синергией нескольких мегатрендов, включая цифровизацию бизнес-процессов, удешевление и развитие инструментов машинного обучения, экспоненциальный рост данных и повышение компетенций компаний при работе с ними. Это означает, что инвестиции в ИИ будут оставаться стратегическим приоритетом для всех игроков, стремящихся не просто поддерживать бизнес, но и опережать рынок.

Вычислительная техника

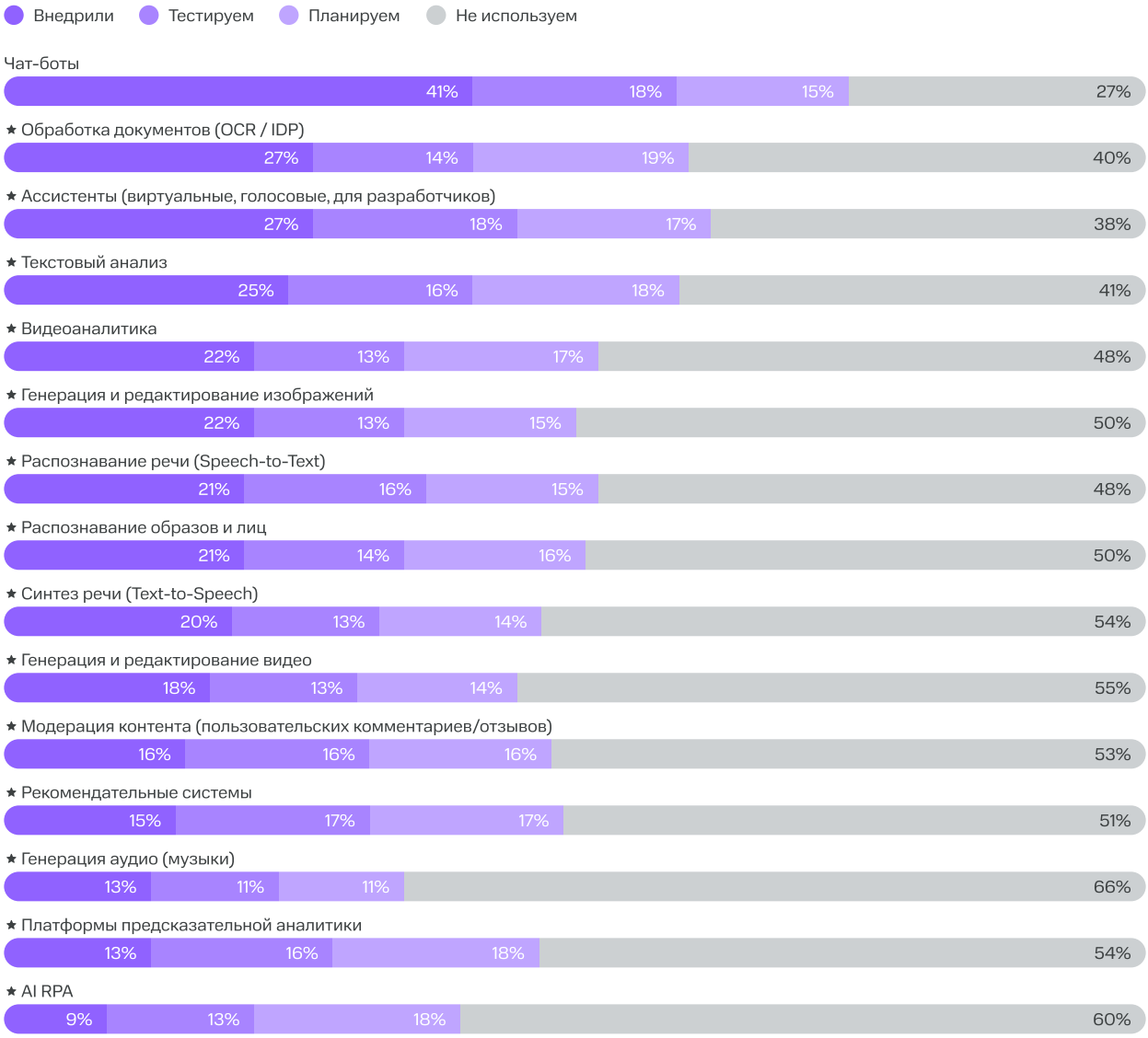


Спрос на аппаратную часть для работы с решениями на основе искусственного интеллекта формируется преимущественно компаниями крупного и крупнейшего бизнеса, а также экосистемными компаниями. Дополнительный спрос формируют специализированные компании в ИТ, FinTech, E-Com, MarTech, EdTech, MedTech, InsureTech и прочих технологических индустриях. Рассматривая полученные значения по параметрам «тестируем» и «планируем», наблюдаются в общей массе ответов респондентов незначительные проценты в категории «Вычислительная техника». Однако опираясь на предложенную ранее формулу по оценке потенциала субкатегорий, можно отметить высокие ожидания респондентов по потреблению данных решений.

Например, значения внедрения для графических ускорителей (GPU) различных моделей между собой сопоставимы, что все еще остается меньше в 5 раз относительно классических вычислений (CPU). Самой популярной видеокартой является NVIDIA A100. Стоимость этого решения меньше, чем NVIDIA H100 примерно в 1,5 раза, что делает ее более доступной для широкого спектра компаний, включая средние и малые предприятия. Новые логистические цепочки поставок видеокарт сформировались, при этом наблюдаются проблемы с технической поддержкой вендоров. С точки зрения спроса, конечному потребителю аппаратных решений критически необходимо сопоставлять практическую цель с моделями различных видеокарт.

★ — высокий потенциал

AI-агенты и приложения

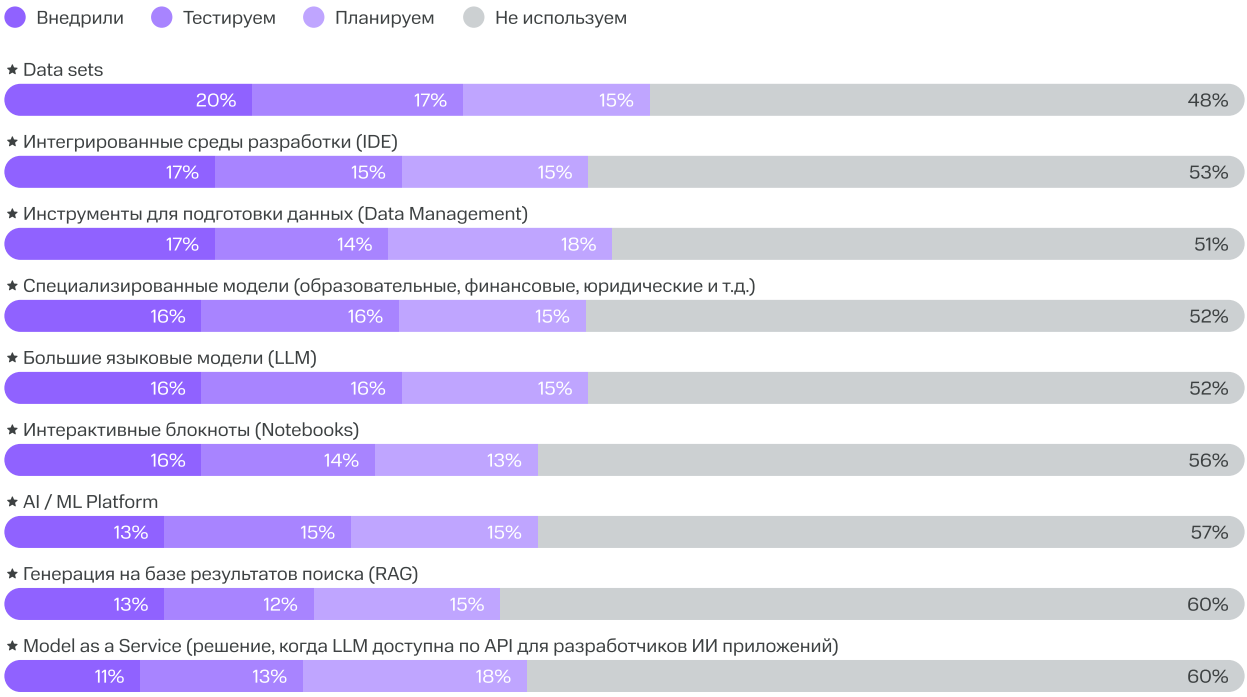


В отличии от категории «Вычислительная техника» субкатегории, которые относятся к «AI-агентам и приложениям», продемонстрировали значительно более высокие показатели внедрения. Это особенно наглядно демонстрируется субкатегорией «Чат-боты», которая является единственной среди всех субкатегорий в технологии ИИ в рамках данного исследования, для которой текущее внедрение превышает тестирование и планирование использования. Данные решения внедрены у 41% компаний-респондентов, против 18% и 15% соответственно, по ответам «тестируем» и «планируем». Остальные субкатегории показали существенные перспективы роста по формуле потенциала дальнейшего внедрения. Широкое использование чат-ботов связано не только с незначительной стоимостью внедрения, но и преимущественно с прозрачной ценностью для бизнеса и конечных пользователей.

Высокие проценты положительных ответов в категории «AI-агенты и приложения» связаны с тем, что для начала экспериментов с данными ИИ решениями характерен невысокий порог входа, в том числе, по причине применения облачной модели поставки большинства исследуемых продуктов. Также положительную настроенность участников рынка относительно решений ИИ можно сопоставить с тем, что разработчики прикладного ПО, решений в сфере кибербезопасности и платформенных решений активно стремятся интегрировать продукты данных субкатегорий в собственные конечные продукты.

Субкатегории, относящиеся к Обработке естественного языка (NLP) и Компьютерному зрению (CV) являются более востребованными относительно прочих решений, которые носят специализированный характер и применяющихся для решения узконаправленных задач, например, Рекомендательные системы, Платформы предсказательной аналитики и AI RPA.

AI-платформы



По всем перечисленным субкатегориям наблюдается относительно невысокий уровень текущего внедрения (11-20%), однако также можно отметить высокий потенциал дальнейшего развития, рассчитанный как сумма ответов «планируем» и «тестируем» (27-32%).

Наряду с автоматизированными решениями для ИИ, которые поставляются по облачной модели, крупными и крупнейшими компаниями активно потребляются услуги консалтинговых компаний и системных интеграторов. Данные участники рынка активно реализуют продукты в сфере ИИ, в том числе оказывают услуги по обучению, технической поддержке, тренингу моделей и прочему.

Респонденты активно отмечали развитие data-driven подхода в собственных компаниях, в частности, многие подсветили систематизацию процесса накопления бизнес-данных. Критическую важность для реализации данного подхода имеют не только продвинутые ИИ инструменты, но и базовые облачные, в частности, аналитические инструменты, без которых невозможно полноценное извлечение выгоды от применения ИИ.

Развитие технологий ИИ непосредственно связано с проникновением отдельных субкатегорий в облачные технологии. Здесь наблюдается прямая связь между данными взаимозависимыми технологиями. Дальнейшее развитие облачных систем вычислений и хранения, а также платформенных решений позволит существенно повысить доступность технологий ИИ и снизить барьеры для всех сегментов и индустрий бизнеса.

★ — высокий потенциал

ЗАКЛЮЧЕНИЕ

“ Облачные технологии, кибербезопасность и искусственный интеллект не просто развиваются параллельно — они формируют тесно взаимосвязанную экосистему, где успех одного направления в значительной степени зависит от зрелости других. Такой синергетический рост является основой для обеспечения конкурентоспособности как отдельных корпоративных заказчиков, так и национальной экономики в целом.

Облачные технологии, прежде всего сегменты IaaS и PaaS, остаются наиболее динамично развивающейся частью ИТ-рынка России. Согласно нашим последним оценкам, облака уже составляют около 7,7% общего объема ИТ-рынка и демонстрируют среднегодовые темпы прироста свыше 30% за период 2021–2024 годов. Для значительного числа компаний виртуальные ЦОДы и виртуальные частные облака фактически стали инфраструктурным стандартом — commodity-продуктом. При этом рынок демонстрирует устойчивый интерес не только к публичным, но и к частным и гибридным сценариям, что отвечает растущему запросу на управляемость, кастомизацию и снижение рисков vendor lock-in. Крупнейшие клиенты формируют спрос на мультиоблачные модели и активно тестируют подходы, сочетающие разных провайдеров для решения задач отказоустойчивости и дифференциации сервисов.

Кибербезопасность в свою очередь становится неотъемлемым элементом всех стратегий цифровизации. Особенно высокий уровень вовлеченности характерен для ИТ, добычи полезных ископаемых и науки, где риски киберугроз и регуляторное давление объективно выше. Это определяет необходимость интеграции решений по КБ уже на этапе проектирования архитектуры инфраструктуры, а также формирует значительные перспективы для развития сервисов управляемой безопасности и специализированных платформ мониторинга и реагирования.

Рынок ИИ в России пока находится на более ранней стадии формирования устойчивых корпоративных практик. Видны сравнительно скромные показатели внедрения инфраструктур для высокопроизводительных вычислений (GPU VM и HPC) — спрос на эти ресурсы в основном обеспечивают компании с сильными собственными командами Data Science, доля которых составляет лишь треть рынка.

Если рассмтривать технологии с продуктовой точчки зрения, то в качестве обладающей наибольшими возможностями развития выделяется ИИ. Решения в этой области обладают высокой перспективой дальнейшего развития для большинства субкатегорий (по 29 из 30 субкатегории сумма параметров «тестируем» и «планируем» больше параметра «внедрили», что составляет 97%). По ответам респондентов облачные технологии имеют больший процент внедрений, но, при этом, меньшее количество субкатегорий со значимым потенциалом роста (28 из 67 субкатегорий, что составляет 42%). Наименьшие резервы по выделенным субкатегориям показала технология кибербезопасности (только 8 из 28 субкатегорий имеют высокий рыночный потенциал, что составляет 29%). Полученная аналитика по данной технологии может быть связана с высокой актуальностью рисков кибербезопасности для российских компаний, и, как следствие, существенная часть компаний оперативно отреагировала на данный тип риска, внедрив ключевые продукты информационной безопасности.

Основываясь на комплементарной продуктовой аналитике предложения, в частности, в облачных технологиях, необходимо отметить, что по подавляющему большинству продуктовых субкатегорий у отечественных провайдеров есть сформированный портфель решений собственной разработки или доработанный open source. Представляется, что текущего рыночного предложения по всем 3 исследуемым технологиям, достаточно для удовлетворения не только базовых технологических потребностей, но и для экспериментальной и инновационной деятельности компаний.

Игорь Зарубинский
Исполнительный директор MWS, CEO MWS Cloud

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 публичных облаков одновременно.

MWS CONTAINER PLATFORM

Надёжная платформа для разработки и эксплуатации контейнерных приложений. Помогает быстрее внедрять инновации, проводить цифровую трансформацию и запускать ИТ-продукты

на 40% снижает нагрузку на ИТ-команды	**на 70%** ускоряет выпуск новых приложений и упрощает их эксплуатацию	**на 80%** автоматизирует ручные операции	

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	

ВИРТУАЛЬНАЯ ИНФРАСТРУКТУРА С GPU

Готовая масштабируемая виртуальная инфраструктура для размещения любых информационных систем клиента, разработки и тестирования ПО, а также облачные серверы на базе NVIDIA для ускорения высоконагруженных вычислений и машинного обучения

≥5 минут на развертывание инфраструктуры	**15** 15 зон доступности	**30%** сокращение расходов на ИТ-инфраструктуру	

Авторы

Николай Шуняев
Карина Бабайкина
Полина Ли
Александр Решетняк
Галина Гайдаржи
Светлана Ларина

MTC 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 облачном рынке России. Мы агрегируем лучшие глобальные и российские практики в области облаков, искусственного интеллекта, кибербезопасности и информационных технологий в целом