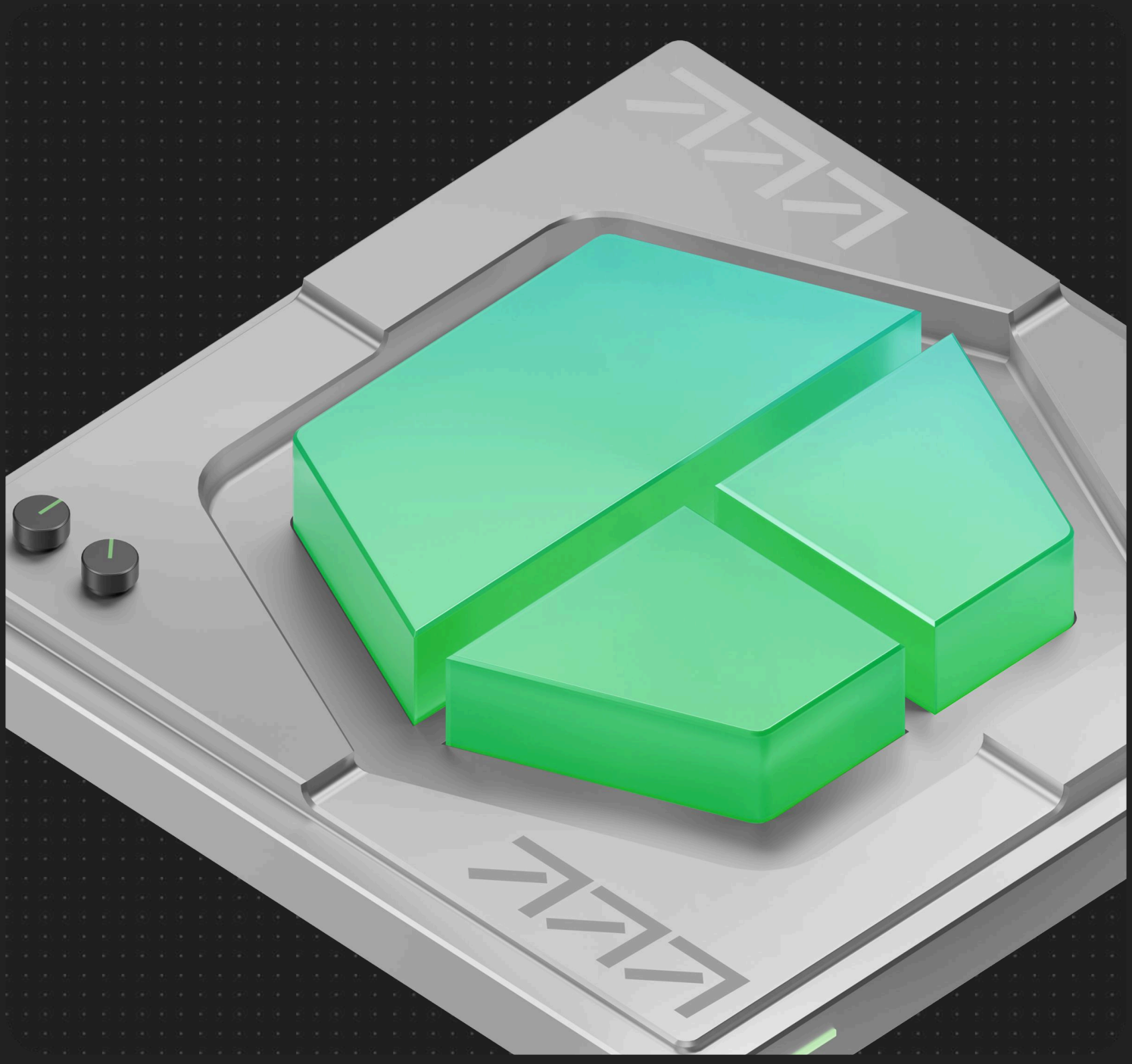
Факторы успеха при внедрении ИИ-агентов



Факторы успеха при внедрении ИИ-агентов

Развитие технологий искусственного интеллекта (далее — ИИ) за последние десятилетия сопровождалось расширением спектра решаемых задач — от автоматизации локальных вычислительных процедур до работы с неструктурированными данными, которая стала возможной благодаря обучению моделей на больших массивах информации. Однако по мере развития алгоритмов все более актуальным становился вопрос о переходе от инструментов, выполняющих единичные действия по запросу человека, к системам, способным самостоятельно ставить цели, планировать сложные последовательности операций и выполнять их в рамках этих целей.

> Именно в этом контексте в 2024–2025 годах сформировался термин **«агентный ИИ»** — искусственный интеллект, реализованный через структуры автономных агентов, способных воспринимать среду, самостоятельно принимать решения, взаимодействовать с цифровыми системами и координировать свои действия с другими агентами и людьми.

Согласно данным исследования Axenix и МГУ, представленным на конференции AI Journey, затраты на внедрение ИИ-агентов в течение трех лет существенно различаются в зависимости от масштаба бизнеса: для корпораций они превысят 950 млн рублей, для крупных компаний составят 200–300 млн рублей, для среднего бизнеса — 30–60 млн рублей, а для малых предприятий — 5–15 млн рублей. Совокупная экономия от внедрения таких систем оценивается в 15–40% в зависимости от отрасли.

Наибольшую эффективность эксперты прогнозируют в финансовом секторе, где ускорение процессов может достичь 25–45%, снижение ошибок — 15–30%, а экономия на фонде оплаты труда — 10–35%. В ретейле косвенные эффекты, такие как персонализация предложений, ведут к росту конверсии на 10–25% [1].

Согласно исследованию МТС, мировой рынок ИИ-агентов демонстрирует взрывной рост: с 25 млрд $ в 2024 году он может достичь 755 млрд $ к 2030 году, что соответствует среднегодовому темпу роста в 76%. Ключевыми драйверами выступают венчурные инвестиции, которые в 2024 году составили 9,7 млрд $ (рост 46% CAGR), при этом уже в первом квартале 2025 года вложения достигли 2,8 млрд $.

Российский рынок пока находится на начальной стадии: совокупные инвестиции в ИИ составили 530 млн $ (+62% год к году), из которых 70% — бигтехи (Яндекс, Сбер, МТС). Исследователи МТС выделяют четыре зоны автоматизации бизнес-функций, отмечая, что наибольший потенциал ИИ-агентов — в операционно-ориентированных задачах с высокой частотой повторения и низкой потребностью в эмпатии [2].

Экономический эффект внедрения ИИ-агентов

Экономические эффекты, обнаруженные у российских компаний в рамках проведения исследования, варьируются от сокращения времени выполнения задач на 40–50% до кратного роста производительности труда.

В финансовом секторе отдельные эксперты оценивают ежегодные затраты лидеров отрасли на ИИ-агентов в десятки миллионов евро, при этом горизонт окупаемости крупных инфраструктурных проектов нередко достигает 5–7 лет.

Но большинство экспертов сходятся во мнении, что оценивать эффект следует не в прямом сокращении затрат, а в повышении эффективности работы команд: одна и та же команда с ИИ-агентами работает намного более продуктивно, чем без них.

Барьеры внедрения

Вместе с тем компании сталкиваются и с серьезными препятствиями. Дефицит квалифицированных специалистов остается главной проблемой: по оценкам некоторых экспертов, сегодня в России инициируется гораздо больше проектов, чем существует специалистов, способных их реализовать.

Сложность интеграции с существующим ИТ-ландшафтом, требования регуляторов и вопросы кибербезопасности также замедляют внедрение. В банковском секторе крайне актуальны проблемы, связанные с приемом решений в области кибербезопасности и соблюдения законодательства, поскольку ошибка в разработке и эксплуатации ИИ-агента может грозить серьезными последствиями вплоть до отзыва лицензии.

В сфере телекоммуникаций использование реальных данных пользователей для машинного обучения ограничено законодательством, что вынуждает российские компании применять синтетические данные.

Мировой опыт

> Мировой опыт также подтверждает востребованность ИИ-агентов. Согласно исследованию **Cloudera**, проведенному среди 1 484 руководителей ИТ-компаний в 14 странах, 96% организаций намерены расширять использование ИИ-агентов в течение ближайших 12 месяцев, а примерно половина — масштабировать эти системы на свои компании [3].

Отчеты **McKinsey** фиксируют, что 88% опрошенных организаций используют ИИ хотя бы в одной бизнес-функции, при этом наиболее активной сферой инвестиций является автономная автоматизация процессов [4].

Параллельно с этим аналитики **Gartner** предупреждают: более 40% проектов по внедрению ИИ-агентов могут быть закрыты к концу 2027 года из-за недостаточной зрелости данных, низкой устойчивости бизнес-процессов и завышенных ожиданий [5].

А в **Deloitte** подчеркивают, что автономность агентов порождает новые классы рисков: непреднамеренные действия, нестабильность поведения, отсутствие прозрачности и трудность аудита [6].

ИИ-агенты к концу 2025 года перестали быть экспериментальными инструментами и стали все чаще рассматриваться как одна из форм автоматизации бизнес-процессов. На момент проведения исследования существовало пять типов ИИ-агентов, разрабатываемых и внедряемых российскими компаниями:

- ассистент оператора бизнес-процесса;
- агент-оркестратор или агент-интегратор;
- аналитический агент;
- агент поддержки клиента;
- агент-наблюдатель (мониторинг процессов).

Чаще всего разрабатывались и внедрялись аналитические ИИ-агенты, чуть реже — агенты-наблюдатели, агенты поддержки и ассистенты оператора бизнес-процесса (рис. 1). При этом эксперты СберАналитики отмечают, что ИИ-ассистентов и ИИ-агентов используют уже 39% российских компаний [7].

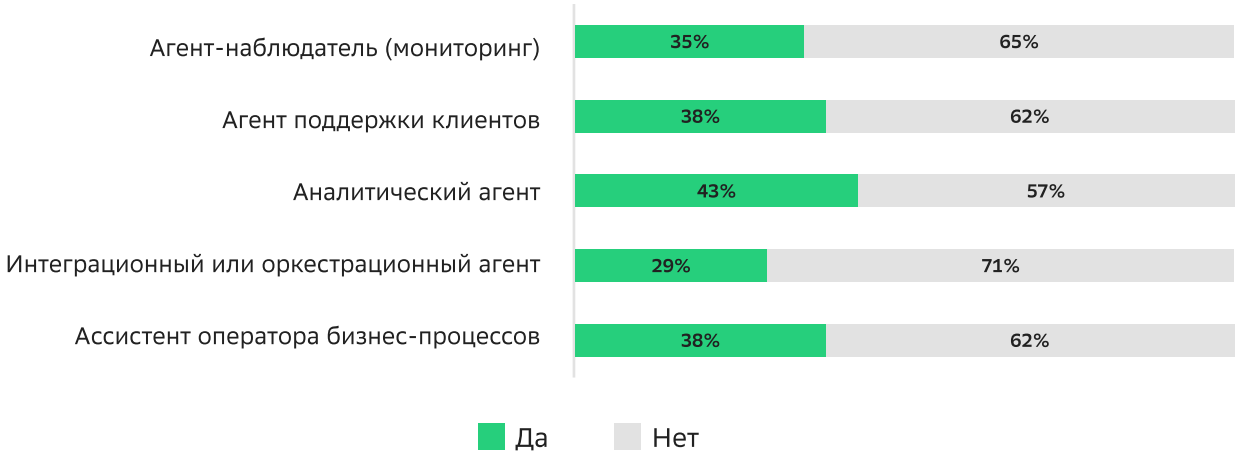


Рисунок 1. Типы ИИ-агентов, разрабатываемых и внедряемых в компаниях респондентов

Российская практика

Российская практика, выявленная и обобщенная при анализе кейсов Газпромбанка, Сбера, Альфа-Банка, Билайна, МТС, Группы Лента, Московской биржи и других компаний, демонстрирует как высокий потенциал технологии, так и специфические ограничения, связанные с регуляторной средой, кадровым дефицитом и необходимостью адаптации глобальных решений к российским экономическим условиям. Именно эта многоаспектность обусловливает анализ факторов успеха, представленный в настоящем отчете.

Разработка модели зрелости и определение факторов успеха

В рамках проведения исследования удалось сформировать модель зрелости внедрения ИИ-агентов и выявить ключевые факторы успеха. Эмпирическую базу модели составили данные, полученные из четырех взаимодополняющих источников:

- глубинные интервью с экспертами-практиками;
- экспертная сессия с представителями российского бизнеса;
- количественный опрос представителей компаний;
- анализ источников, отражающих российский и зарубежный опыт внедрения ИИ-агентов.

Такой подход позволил обеспечить как значимость выводов, так и глубину понимания контекстуальных факторов, влияющих на успех внедрения агентных систем.

Глубинные интервью с экспертами-практиками

Для сбора качественных данных о практиках внедрения и применения ИИ-агентов было проведено 30 глубинных полуструктурированных интервью с руководителями ИИ-направлений, техническими директорами и ведущими специалистами компаний из различных секторов экономики. География интервью и охват порядка десяти отраслей включали финансовый сектор (Газпромбанк, Сбер, Альфа-Банк, Мосбиржа), ритейл (Лента, X5), телекоммуникации (Билайн, МТС), ИТ и разработку, производственный сектор, включая добывающую отрасль, а также EdTech (СберОбразование). Такой широкий охват позволил выявить как отраслевую специфику, так и кросс-отраслевые закономерности внедрения агентных систем.

Структура интервью охватывала 13 ключевых тематических блоков: автоматизируемые процессы и задачи, экономическая эффективность внедрения, риски и ограничения, требования к данным и инфраструктуре, типы выбираемых агентов и уровни их автономности, UX-паттерны доверия, количественные показатели затрат и окупаемости, структура зрелостной модели, подходы к ускорению возврата инвестиций, практики управления рисками, факторы выбора стратегий, рыночные и технологические тренды, а также стратегии развития агентных систем в компаниях. Полученные качественные данные позволили выявить глубинные причинно-следственные связи, объясняющие успех или неудачу проектов по внедрению ИИ-агентов.

Экспертная сессия с представителями российского бизнеса

Для сбора качественных данных о состоянии внедрения ИИ-агентов в российских компаниях была проведена экспертная сессия, в которой приняли участие представители крупных российских компаний. Экспертная сессия прошла под модерацией представителей Высшей школы бизнеса НИУ ВШЭ.

Количественный опрос представителей компаний

Для сбора количественных данных о практиках внедрения и применения ИИ-агентов была разработана структурированная анкета. Учитывались ответы только тех респондентов, чьи компании уже имеют хотя бы одного ИИ-агента в промышленной эксплуатации. Ответы представителей компаний, не имеющих работающих ИИ-агентов, не учитывались, что позволило выявить ключевые факторы, обуславливающие успех внедрения ИИ-агента.

Значительная часть вопросов была основана на использовании шкалы Ликерта. В таких вопросах респондент должен был выразить согласие или несогласие с тем или иным утверждением по шкале от 1 (полностью не согласен) до 7 (полностью согласен). Утверждения, которые вызывали наибольшую уверенность респондентов, зачастую ложились в основу модели зрелости и рассматривались как фактор успеха.

Опрос включал широкий спектр вопросов: контекст компании и ее отраслевая принадлежность, зрелость использования искусственного интеллекта, доступность данных и состояние ИТ-инфраструктуры, практики управления рисками и доверием, экономические и стратегические аспекты применения агентных систем. Анкета включала также блок вопросов, посвященных конкретным кейсам внедрения, что позволило собрать детализированную информацию о реальных практиках, включая данные о CAPEX, OPEX, сроках окупаемости и достигаемых эффектах.

Целевую аудиторию опроса составили представители компаний, численность которых составляет свыше 100 человек. Учитывались только ответы респондентов, которые относятся к топ-руководству компании или к категории ИТ-специалистов: владельцы продукта, разработчики, специалисты по автоматизации, специалисты технической поддержки, ИТ-архитекторы, специалисты по кибербезопасности и пр. Отдельно оценивалась связь респондента с реализацией проектов по разработке и внедрению ИИ-агентов. Если респондент не имел практического опыта, то опрос завершался.

Для повышения репрезентативности ответов участники опроса были сбалансированы по уровню цифровой зрелости их предприятий. Если респондент заявлял, что его компания ориентируется на цифровизацию, то он продолжал опрос, причем доля таких респондентов составила порядка 50%. Если сообщалось о том, что компания может частично ориентироваться на цифровизацию, то участие в опросе также продолжалось, но в итоговых результатах доля подобных ответов не превышала 20%. Квота для респондентов, чья компания не ориентируется на цифровизацию, составила 30%. Ответы респондентов, не определившихся при ответе на этот вопрос, не учитывались.

Анализ литературы, отражающей российский и зарубежный опыт внедрения ИИ-агентов

Четвертым источником эмпирических данных стал структурированный разбор практик внедрения ИИ-агентов в России и за рубежом. В рамках исследования были проанализированы материалы, отражающие опыт множества реальных внедрений ИИ-агентов в различных юрисдикциях: в РФ, в Евросоюзе, в Китае, а также в США. Особое внимание было уделено анализу корпоративных публикаций и стратегических документов ведущих технологических компаний, включая Huawei, Alibaba Group, Tencent, Baidu, Meituan, Ant Group и ByteDance, что позволило выявить специфику восточного подхода к развитию агентных систем. Дополнительно были изучены отраслевые отчеты и аналитические материалы международных исследовательских и консалтинговых организаций: Cloudera, McKinsey, IBM, Deloitte, Gartner, а также профильные публикации по медицине, финансам, телекоммуникациям и розничной торговле. Такой комплексный анализ позволил сопоставить российскую практику с мировыми трендами и выявить как универсальные закономерности, так и национальную специфику внедрения ИИ-агентов в корпоративных информационных системах.

Модель зрелости внедрения ИИ-агентов

«Представленная модель зрелости обобщает текущий опыт по ИИ-агентам российских и зарубежных предприятий и предлагает стройную систему для оценки зрелости компании при их разработке и внедрении в бизнес».

Евгений Зараменских
Профессор, руководитель департамента бизнес-информатики ВШБ НИУ ВШЭ

Переход от экспериментального использования ИИ-агентов к их промышленной эксплуатации требует от компаний не только значительных инвестиций, но и высокой степени цифровизации бизнес-процессов. Анализ практик внедрения, собранных в ходе исследования, подтверждает, что успех масштабирования напрямую зависит от уровня цифровой зрелости компании. На основе экспертных интервью и анализа кейсов была разработана пятиуровневая модель цифровой зрелости, которая поможет компаниям диагностировать свое текущее состояние, выявлять узкие места и формировать дорожную карту внедрения агентных ИИ-решений.

Уровень 1: Начальный

На этом этапе компания характеризуется наличием единичных, часто инициативных пилотных проектов с ИИ-агентами, которые реализуются в низкорисковых изолированных сферах. Системные процессы управления такими инициативами отсутствуют. Интеграция агентов с корпоративными системами (CRM, ERP) не проводится, экспертиза сконцентрирована в руках отдельных энтузиастов, а не выделена в отдельную команду или центр компетенций. Стратегическое видение роли ИИ-агентов в бизнесе отсутствует, а инвестиции носят разовый несистемный характер. Культура компании характеризуется высоким уровнем неопределенности и насторо-женности в отношении автономных систем.

Уровень 2: Повторяемый

Компания переходит к осознанным экспериментам с ИИ-агентами. На этом уровне у компании уже имеется несколько успешных кейсов внедрения ИИ-агентов, что позволяет сформировать первые повторяемые подходы. Появляются формализо-ванные, но не закрепленные в стандартах, процессы отбора и предварительной оценки проектов по созданию агентов. Начинается интеграция ИИ-агентов с отдельными корпоративными системами через API (Application Programming Interface — програмный интерфейс приложений). Формируется команда специалистов, отвечающая за развитие направления. Руководство начинает проявлять интерес и поддерживать инициативы, однако финансирование остается единичным. В компании начинает складываться понимание потенциальной ценности ИИ-агентов.

Уровень 3: Определенный

Главная характеристика этого уровня — институционализация практик работы с ИИ-агентами. ИИ-агенты начинают внедряться в бизнес-процессы, выходя за рамки простых экспериментов. В компании утверждены корпоративные стандарты разработки, тестирования и внедрения ИИ-агентов. Налажены базовые процессы мониторинга качества работы моделей, лежащих в основе агентов, и их технической поддержки. Создан центр компетенций или специальное подразделение, которое аккумулирует экспертизу по ИИ-агентам и распространяет лучшие практики. Появляется понятная стратегия и дорожная карта развития ИИ-агентов, а инвестиции начинают планироваться в среднесрочной перспективе. Сотрудники проходят обучение работе с ИИ-агентами и уровень доверия к технологии повышается.

Уровень 4: Управляемый

На этом этапе компания переходит от простой автоматизации отдельных задач к сквозной оркестрации процессов с помощью многоагентных ИИ-систем. Внедрена система ключевых показателей эффективности для оценки влияния ИИ-агентов на операционные и финансовые показатели бизнеса. Управление рисками становится проактивным: внедрены механизмы контроля действий, цензурирования, полного логирования и аудита действий агентов. Успешные практики масштабируются на все подразделения компании. ИИ-агенты становятся неотъемлемой частью операционной модели, а инвестиции в это направление рассматриваются как стратегические. С точки зрения корпоративной культуры компания готова к экспериментам и быстрой интеграции решений с участием ИИ-агентов.

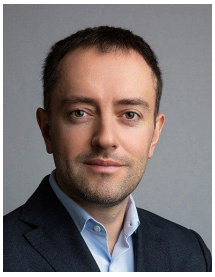
Уровень 5: Оптимизируемый

Это высший уровень зрелости, который характеризуется переходом компании к модели, управляемой данными и автономными системами. Бизнес-процессы становятся адаптивными и самооптимизирующимися благодаря взаимодействию множества специализированных ИИ-агентов, способных к самообучению на основе накапливаемого опыта, что создает устойчивое конкурентное преимущество, которое сложно скопировать. Технология ИИ-агентов глубоко интегрирована во все аспекты деятельности — от разработки продуктов до взаимодействия с клиентами и партнерами. Компания обладает культурой непрерывных инноваций, а сотрудники всех уровней владеют компетенциями для эффективной работы в симбиозес ИИ-агентами. На этом уровне ИИ-агенты становятся движущей силой стратегии и основой для формирования новых бизнес-моделей.

Можно также выделить четыре типа готовности бизнеса к внедрению ИИ-агентов:

1 **технологическая** (инфраструктура и данные)	2 **организационная** (процессы и экспертиза)
3 **технологическая** (инфраструктура и данные)	4 **культурная** (принятие и доверие к автономным системам)

Данные и интеграция



Иван Чередниченко
Сфера государственных лотерей

> «Базовые проблемы — если данные не готовы, правильно не собраны, нет правильной архитектуры, то ничего не получится. Это основа».

Качество данных и глубина интеграции с корпоративным ИТ-ландшафтом являются основными факторами, определяющими успешность внедрения и масштабирования ИИ-агентов [8]. Аналитики РБК отмечают, что фрагментация данных и проблемы с интеграцией в целом являются критическими проблемами для российских компаний, принявших решение разработать и внедрить ИИ-агента [9].

Анализ экспертных интервью и отраслевых данных, собранных в ходе исследования, показывает прямую корреляцию между зрелостью инфраструктуры данных и достигнутым уровнем автономности агентных систем. В тех секторах, где данные структурированы, унифицированы и централизованы (преимущественно финансы и информационные технологии), ИИ-агенты демонстрируют высокую эффективность и высокую автономность. В отраслях с фрагментированными, неструктурированными данными (в частности, медицина и промышленное производство) эффективность и автономность ИИ-агентов существенно ниже.

Доступность и качество данных

Основным ограничением для большинства организаций остается неполнота данных, сложность их получения и низкое качество. Для корректной работы агента необходимы структурированные ретроспективные данные по бизнес-процессам, базы знаний и контекстная информация, используемая в RAG-архитектурах (Retrieval Augmented Generation — поисковая дополненная генерация). В ряде отраслей, например в телекоммуникации, использование реальных данных для обучения ограничено законодательством, что вынуждает компании применять синтетические данные. Эксперты подчеркивают, что если объем данных недостаточен, если данные не собраны должным образом или отсутствует правильная архитектура данных, проекты по внедрению ИИ-агентов обречены на неудачу.

Успех ИИ-агента во многом зависит не от лежащей в его основе модели, а от качества данных, на которых его модель будет обучаться и с которыми в дальнейшем будет работать. Результаты опроса подтверждают важность качества данных (табл. 1). Практически все респонденты, чьи компании сумели внедрить в свою деятельность ИИ-агентов, указывают на качество данных, достаточное для промышленного использования в ИИ-решениях. Напротив, практически никто из респондентов не оценил качество данных как низкое. Компании с низким качеством данных попросту не сумели разработать и внедрить ИИ-агента.

Вопрос \ Шкала	1 — полностью не согласен (а)	2	3	4	5	6	7 — полностью согласен (а)
Качество данных в нашей компании достаточно для промышленного использования в ИИ-решениях	0%	3%	5%	11%	26%	25%	30%
Базовые системы (ERP, CRM, платформы) достаточно интегрированы для подключения ИИ-решений в компании	0%	3%	2%	11%	23%	19%	32%
В нашей компании есть формализованная политика управления данными для ИИ (безопасность, приватность, хранение)	0%	2%	1%	10%	24%	25%	38%

Таблица 1. Распределение ответов респондентов по вопросам о данных и интеграции

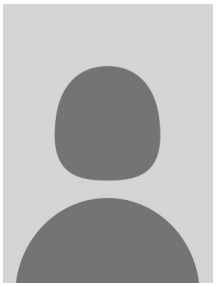
Интеграция и архитектура

> Способность ИИ-агента взаимодействовать с существующими корпоративными системами (CRM, ERP и др.) критически важна. Значительной проблемой часто становится интеграция с унаследованными системами. Для обеспе-чения безопасности часто применяется изоляция процессов: ИИ-агенты работают в контейнерных средах с ограниченным набором разре-шенных команд. Зачастую параллельно с разработкой ИИ-агентов создается среда исполнения моделей, которая обеспечивает их безопасное функцио-нирование в защищенном контуре. Эксперты также отмечают, что встраи-вание ИИ-агента в текущий ИТ-ландшафт часто является сложной задачей, которая в некоторых организациях решается на уровне принятия рисков высшим руководством.

Проведенный опрос подтвердил, что интеграция информационных систем предприятия имеет важное значение для внедрения ИИ-агента (см. табл. 1). Практически все респонденты, чьи компании успешно разработали и внедрили ИИ-агентов, оценивают уровень интеграции информационных систем выше среднего, причем чаще всего эксперты отмечали наличие максимально возможного уровня интеграции.

Формализованные политики управления данными становятся главным фактором успешного внедрения ИИ-агентов. Согласно данным опроса (см. табл. 1), компании, достигшие значимых результатов в агентной автоматизации, значительно чаще обладают документированными и соблюдаемыми политиками работы с данными. Напротив, отсутствие таких политик ограничивает или замедляет внедрение агентных систем, особенно в таких жестко регулируемых отраслях, как финансы и телекоммуникации.

Инженерные навыки и платформа разработки



«Есть дисбаланс между пониманием внедрения ИИ-агентов самим бизнесом и людьми (преимущественно специалистами по Data Science), которые его внедряют. Сейчас продают больше и инициируют больше проектов в РФ на порядки, чем существует число специалистов, которые могут их реализовать».

Андрей Бугаенко
Ранее – Мосбиржа

Развитие и масштабирование ИИ-агентов в корпоративной среде невозможно без наличия соответствующих инженерных компетенций и зрелой платформенной инфраструктуры. Исследование показывает, что дефицит квалифицированных кадров и незрелость инструментов разработки являются одними из главных барьеров, замедляющих переход от пилотных проектов к промышленной эксплуатации.

Дефицит экспертизы как главное ограничение

Экспертные интервью однозначно указывают на нехватку специалистов, способных проектировать, разрабатывать и сопровождать агентные системы. Рынок испытывает острый дефицит экспертов по архитектурам больших языковых моделей, проектированию мультиагентных систем, работе с вычислительной инфраструктурой и интеграции ИИ в цифровые сервисы предприятий. Российские компании вынуждены конкурировать за ограниченные кадровые ресурсы, что увеличивает стоимость проектов и снижает темпы внедрения. При этом требуются не только специалисты в области науки о данных, но и инженеры по ИИ и машинному обучению, а также бизнес-аналитики, понимающие не только процессы предприятия, но и агентные технологии.

В российских компаниях сегодня наблюдается значительный дефицит экспертизы, что вынуждает бизнес достаточно часто привлекать внешних поставщиков для разработки агентных ИИ-решений — об этом заявило более половины респондентов. Разумеется, не стоит сбрасывать со счетов немалое число организаций, полагающихся преимущественно на собственные разработки или комбинирующих их с внешними. Но чаще всего дефицит компетенций и квалифицированных кадров на предприятии сильнее ощутим и вынуждает бизнес обращаться к услугам внешних разработчиков (табл. 2).

Вопрос \ Шкала	1 — полностью не согласен (а)	2	3	4	5	6	7 — полностью согласен (а)
Наша компания полагается на внешних вендоров для разработки ИИ-решений	1%	4%	10%	14%	21%	21%	29%
Рыночные вендорские решения покрывают функциональные потребности нашей компании в области ИИ	2%	4%	7%	7%	24%	26%	30%
В нашей компании есть внутренние ресурсы по ИИ и ML-инжинирингу	0%	1%	3%	11%	19%	29%	37%

Таблица 2. Распределение ответов респондентов по вопросам об инженерных навыках и платформах разработки

Интересно, что большинство респондентов отмечают высокую степень соответствия представленных на рынке решений потребностям организации (см. табл. 2). И хотя в российской экономике существует значительная доля компаний, чьи потребности сейчас не закрываются или слабо закрываются функциональностью готовых решений, в целом поставщикам все-таки удается удовлетворять основные потребности российского бизнеса.

Платформенный подход

Для преодоления кадрового голода и ускорения разработки крупные игроки идут по пути создания собственных платфор-менных решений. Платформа позволяет стандартизировать процесс создания агентов, переиспользовать наработанные компоненты и снизить требования к квалификации разработчиков на местах. Пример Tencent Cloud Agent Development Platform показывает типовую структуру такой платформы: LLM-ядро, усиление знаний через retrieval (RAG), автоматизация через workflow-оркестрацию и поддержка многоагентных конфигураций.
В этой логике модель не равна агенту; она становится агентом только при наличии инструментария, оркестрации и контролируемого контура выполнения задач.

Вопрос интеграции является главным для платформенного подхода. Наиболее популярным вариантом интеграции для российских компаний стала интеграция через API, однако говорить о подавляющем перевесе в пользу этого варианта не приходится: отечественный бизнес также активно применяет событийную интеграцию в реальном времени (real-time интеграция), RPA-взаимодействие (Robotic Process Automation — роботизированная автоматизация процессов) и пакетную обработку данных (Extract, Transform, Load — ETL). Перевес API-интеграции объясняется, прежде всего, относительной простотой и понятностью этого формата интеграции для большинства разработчиков (рис. 2).

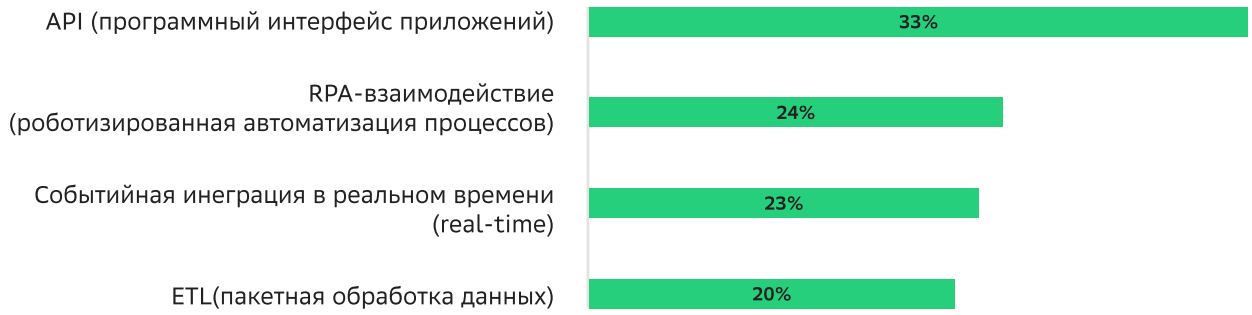


Рисунок 2. Наиболее распространенные типы интеграции ИИ-агентов в компаниях респондентов

Выбор между внутренней разработкой и готовыми решениями

Результат такого выбора напрямую зависит от наличия необходимых компетенций у специалистов компании. Если у компании есть квалифицированные специалисты и сформировалась готовность инвестировать финансовые средства в развитие ИИ-направления, то обычно она выбирает путь собственной разработки, особенно когда речь идет об обеспечении стратегической независимости.

Крупные игроки также часто идут именно по этому пути, создавая собственные большие языковые модели и платформы. Если же компания не имеет квалифицированного персонала и не готова вкладываться в достаточно рискованный проект, то она вынуждена ждать появления готовых продуктов на рынке или использовать облачные сервисы для быстрого запуска пилотных проектов. В этом случае решающими факторами становятся скорость вывода продукта и совокупная стоимость владения.

При проведении опроса были выделены восемь потенциальных факторов, которые могут влиять на выбор между покупкой готового решения и собственной разработкой. Респонденты чаще всего указывали, как важные, три фактора: 1) безопасность и соответствие требованиям; 2) скорость получения эффекта и 3) адаптация под специфику бизнес-процессов. Интересно, что чувствительность данных и сложность интеграции с существующими информационными системами крайне редко рассматривались как ключевой фактор (рис. 3).

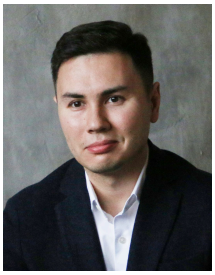
Рисунок 3. Наиболее важные факторы при выборе между собственной и внешней разработкой агентного ИИ-решения в компаниях респондентов

Выбор между внутренней разработкой и готовыми решениями

Результаты исследования свидетельствуют об изменении подходов к разработке. В отличие от традиционных алгоритмических ИТ-решений, где результат разработки предсказуем, при создании ИИ-агентов нет гарантии, что вся изначально запланированная функциональность будет реализована. Разработка ИИ-агентов предполагает итеративный подход: выбирается несколько подходящих моделей, после чего проводится предварительная оценка с целью понимания, реализуема ли задача и каковы будут затраты на реализацию. При таком подходе разработчик концентрируется на постановке целей и архитектурном проектировании. Непосредственная разработка и тестирование нередко осуществляются с использованием соответствующих ИИ-сервисов, что требует от инженерных команд наличия компетенций в области промпт-инжиниринга, построения RAG-контуров и обеспечения надежности агентных цепочек.

Важным способом обеспечить для компании эволюцию собственных инженерных практик становится разработка, поддержание и развитие внутренних ресурсов по ИИ и ML-инжинирингу. Более половины организаций, сумевших успешно внедрить ИИ-агентов, заявляют о наличии подобных ресурсов. Однако некоторая часть компаний обходится и без них, это связано в том числе с использованием готовых рыночных решений или привлечением внешних разработчиков (см. табл. 2).

Доверие к ИИ-агентам и контроль автономности



«Перед тем, как запрос приходит в языковую модель, стоит модуль цензурирования, который проверяет запрос от клиента, чтобы не было нарушения законодательства, например.
Если находятся нарушения, запрос дальше в работу не идет».

Тимур Измайлов
Альфа-Банк

По мере того как ИИ-агенты переходят от роли ассистентов к роли автономных исполнителей, способных самостоятельно инициировать действия в корпоративных информационных системах, вопросы доверия и контроля выходят на первый план. Согласно отраслевым исследованиям, применение агентных систем в телекоммуникационной отрасли требует создания формализованной архитектуры доверия, включающей контроль над последовательностью действий агентов и защиту от несанкционированного вмешательства [13].

Интересно отметить, что российское общество в целом доверяет ИИ. Можно ожидать, что клиенты крупных компаний в целом одобрительно отнесутся к применению ИИ-агентов в рамках бизнес-процессов и сервисов, взаимодействующих напрямую с клиентом. Как показали данные агентства FAVES Communications, почти половина россиян доверяет ответам нейросетей в поисковиках. Согласно опросу, в котором приняли участие 1 579 человек, 42% респондентов заявили о доверии полученной от ИИ информации и советам. При этом уровень доверия различается: 20,9% безоговорочно верят нейросетям, считая, что они анализируют большой массив данных, а 4,4% — из-за их непредвзятости. Еще 17,6% доверяют ответам при наличии ссылок на авторитетные источники. В то же время доля скептиков также значительна: 17% относятся к информации с недоверием из-за возможных ошибок ИИ, а 20,3% не хотят, чтобы ими управлял алгоритм. Исследование также показало, что 28% пользователей обычно полностью удовлетворены ответами нейросети и не ищут дополнительную информацию, а 34,1% никогда не переходят по ссылкам на первоисточники после прочтения ИИ-обзора [14].

Уровни автономности

На практике компании редко внедряют полностью автономные системы. Экспертные интервью свидетельствуют о широком спектре уровней автономности в зависимости от критичности процессов. В финансовом секторе и производстве, где цена ошибки высока, доминируют ИИ-агенты с низкой автономностью (уровни 0–1), выполняющие 1–4 простых действия и требующие постоянного контроля человека. В телекоммуникациях и отдельных банковских сервисах встречаются ИИ-агенты с высокой автономностью (уровни 3–4), способные самостоятельно вести диалог или обрабатывать заявки. Однако даже в этих случаях сохраняется возможность вмешательства человека. В целом можно констатировать, что полная автономность практически не встречается: всегда применяются инструменты мониторинга и остается возможность эскалации для решения задачи человеком.

Одним из способов управления уровнем автономности ИИ-агента является определение порогов участия человека в принятии решений с использованием ИИ. Как показал опрос, к подобному способу в том или ином виде склонны порядка ¾ российских организаций. При этом большинство респондентов утверждает, что в их компаниях четко определены соответствующие пороги. Отдельные организации их не применяют, что может быть связано как с иными способами управления автономностью ИИ-агентов, так и с применением полностью автономных ИИ-агентов в областях, где это допустимо с точки зрения рисков (табл. 3).

Вопрос \ Шкала	1 — полностью не согласен (а)	2	3	4	5	6	7 — полностью согласен (а)
В нашей компании определены пороги участия человека в принятии решений с использованием ИИ	1%	1%	6%	8%	23%	20%	41%
Ограничения на действия ИИ-агентов (правила и ограничения) формализованы и применяются в нашей компании	3%	2%	4%	5%	26%	25%	35%
В нашей компании ведутся журналы действий ИИ-агентов	1%	2%	3%	15%	25%	20%	34%
Сотрудники нашей компании доверяют результатам ИИ-систем	0%	2%	2%	14%	26%	27%	29%
Действия ИИ-агента явно помечаются и являются прозрачными для пользователя	0%	1%	7%	11%	27%	20%	34%

Таблица 3. Распределение ответов респондентов по вопросам доверии к ИИ-агентам и контролю автономности

Технические механизмы контроля

Для ограничения автономности ИИ-агентов компании внедряют специальные технические средства. Широкое распространение получила практика цензурирования: перед тем, как запрос попадает в большую языковую модель (или до возвращения ответа пользователю), он проходит через фильтры, отсекающие нерелевантные или опасные промпты.

В банковском секторе такие механизмы нередко сравнивают с сетевыми экранами. Дополнительно используются многоуровневые системы проверки, когда один ИИ-агент выступает цензором для другого. Часто практикуется запуск ИИ-агентов в изолированных контейнерных средах с ограниченным (белым) списком разрешенных команд, что исключает возможность несанкционированных действий.

Необходимость использования технических механизмов контроля над работой ИИ-агентов в целом практически не вызывает сомнений у представителей российских организаций. Российский бизнес чаще всего устанавливает технические ограничения на действия ИИ-агентов на основе описанных и формализованных правил (см. табл. 3). Некоторые организации, однако, не используют подобный подход. Причина кроется в том, что в ряде случаев цена ошибки ИИ-агента невысока, а вероятность ошибки является низкой. В подобной ситуации разработка технических механизмов ограничений и формализация правил становится нецелесообразной.

Прозрачность и логирование

> Фундаментальным требованием к агентным системам становится полная прослеживаемость их действий. Эксперты подчеркивают необходимость фиксации каждой промежуточной точки в системах контроля версий и детального логирования всех операций, выполненных ИИ-агентом. Это позволяет не только проводить последующий аудит, но и воспроизводить цепочку решений при возникновении инцидентов. Пользователь должен иметь возможность в любой момент понять, на каком этапе находится выполнение задачи, и при необходимости вмешаться или отменить действие ИИ-агента. Такой подход формирует базовое доверие к системе через ее предсказуемость и контролируемость.

Как показал опрос, российские организации, которые внедрили ИИ-агентов, обычно ведут логирование в том или ином виде, причем его интенсивность зависит от области применения ИИ-агентов. Более трети респондентов заявили о первостепенной важности логирования в их организации. При этом существуют компании, специфика использования ИИ-агентов в которых такова, что журналам действий ИИ-агентов уделяется мало внимания. Однако количество таких организаций невелико (см. табл. 3).

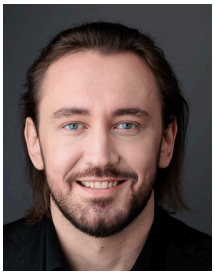
Интерфейсные паттерны доверия

> Интерфейсные решения играют важную роль в формировании доверия к агентам. Компании внедряют индикаторы уверенности ИИ-агента в ответе, например вероятность точности, кнопки экстренной остановки и паузы, явные уведомления о том, что действие выполняется ИИ-агентом, а не человеком.
> В ряде случаев, если уверенность модели в ответе низкая, система автоматически подключает человека к диалогу. Визуализация процесса выполнения (этапы, текущий статус) также способствует повышению прозрачности и, как следствие, доверия пользователей. Некоторые компании сознательно делают использование ИИ-агентов незаметным, встраивая их в существующие интерфейсы так, что пользователь даже не осознает, что взаимодействует с ИИ, что также является способом повысить принятие технологии.

Широкое применение интерфейсных паттернов доверия, отмеченное при интервьюировании, обусловливает высокий уровень доверия сотрудников компании к результатам работы ИИ-агентов (см. табл. 3). Наблюдается исчезающе малое количество организаций, чьи сотрудники не доверяют ИИ-агентам или доверяют им достаточно слабо. При этом существует значительная доля колеблющихся организаций, чьи сотрудники относятся к ИИ-агентам со средним уровнем недоверия. Но сегодня можно ожидать, что со временем количество даже таких компаний будет неуклонно снижаться.

Данные опроса также демонстрируют, что наиболее предпочитаемый способ повышения прозрачности агентных ИИ-решений для российского бизнеса —использование явных отметок (см. табл. 3). С их помощью принятие итоговых решений смещается в сторону бизнес-пользователя, который получает возможность решить, следует ли в конкретной ситуации и с учетом конкретного контекста положиться на действия ИИ-агента или требуется перепроверить их и выполнить те или иные операции самостоятельно.

Экономика внедрения и масштабирования



«Мы оцениваем эффективность ИИ-агентов и ИИ-помощников не в деньгах, а в эффективности сотрудников, т.е. один и тот же сотрудник с ИИ-агентом/помощником эффективней, чем без ИИ. Это технологический переход, сравнимый с созданием компьютера, интернетом и сотовой связью — переход к человекоцентричному развитию».

Никита Кузнецов
Газпромбанк

Переход от единичных пилотов к масштабному промышленному внедрению ИИ-агентов требует от компаний не только технологической готовности, но и серьезного подхода к оценке экономической эффективности. Исследование показывает, что непонимание финансовых аспектов и неспособность измерить реальный экономический эффект становятся одной из главных причин, по которой до 2/3 проектов остаются на стадии эксперимента. Как показала практика российских компаний, успешное масштабирование возможно только при выстраивании прозрачной системы финансового учета и управления инвестициями в агентные системы. Аналогичная ситуация наблюдается и за рубежом. Данные из открытых источников свидетельствуют о том, что при оценке экономической эффективности ИИ-агентов зарубежные предприятия нередко сталкиваются с трудностями измерения эффекта, что часто приводит к застреванию проектов на пилотной стадии [15].

Следует четко понимать, что затраты на разработку и внедрение ИИ-агентов — это не пустые затраты. Эксперты из «Яков и Партнеры» и Яндекса ожидают, что к 2030 году экономический эффект от внедрения ИИ достигнет 7,9–12,8 трлн рублей в год или 5,5% от прогнозируемого ВВП. При этом уже сейчас 78% опрошенных компаний отмечают реальный экономический эффект от внедрения ИИ. А наибольшее влияние на показатель EBITDA будет наблюдаться в отраслях, где ИИ используется как средство цифровой трансформации бизнес-модели и монетизируется. В частности, к таким отраслям аналитики отнесли телекоммуникации, ИТ, электронную коммерцию, медицину, строительство и недвижимость [16].

Структура затрат

Инвестиции в ИИ-агентов обязательно учитывают капитальные затраты (CAPEX) и операционные расходы (OPEX). CAPEX складывается из расходов на вычислительную инфраструктуру (GPU-кластеры, серверы), разработку или закупку ИИ-решений, а также интеграцию с существующими корпо-ративными информационными системами. OPEX включает поддержку и дообучение моделей, мониторинг, оплату облачных сервисов и содержание команды специалистов. На основе анализа успешных кейсов можно выделить несколько ключевых факторов, обеспечивающих положительную экономику внедрения. Во-первых, четкая приоритизация процессов с измеримым эффектом. Масштаб инвестиций существенно варьируется от нескольких десятков миллионов рублей в год для крупных игроков до 100–500 тыс. долларов для средних компаний и совсем небольших бюджетов для пилотных проектов.

Интересно, что только треть участников опроса подтвердила наличие четко определенных и прозрачных бюджетов на проекты по разработке и внедрению ИИ-агентов (табл. 4). Подавляющее большинство сталкивается с тем или иным уровнем неопределенности, что обусловлено в первую очередь новизной и сложностью технологии. Ожидается, что со временем точность и прозрачность бюджетов в российских компаниях будет увеличиваться.

Вопрос \ Шкала	1 — полностью не согласен (а)	2	3	4	5	6	7 — полностью согласен (а)
Бюджеты на проекты по ИИ в нашей компании четко определены и прозрачны	1%	0%	9%	13%	22%	24%	31%
Эффект и ROI (возврат инвестиций) ИИ-решений оценивается системно в нашей компании	2%	2%	8%	10%	20%	18%	40%
В нашей компании рассчитывается NPV (чистая приведенная стоимость) перед масштабированием решений с ИИ-агентами	4%	2%	5%	11%	19%	27%	32%
Стоимость является серьезным барьером для масштабирования ИИ в нашей компании	7%	2%	7%	12%	27%	18%	27%

Таблица 4. Распределение ответов респондентов по вопросам экономики внедрения и масштабирования

Чаще всего российские компании финансируют проекты по разработке и внедрению ИИ-агентов через централизованный ИТ-бюджет. Нередко финансирование осуществляется в рамках специального фонда инвестиций или платформенного решения. Реже всего встречается финансирование операционных расходов или вендорского контракта (рис. 4).

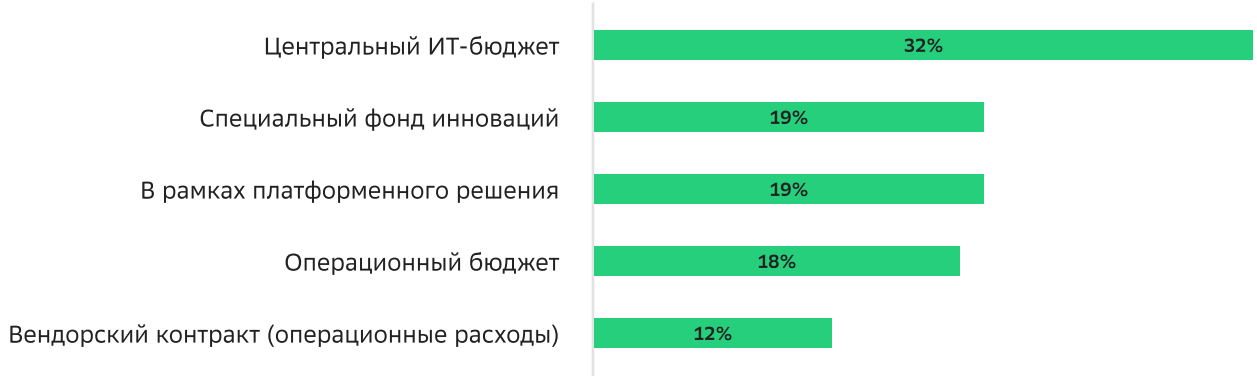


Рисунок 4. Модели финансирования проектов по разработке и внедрению ИИ-агентов в компаниях респондентов

Оценка экономического эффекта

Главным фактором успеха становится способность компании измерять влияние ИИ-агентов на бизнес-показатели. Эксперты подчеркивают важность измерения не прямого сокращения затрат, а изменений в эффективности сотрудников: продуктивность специалиста с ИИ-агентом может быть существенно выше, чем без него. В некоторых случаях значимый экономический эффект может быть достигнут за считанные дни, однако для инфраструктурных проектов характерны более длительные сроки окупаемости — обычно 5–7 лет.

Участники опроса отметили, что в их компаниях достаточно системно оценивается эффективность разработки и внедрения ИИ-агентов, а также показатель возврата инвестиций. Однако ряд респондентов отмечают, что подобная оценка в их организациях не производится системно и регулярно (см. табл. 4). Это связывается, в первую очередь, с высокой степенью неопределенности на этапах анализа, проектирования и разработки ИИ-агентов. Фактически, в некоторых случаях предварительно оценить экономический эффект и спрогнозировать ROI агентного решения не представляется возможным.

Перечень показателей, определяющих финансовую отдачу от разработки и внедрения ИИ-агентов достаточно предсказуем. Большинство российских предприятий ориентируются на пять факторов: сокращение трудозатрат, рост выручки, снижение доли ошибок и связанных с ними затрат, снижение регуляторных рисков, рост пропу-скной способности процессов. При этом чаще всего бизнес делает ставку на снижение трудозатрат, а реже — на рост пропускной способности процессов (рис. 5).

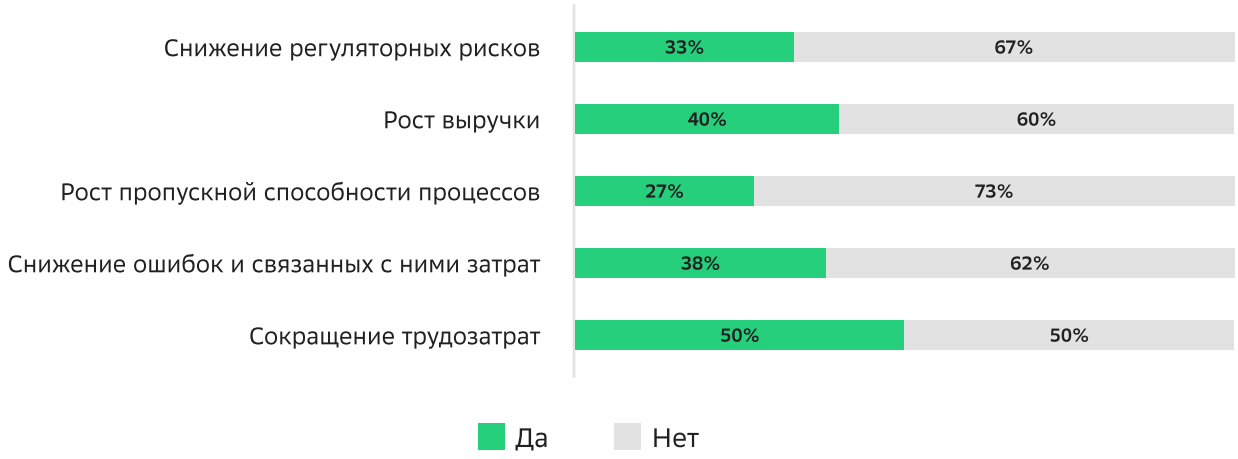


Рисунок 5. Структура финансового эффекта от внедрения ИИ-агентов в компаниях респондентов

Сроки окупаемости и возврат инвестиций

Результаты исследования свидетельствуют о широком разбросе в сроках окупаемости. Быстрые проекты (простая автоматизация, внедрение готовых решений) могут окупиться менее чем за 12 месяцев. Средние проекты с необходимостью донастройки и интеграции требуют 12–24 месяцев. Крупные инфраструктурные инициативы, связанные с созданием собственных платформ и моделей, имеют горизонт окупаемости более 24 месяцев, но часто — 5 лет и более. При этом расчет чистой приведенной стоимости (Net Present Value, NPV) перед масштабированием проводится далеко не во всех компаниях, что является серьезным организационным ограничением. Эксперты отмечают, что о реальных результатах чаще говорят, чем их показывают.

Однако чаще всего российский бизнес все-таки пытается рассчитать NPV — об этом сообщает подавляющее большинство респондентов (см. табл. 4). Полученный результат свидетельствует о достаточно высокой степени финансовой дисциплины, а также о доминировании осознанного подхода к масштабированию ИИ-решений в российских предприятиях.

Представители российских компаний не питают излишнего оптимизма по вопросам окупаемости агентных ИИ-решений, в том числе у лидеров отрасли. Наибольшее число респондентов считает, что окупаемость на временном интервале 1–2 года лежит в диапазоне 26–55%. Полученные оценки можно считать достаточно реалистичными: крайне низкое число респондентов оценило среднесрочную окупаемость как 101–199% и более 200%. Также следует принимать во внимание, что значительная доля респондентов заявляет о принципиальной невозможности оценить окупаемость агентных ИИ-решений или не представляет, как объективно ее оценить (рис. 6).

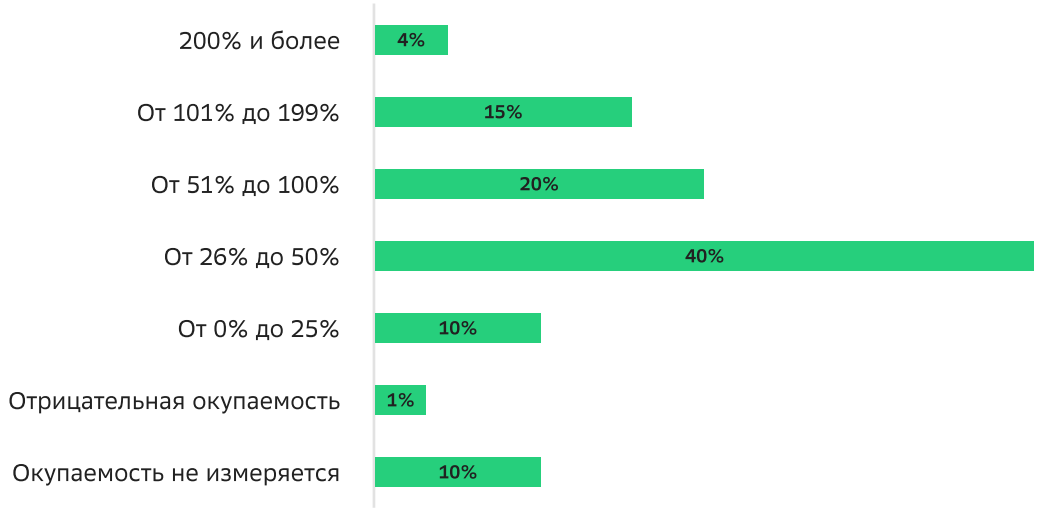


Рисунок 6. Оценка окупаемости инвестиций в ИИ-агентов за 12–24 месяца у лидеров отрасли

Барьеры при масштабировании и факторы успешного масштабирования

Масштабирование ИИ-агентов сталкивается с несколькими характерными препятствиями:

1

Отрицательной экономикой на начальном этапе — многие проекты, особенно связанные с анализом и разработкой, не окупаются в первые годы.

2

Высокой стоимостью вычислительных ресурсов и дефицитом квалифицированных кадров, которые делают масштабирование дорогостоящим.

3

Сложностью оценки эффекта в денежном выражении (особенно когда речь идет о росте качества или снижении рисков), вследствие чего финансовый эффект либо не измеряется, либо фиксируется лишь через рост производительности без прямого отражения в отчетах о прибылях и убытках.

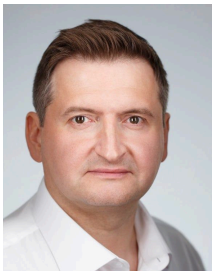
Как результат, многие компании испытывают трудности при обосновании дальнейших инвестиций перед руководством.

На основе анализа успешных кейсов были выделены несколько факторов, обеспечивающих положительную экономику внедрения:

- Четкая приоритизация процессов с измеримым эффектом: ускорение клиентского пути, снижение ошибок
- Использование итеративного подхода с быстрым запуском минимально жизнеспособных продуктов и последующим дообучением лежащих в основе моделей на реальных данных
- Применение готовых платформенных решений и открытого программного обеспечения (ПО) на начальном этапе для снижения CAPEX (аналитические материалы указывают, что использование платформенных решений позволяет снизить порог входа и ускорить получение первых результатов [17])
- Выстраивание прозрачной системы учета эффекта с фиксацией как прямой экономии, так и непрямых выгод (рост удовлетворенности клиентов, снижение регуляторных рисков и пр.). Наконец, решающе важным фактором становится поддержка со стороны руководства и готовность инвестировать в долгосрочные проекты без ожидания мгновенной окупаемости

Несмотря на то, что ИИ-агентов внедряют преимущественно финансово устойчивые компании, фактор стоимости остается одним из главных ограничений при масштабировании агентных решений (см. табл. 4). Хотя некоторые компании считают стоимостный фактор не слишком значимым, в целом влияние стоимости сложно переоценить: более ¾ респондентов оценивают важность этого фактора выше средней.

Процессная готовность и операционная модель



Александр Шевкунов
Страховой Дом ВСК

> «Основные эффекты пока наблюдаются в бэк-офисе. Простые оптимизационные задачи».

Успешное внедрение ИИ-агентов требует не только технологической базы, но и глубокой перестройки операционной модели компании. Исследование показывает, что попытки встроить агентов в неизмененные, исторически сложившиеся процессы приводят к провалу проектов или их застреванию на стадии пилотов. Ключевым фактором успеха становится способность компании переосмыслить свои бизнес-процессы с учетом воз-можностей и ограничений агентных систем. Международный опыт подтверждает сказан-ное. Согласно международным отраслевым отчетам, успешные компании перестраивают свои операционные модели под возможности агентных систем, переходя от линейных цепочек к распределенным адаптивным схемам, где агенты динамически распределяют задачи в зависимости от контекста [18].

Эксперты Билайн Big Data & AI отдельно отмечают, что если сегодня ИИ-агенты часто используются как вторая рука исполнителя-человека (т.е. действуют под его присмотром), то в будущем ИИ-агенты станут полноценными исполнителями [19]. И крайне высока вероятность того, что бизнес-процесс, оптимизированный под сотрудника-человека, не сможет считаться оптимизированным для сотрудника-агента ввиду специфики их функционирования.

Формализованность процессов

Анализ отраслевых различий демонстрирует прямую зависимость: чем выше степень формализованности процессов, тем успешнее внедрение ИИ-агентов. Финансовый сектор, где кредитование, соблюдение требований регулятора и бухгалтерские операции давно описаны в виде четких правил и процедур, демонстрирует высокую эффективность агентных систем (в отдельных случаях возможна автоматизация до 60–90% операций). В отраслях с традиционно низкой формализацией (медицина, креативные индустрии) ИИ-агенты вынуждены оставаться в роли ассистентов.

Можно констатировать следующее: прежде чем автоматизировать процесс с помощью ИИ-агента, компания должна описать его в виде формализованной, однозначно интерпретируемой схемы. Если процесс не полностью прозрачен для человека, он не будет понятным и для ИИ-агента. Опрос показывает, что российские компании предпочитают использовать ИИ-агентов в четко определенных задачах, где их применение позволит сэкономить ресурсы предприятия (табл. 5). Такому подходу привержены не все компании: на текущий момент экономический эффект и итоговая функциональность ИИ-агента могут быть недостаточно явными на ранних этапах проекта.

Вопрос \ Шкала	1 — полностью не согласен (а)	2	3	4	5	6	7 — полностью согласен (а)
ИИ применяется в четко определенных задачах, где это экономит время и ресурсы	0%	1%	6%	11%	24%	23%	35%
В нашей компании есть документированный пул кейсов использования ИИ с приоритизацией по ценности и реализуемости	2%	2%	8%	10%	20%	18%	35%
В нашей компании определены процессы, где ИИ дает наибольшую ценность	4%	2%	5%	11%	19%	27%	34%
Для пилотных проектов в нашей компании заранее устанавливаются метрики успеха и критерии масштабирования	4%	2%	5%	11%	19%	27%	38%
После завершения пилотных проектов по ИИ наша компания адаптирует и перестраивает бизнес-процессы	4%	2%	5%	11%	19%	27%	29%
Проекты по ИИ в нашей компании обычно стартуют с пилотов или ограниченных экспериментов	4%	2%	5%	11%	19%	27%	37%

Таблица 5. Распределение ответов респондентов по вопросам процессной готовности и операционной модели

База из формализованных бизнес-процессов позволяет рассматривать ИИ-агентов как один из факторов стратегического развития организации. Российские компании в целом стремятся к документированию кейсов по использованию ИИ с приоритизацией по ценности и реализуемости (см. табл. 5). Оценить же ценность и реализуемость чаще всего можно только в случае, если связанные с ИИ-решением бизнес-процессы формализованы, документированы, описаны и имеют показатели эффективности.

Идентификация процессов с наибольшей ценностью

> Экспертные интервью фиксируют, что успешные компании не пытаются автоматизировать все подряд. Они проводят системную инвентаризацию бизнес-процессов, стремясь обнаружить те из них, где внедрение ИИ-агента даст максимальный эффект. Как правило, это процессы с высоким объемом рутинных, повторяющихся операций, требующие сбора информации из множественных источников или работающие круглосуточно.

Как показали результаты опроса, все организации стремятся в той или иной степени выявлять процессы, в которых применение ИИ-агентов создает наибольшую ценность. Как показали интервью и анализ кейсов, выявление и описание таких процессов зачастую входит в проект по разработке и внедрению ИИ-агентов на начальном этапе. Тем не менее, ввиду низкой степени зрелости ИИ-агентов как технологии и низкой степени формализации процессов в ряде случаев российские компании вынуждены действовать интуитивно, в каком-то смысле — двигаться наощупь.

Российские компании стремятся обеспечивать четкое понимание будущего ИИ-агентов даже в случае, когда они разрабатываются в формате пилотных проектов (см. табл. 5). Бизнес не ограничивается определением метрик успеха в новых проектах: российские предприятия сразу стремятся выявить критерии, условия и направления роста для нового агентного решения.

Перестройка процессов под агентов

> Наиболее важным фактором становится готовность компании не просто дополнять ИИ-агентами существующие процессы, а перестраивать процессы с учетом функциональных возможностей ИИ-агентов. Эксперты подчеркивают: каждый ИИ-агент должен встраиваться в процесс и менять его итерационно. Это означает отказ от линейных, жестко заданных цепочек в пользу распределенных, адаптивных моделей бизнес-процессов, где агенты могут динамически перераспределять задачи в зависимости от контекста. Компании, достигшие успеха, используют пилоты не только для проверки технологии, но и для отработки новых операционных моделей, которые затем тиражируются.

Результаты опроса подтверждают, что добившиеся успеха в применении ИИ-агентов предприятия в целом склонны к адаптации бизнес-процессов по результатам внедрения. При этом в реальности глубина изменений бизнес-процесса зависит не только от функциональности и эффективности ИИ-агента, но и от требований регулятора, от степени формализованности и значимости бизнес-процесса и даже от бизнес-модели компании в целом (см. табл. 5).

Интервьюирование и анализ кейсов подтверждают, что чаще всего внедрение ИИ-агента приводит к необходимости изменить бизнес-процесс. Возможность автома-тизировать бизнес-процесс в текущем состоянии, без изменений, сохраняется, и после внедрения ИИ-агента его эффективность увеличится. Однако адаптация бизнес-процесса под особенности конкретного ИИ-решения позволяет добиться более впечатляющих результатов. Особенно заметным прирост результативности становится в бизнес-процессах аналитики и отчетности, которые чаще всего автоматизируются ИИ-агентами и трансформируются в зависимости от особенностей внедренного ИИ-агента (рис. 7).

Можно констатировать следующее: прежде чем автоматизировать процесс с помощью ИИ-агента, компания должна описать его в виде формализованной, однозначно интерпретируемой схемы. Если процесс не полностью прозрачен для человека, он не будет понятным и для ИИ-агента. Опрос показывает, что российские компании предпочитают использовать ИИ-агентов в четко определенных задачах, где их применение позволит сэкономить ресурсы предприятия (табл. 5). Такому подходу привержены не все компании: на текущий момент экономический эффект и итоговая функциональность ИИ-агента могут быть недостаточно явными на ранних этапах проекта.

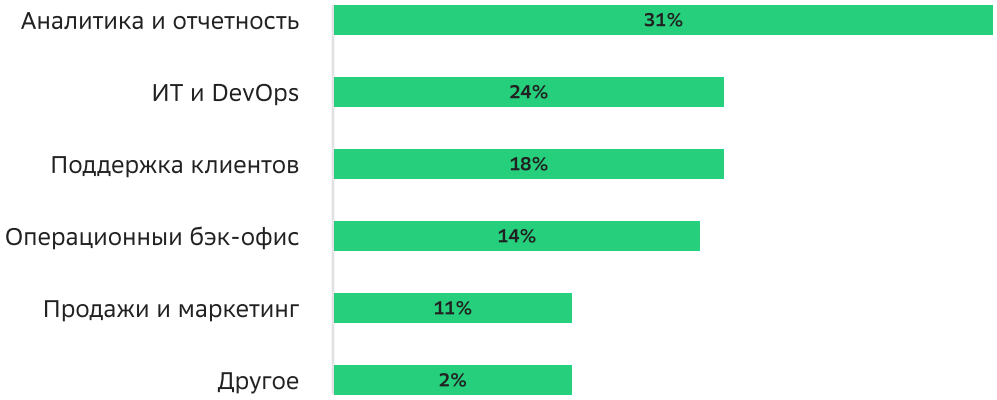


Рисунок 7. Область применения ИИ-агентов в компаниях респондентов

Гибридные операционные модели

Исследование показывает, что в большинстве отраслей полного вытеснения человека ИИ-агентами не наблюдается: вместо этого формируется симбиотическая операционная модель. В такой модели ИИ-агенты выполняют рутинные операционные задачи, а человек осуществляет стратегический надзор и принимает финальные решения в нестандартных ситуациях.

Гибридная модель проникла во все секторы. В медицине ИИ-агент анализирует данные и формирует предварительные заключения, но клиническое решение остается за врачом. В финансах ИИ-агент проверяет транзакции и выявляет подозрительные паттерны, но окончательное решение по блокировкам принимает профильный специалист. В ИТ ИИ-агент проводит диагностику и выполняет типовые восстановительные операции, но при возникновении нештатных ситуаций подключается инженер.

Фактором успеха становится осознанное проектирование таких гибридных моделей, где четко определены границы автономности ИИ-агента и случаи для обязательного вмешательства человека, что позволяет сочетать эффективность автоматизации с надежностью человеческого контроля.

Российский бизнес демонстрирует явную тенденцию к использованию гибридных операционных моделей. Подавляющее большинство участников опроса оценило степень автономности агентных ИИ-решений как среднюю, и менее 10% сообщили о наличии полностью автономных ИИ-агентов (рис. 8). В будущем вполне предсказуем рост количества ИИ-агентов с высокой степенью автономности, однако ожидать массового роста полностью автономных ИИ-агентов сегодня не приходится.

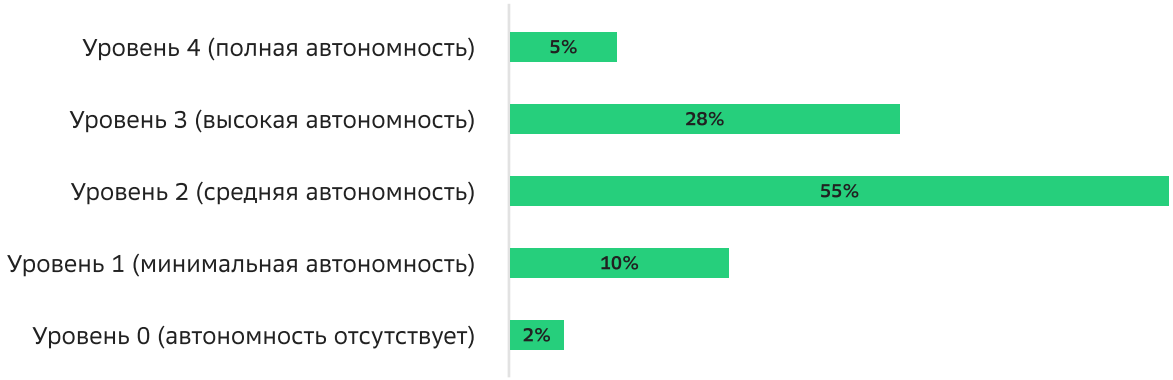


Рисунок 8. Уровни автономности ИИ-агентов в компаниях респондентов

Масштабирование и тиражирование

Переход от успешного пилота к масштабному внедрению требует наличия утвержденных подходов и стандартов. Исследование показывает, что без централизованной политики управления ИИ-агентами, единой архитектуры данных и зрелых процессов MLOps/LLMOps даже удачные пилоты не масшта-бируются. Фактором успеха часто выступает создание платформенных решений и стандартов, позволяющих масштабировать успешные практики на другие подразделения без необходимости каждый раз начинать с нуля. Компании, достигшие уровня цифровой зрелости «управляемый» и выше (см. раздел 2), обладают формализованными процессами отбора, разработки, мониторинга и поддержки агентных систем, что делает масштабирование предсказуемым и экономически оправданным.

Вопросы масштабирования и тиражирования имеют приоритетное значение для российской бизнес-практики, поскольку чаще всего проекты по разработке и внедрению ИИ-агентов зарождаются в формате пилотов или ограниченных экспериментов (см. табл. 5). Однако если не учитывать заранее возможности и потенциал для масштабирования, то проект не сможет развиваться и со временем будет прекращен по объективным организационно-экономическим причинам. Крайне редко российские организации имеют полное представление о будущем проекта в самом его начале, но крайне часто учитывают потенциальные шаги по его развитию и доступные перспективы.

ИТ-инфраструктура и эксплуатация

«Мы используем актуальные ИИ-модели в своих сервисах. Это в том числе включает постоянный процесс поддержки и развития платформ наших продуктов».

Сергей Костин
Председатель совета директоров группы .redev,
сооснователь и CEO сервиса «Курьерика»

Внедрение и последующая эксплуатация ИИ-агентов предъявляют принципиально новые требования к ИТ-инфраструктуре предприятия. В материалах Huawei подчеркивается, что реализация агентно-ориентированной модели невозможна без радикальной трансформации вычислительной инфраструктуры, включая развитие оптических, нейроморфных и квантовых вычислений для обеспечения работы миллионов ИИ-агентов [20]. А согласно техническим документам Alibaba Cloud, агентные системы должны быть по своей природе облачно-ориентированными, что обеспечивает их масштабируемость и возможность интеграции в существующие корпоративные ИТ-ландшафты без необходимости кардинальной перестройки ИТ-инфраструктуры [21].

Вопрос ИТ-инфраструктуры и вычислительных мощностей имеет критическое значение для распространения ИИ-агентов в российских компаниях. Как отмечают отдельные эксперты, на текущий момент доля ИИ-нагрузки в российских ЦОД достаточно низкая, однако в обозримом будущем на нее может прийтись до 30-40% от общей производительности аппаратного обеспечения [22]. При этом российские производители уже пытаются предложить готовые решения для корпоративного ИИ, которые включают в том числе аппаратные платформы от Yadro, Delta Computers, FPlus или R-Style [23].

Исследование показывает, что недостаточная готовность ИТ-инфраструктуры становится одним из ключевых барьеров, препятствующих успешному запуску даже пилотных проектов, не говоря уже о переходе к промышленному использованию. Устойчивое функционирование агентных систем возможно только при наличии зрелой, производительной, адаптивной и защищенной ИТ-инфраструктуры, способной обеспечить бесперебойную работу ИИ-агентов на всех этапах их жизненного цикла — от разработки до вывода из эксплуатации.

Инфраструктурная готовность

Для функционирования ИИ-агентов требуется высоко производительная ИТ-инфраструктура. Крупные игроки инвестируют в собственные вычислительные мощности и внутренние хостинги больших языковых моделей для обработки конфиденциальных данных. Другие компании полагаются на облачные решения и API-интеграции. Опыт отдельных компаний из добывающей отрасли показывает, что за время внедрения ИИ-решений потребность в аппаратном обеспечении может вырасти в 12 раз. На практике это значит, что ИТ-инфраструктура должна не просто существовать, но и обладать потенциалом для развития и масштабирования

Опрос демонстрирует высокую степень инфраструктурной готовности компаний, сумевших реально внедрить ИИ-агентов. Более четверти респондентов оценили степень готовности как максимальную, и порядка 80% суммарно оценили ее выше средней (табл. 6). Можно констатировать, что компании, не сумевшие обеспечить готовность собственной ИТ-инфраструктуры к внедрению ИИ-агентов, практически всегда оказывались неспособными их внедрить.

Вопрос \ Шкала	1 — полностью не согласен (а)	2	3	4	5	6	7 — полностью согласен (а)
Наша инфраструктура (облачная или локальная) соответствует требованиям SLA для работы ИИ-агентов	0%	0%	5%	4%	32%	30%	29%
Смена поставщика была бы затратной и сложной для нашей компании	5%	5%	6%	9%	26%	25%	24%
У каждого предварительного анализа есть назначенный ответственный представитель бизнес-подразделения, принимающий решение о масштабировании	0%	1%	1%	8%	21%	32%	37%

Таблица 6. Распределение ответов респондентов по вопросам ИТ-инфраструктуры и эксплуатации

Требования к вычислительной инфраструктуре

Для функционирования ИИ-агентов необходима ИТ-инфраструктура, обеспечивающая минимальные задержки при работе моделей, возможность оперативного дообучения и масштабируемость по мере роста числа агентов. Крупные игроки создают собственные вычислительные кластеры, позволяющие обрабатывать запросы в реальном времени и хранить большие объемы контекстных данных. Компании, не имеющие возможности развертывать собственную вычислительную базу, используют облачные платформы, однако такой подход накладывает ограничения по времени отклика и требует гарантий безопасности при передаче данных. Критическим фактором становится способность ИТ-инфраструктуры обеспечивать стабильную работу агентов в периоды пиковых нагрузок без деградации качества обслуживания.

Интеграция с существующим ИТ-ландшафтом

Критическим фактором успеха становится способность ИИ-агентов интегрироваться с текущим ИТ-ландшафтом предприятия. Эксперты отмечают, что встраивание агентов в существующий ИТ-ландшафт часто является сложнейшей задачей, которая в некоторых организациях решается на уровне принятия рисков высшим руководством. Базовые системы (ERP, CRM, платформы и пр.) должны быть достаточно интегрированы для подключения агентных решений. Одним из факторов успеха может оказаться **предварительный аудит ИТ-инфраструктуры** на предмет готов-ности к интеграции, а также планомерная модернизация устаревших компо-нентов.

Опрос позволяет косвенно оценить степень интеграции ИИ-агентов с существующим ИТ-ландшафтом, и эта степень достаточно высока (см. табл. 6). Смена поставщика или переход от ИИ-решения собственной разработки к ИИ-решению поставщика чаще всего ассоциируется с высокой сложностью и высокими затратами для бизнеса. Интервью и описание кейсов позволяют сделать вывод о том, что низкая степень интеграции ИИ-агентов наблюдается только у пилотных проектов, которые по тем или иным причинам оказались непригодными или малопривлекательными для масштабирования. В остальных же случаях степень интеграции ИИ-агента с другими ИТ-системами достаточно высока и имеет тенденцию к росту по мере его доработки и развития.

Безопасность и технологии изоляции

Поскольку ИИ-агенты получают доступ к корпоративным данным и могут инициировать действия, влияющие на бизнес-процессы, безопасность ИТ-инфраструктуры становится приоритетом. Часто российскими компаниями практикуется **запуск агентов в изолированных, контейнерных средах с ограниченным (белым) списком разрешенных команд**. В Сбере, например, параллельно с разработкой агентов создается специализи-рованная среда исполнения моделей, обеспечивающая их безопасное функционирование в защищенном контуре. Все действия ИИ-агентов подлежат обязательному логированию для последующего аудита и рассле-дования инцидентов. Такой подход позволяет минимизировать риски несанкционированных или ошибочных действий.

Следует четко понимать, проблемы безопасности более чем реальны. Российские компании, использующие ИИ-агентов, регулярно сталкиваются с ними. Опрос показал, что порядка 40% организаций в течение последнего года сталкивались с необходимостью отключить часть функций ИИ-агента или откатить его до предыдущей версии из-за проблем с безопасностью, а 31% организаций столкнулись с инцидентами в области безопасности из-за действий ИИ-агентов, которые потребовали оперативной реакции (рис. 10).

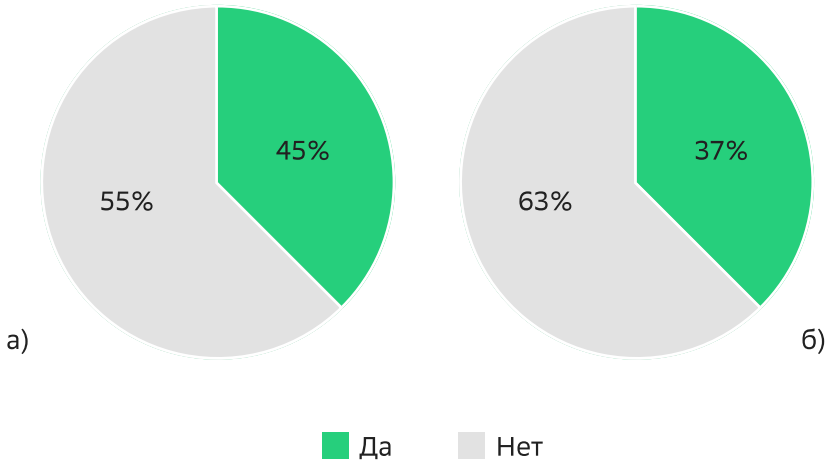


Рисунок 10. Доля компаний, которые столкнулись с проблемами в области безопасности при использовании ИИ-агентов: а — сталкивались с необходимостью отключить часть функций ИИ-агента или откатить версию; б — сталкивались с инцидентами в области безопасности

Наблюдаемость и мониторинг

Эксплуатация агентных систем требует принципиально иных подходов к мониторингу по сравнению с алгоритмическим ПО. Недостаточно отслеживать доступность сервиса — необходимо контролировать качество принимаемых ИИ-агентами решений, выявлять аномалии в их поведении и своевременно обнаруживать деградацию моделей. Компании с высоким уровнем зрелости внедряют системы непрерывного мониторинга качества ИИ-агентов, включающие отслеживание точности ответов, частоты ошибок и необходимости ручного вмешательства. Регулярное тестирование агентов на нестандартные сценарии и атаки становится обязательной практикой.

В качестве фактора успеха может быть названо выстраивание многоуровневой системы мониторинга, позволяющей не только фиксировать сбои, но и прогнозировать потенциальные проблемы до того, как они возникнут и повлияют на бизнес-процессы.

Опрос показал, что практически треть компаний вынуждена вручную отменять 5–10% действий ИИ-агентов, а сотрудники каждого десятого предприятия и вовсе вручную отменяют более 10% действий ИИ-агентов (рис. 11). Доля компаний, которая не сталкивается с необходимостью отменять действия ИИ-агентов, исчезающе мала. Этот факт делает обязательным условием разработку инструментов и внедрение процессов, которые обес-печат наблюдаемость и мониторинг используемых ИИ-агентов.

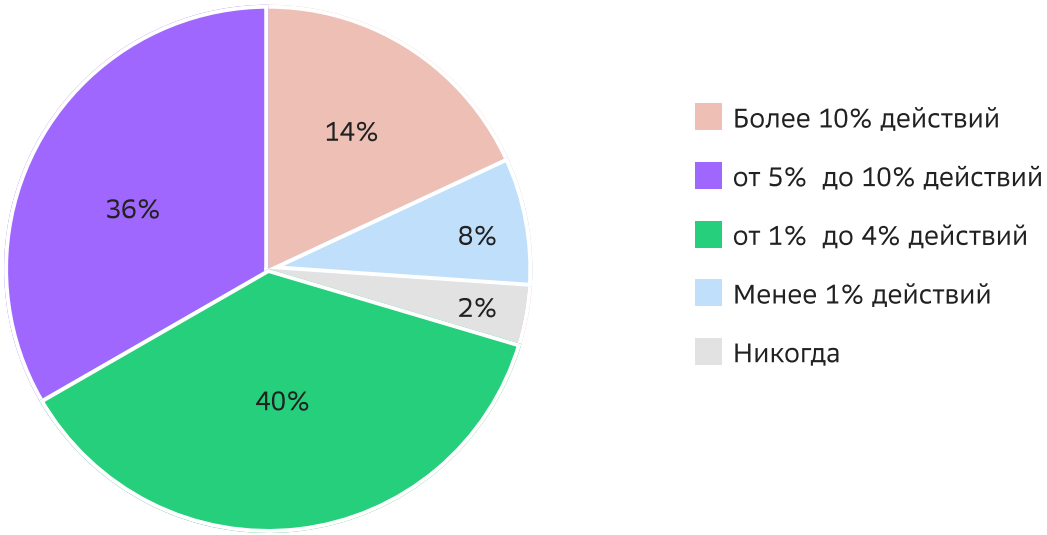


Рисунок 11. Частота ручных исправлений действий ИИ-агентов в компаниях респондентов

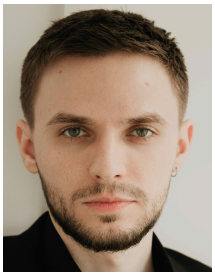
Управление жизненным циклом

Масштабная эксплуатация ИИ-агентов требует формализованных процессов управления их жизненным циклом. Это включает процедуры запуска новых версий, отката при возникновении проблем, A/B-тестирования изменений и планового вывода устаревших ИИ-агентов из эксплуатации. Компании, достигшие уровня «управляемый» в модели зрелости, обладают устойчивыми процессами MLOps/LLMOps, автоматизирующими развертывание, мониторинг и обновление агентных систем.

Ключевым фактором успеха становится переход от ручного управления ИИ-агентами к платформенным решениям, обеспечивающим стандартизиро-ванное развертывание, контроль версий и централизованное управление политиками доступа и безопасности.

Помимо стандартных практик управления жизненным циклом информационных систем российские организации используют инструменты, которые позволяют вовлечь в управление жизненным циклом ИТ-систем представителей бизнеса. Российский бизнес стремится выделить отдельную роль ответственного предс-тавителя бизнес-подразделения, принимающего решение о масштабировании. Это позволяет отсеивать проекты по разработке и внедрению ИИ-агентов, которые не соответствуют бизнес-целям (см. табл. 6).

Риски, безопасность и соответствие требованиям законодательства



Марк Маджидов
Ранее – Сбер, EdTech

> «Из опыта работы в Сбере могу сказать, что пользовательские данные и кибербезопасность там очень сильно влияют, особенно при сборке наборов данных. Это дополнительная надстройка, время и вычислительный ресурс».

Согласно международным исследованиям, требования регуляторов могут существенно ограничивать развитие ИИ-агентов. Так, регуляторные требования в сфере здравоохранения ограничивают автономность ИИ-агентов, допуская их использование только в ассистирующем режиме с сохранением окончательного решения за человеком [24]. В зарубежной практике также особое внимание уделяется вопросам кибербезопасности при внедрении агентных систем: международные стандарты требуют внедрения механизмов аутентификации и аудита, обеспечивающих прозрачность действий агентов [25].

Российские эксперты отмечают, что действующее законодательство не рассматривает искусственный интеллект в качестве самостоятельного субъекта права. При использовании автономных ИИ-систем ответственность за их действия, вероятнее всего, будет возложена на оператора — компанию, которая внедрила технологию. В ряде случаев суды могут применять принцип ответственности за источник повышенной опасности (статья 1079 ГК РФ).

Особое внимание бизнесу необходимо уделить соблюдению Феде-рального закона №152-ФЗ «О персональных данных»: ИИ-агенты, имеющие доступ к файловой системе и интернету, могут непреднамеренно нарушить требования по обработке и трансграничной передаче данных. Для снижения рисков эксперты рекомендуют использовать платформы с функцией полного логирования действий агента, механизмами анонимизации данных, а также рассмотреть возможность участия в Экспериментальных Правовых Режимах («регуляторных песочницах»), которые позволяют тестировать технологии с временным отступлением от действующих норм [26].

Исследование показывает, что недостаточное внимание к вопросам риска, безопасности и соответствию законодательству становится причиной приостановки значительной доли проектов или их застревания на пилотной стадии. Успешное внедрение агентных систем возможно только при наличии или параллельном выстраивании комплексной системы управления рисками, охватывающей технические, организационные и регуляторные аспекты.

Типология рисков

Экспертные интервью и аналитические материалы фиксируют широкий спектр рисков, связанных с эксплуатацией ИИ-агентов:

- **Технологические риски** включают галлюцинации больших языковых моделей, частые ошибки, требующие саморефлексии или проверки другими ИИ-агентами, а также сложность интеграции с унаследованными системами.
- **Риски кибербезопасности** связаны с увеличением поверхности атаки: ИИ-агенты, имеющие доступ к инструментам и API, становятся потенциальной целью для злоумышленников, которые могут пытаться манипулировать моделью, подменять данные или использовать ИИ-агента как точку проникновения в ИТ-инфраструктуру.
- **Организационные риски** включают сопротивление сотрудников, неготовность бизнес-заказчиков правильно формулировать задачи и отсутствие внутренней экспертизы.
- **Особую категорию** составляют регуляторные риски, связанные с неопределенностью нормативной базы и требованиями отраслевого законодательства.

Изоляция ИИ-агентов позволяет значительно снизить влияние на непрерывность бизнес-процессов большинства категорий рисков. Это делает критически важными требованиями при разработке ИИ-агентов требования к обеспечению безопасности их исполнения. Также рекомендуется формировать требования к прослеживаемости данных. Порядка 85% респон-дентов считают важность прослеживаемости данных выше средней, причем более четверти респондентов считают ее критической. Организации, которые не придают значения прослеживаемости данных, практически отсутствуют (табл. 7).

Вопрос \ Шкала	1 — полностью не согласен (а)	2	3	4	5	6	7 — полностью согласен (а)
В нашей компании поддерживается прослеживаемость данных для агентных решений	0%	2%	0%	13%	25%	32%	28%
Мы осведомлены о регулировании и правилах, которые влияют на применение ИИ в нашей отрасли	1%	0%	8%	7%	24%	22%	38%
Мы ощущаем давление со стороны регуляторов и стандартов по соблюдению требований к использованию ИИ	6%	2%	7%	9%	27%	26%	23%
Чувствительность данных (персональные данные, требования комплаенса) ограничивает или замедляет внедрение ИИ-агентов в нашей компании	8%	1%	4%	10%	26%	26%	25%
Политики использования ИИ документированы и соблюдаются в нашей компании	3%	3%	5%	11%	16%	26%	36%

Таблица 7. Распределение ответов респондентов по вопросам рисков, безопасности и соответствия требованиям законодательства

Регуляторные ограничения

> Отраслевая специфика налагает существенные ограничения на автономность агентов. В финансовом секторе требования Центрального Банка РФ и регуляторов других стран обязывают сохранять человека в контуре принятия решений, обеспечивать объяснимость действий ИИ-агентов и возможность полного аудита. В здравоохранении автономные диагностические решения запрещены или строго ограничены: ИИ-агент может анализировать данные и предлагать решения, но окончательное клиническое решение остается за врачом. В телекоммуникации использование реальных данных для обучения ограничено законодательством, что вынуждает применять синтетические данные. В подобных условиях фактором успеха становится заблаговременный аудит регуляторных требований и встраивание контроля за соблюдением требований законодательства в архитектуру агентных систем еще на этапе проектирования, а не после возникновения инцидентов.

В целом ограничения регуляторов являются краеугольным камнем, от которых зависит развитие решений на базе ИИ внутри компании. Как уточнялось ранее, именно фактор безопасности и соответствия требованиям регулятора занимает первое место при выборе поставщика или при принятии решения о внутренней разработке. Однако данные опроса (см. табл. 7) свидетельствуют о том, что требования регулятора все еще нельзя назвать абсолютно понятными и прозрачными для российского бизнеса. Можно констатировать, что бизнес понимает отдельные и наиболее важные ограничения, однако многие из них по-прежнему обсуждаются или требуют более детальное проработки.

При этом говорить о жестком давлении со стороны регулятора не приходится. Ощутимая доля респондентов (см. табл. 7) заявила о том, что не наблюдает значимого давления со стороны регуляторов или стандартов по соблюдению требований в сфере применения ИИ. С другой стороны, организации, которые работают с чувствительными и персональными данными, сталкиваются с подобным давлением относительно часто. Ожидается, что в будущем давление со стороны регулятора будет усиливаться, однако прежде будет производиться расширение и уточнение соответствующей нормативно-правовой базы.

Чувствительные данные и комплаенс

> Особую сложность представляют вопросы работы с персональными данными и соблюдения требований законодательства. В финансовом секторе доступ к клиентским данным требует отдельных протоколов интеграции и строгих мер безопасности. Используются различные подходы к анонимизации: заключение пользовательских соглашений, анонимизация на этапе дообучения, замещение информации на смежную, шифрование. Для крупных технологических компаний сохранность персональных данных и невозможность их передачи вовне становится ключевым фактором, стимулирующим переход от покупки готовых решений к собственной разработке. Опасения, что функциональность ИИ-агента может быть отключена внешним поставщиком, также усиливают тренд на создание автономных независимых инфраструктурных решений.

Интересно, что существует небольшая, но все-таки заметная доля компаний, на проекты по внедрению ИИ-агентов которых практически не влияет чувствительность данных (см. табл. 7). Заметное количество организаций также оценивает влияние чувствительности данных ниже среднего. Однако чаще всего чувствительность данных все-таки становится существенным препятствием для разработки и внедрения ИИ-агентов, о чем заявляют порядка ¾ участников опроса.

Организационные практики управления рисками

> Помимо технических средств, компании выстраивают организационные механизмы контроля. Практикуется постепенная передача ответственности от человека к ИИ-агенту: сначала ИИ-агент работает под полным контролем человека, затем автономность агента постепенно увеличивается по мере накопления статистики в случае безошибочной работы. Важным элементом становится регулярное тестирование агентов на нестандартные сценарии и атаки. В Сбере, например, если в ходе тестирования находят уязвимости, которые могут создать риски для бренда, ИИ-агент отзывается на доработку. Культура безопасности, включающая обучение сотрудников основам работы с ИИ и механизмам выявления ошибок, становится неотъемлемой частью корпоративной практики. Как отмечают эксперты, любая промежуточная точка в действиях ИИ-агента должна фиксироваться, а любые его действия — быть объяснимыми и проверяемыми.

Одна из важнейших организационных практик управления рисками — это **документирование и соблюдение политик использования ИИ-агентов**. Российские компании, сумевшие внедрить в свою деятельность ИИ-агентов, в целом сообщают о достаточно высокой степени внедрения политик использования агентных решений (см. табл. 7). При этом в некоторых областях документированные политики являются избыточными: порядка 1/5 респондентов заявили о средней и низкой интенсивности документирования и соблюдения политик использования ИИ-агентов.

Российские компании, которые выполняют мониторинг качества работы ИИ-агентов, чаще всего делают это ежедневно. Небольшая доля организаций осуществляет мониторинг непрерывно. Сопоставимая доля российских компаний мониторит качество моделей и ИИ-агентов только по мере возникновения инцидентов (рис. 12).

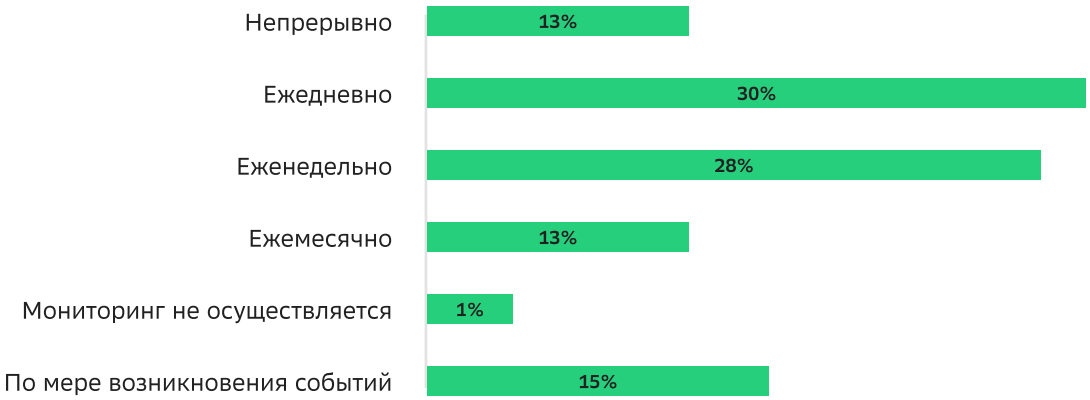


Рисунок 12. Частота мониторинга качества моделей и ИИ-агентов в компаниях респондентов

Однако следует учитывать, что регулярный мониторинг требует значительных финансовых затрат и соответствующих компетенций, поэтому многие организации осуществляют мониторинг не так часто, как того требует качество выполнения бизнес-процессов. По мере появления на рынке автоматизированных средств мониторинга качества ИИ-агентов ситуация будет меняться, и компании будут переходить к непрерывному мониторингу.

Список использованных источников

1. Кречатова А. Эксперты Axenix и МГУ оценили эффекты внедрения бизнесом ИИ-агентов, forbes.ru
2. ИИ-агенты: обзор мирового и российского рынков, memory.mts.ru
3. Cloudera. The Future of Enterprise AI Agents. USA: Cloudera Inc., cloudera.com
4. McKinsey & Company. The State of AI in 2025: Reaching Operational Scale. New York: McKinsey Global Institute, mckinsey.com
5. Gartner Research. Forecast: Adoption and Failure Rates of Agentic AI Systems, 2025–2030, gartner.com
6. Deloitte Insights. Autonomous Generative AI Agents: Still Under Development. Deloitte, 2025, deloitte.com
7. Исследование: ИИ-ассистентов и ИИ-агентов используют уже 39% российских компаний, sberanalytics.ru
8. IBM Research. The 2025 Guide to AI Agents: Architectures, Governance and Applications. Armonk: IBM Press, ibm.com
9. ИИ-агенты — не для всех: почему бизнесу рано перестраиваться, companies.rbc.ru
10. CNewsMarket опубликовал первый рейтинг российских ИИ-агентов, cnews.ru
11. Tencent Cloud. 智能体开发平台官方文档, cloud.tencent.com
12. Alibaba Cloud. Artificial Intelligence Solutions, alibabacloud.com
13. ETSI. Security Architecture for AI-Enabled Network Functions, etsi.org
14. 42% россиян доверяют ответам нейросетей в поисковиках, companies.rbc.ru
15. Reuters. Over 40% of Agentic AI Projects Will Be Scrapped by 2027, Gartner Says, reuters.com
16. Злобин А. Экономический эффект от ИИ в России может к 2030 году превысить 7,9 трлн рублей, forbes.ru

17 Multimodal.dev. 17 Useful AI Agent Case Studies. Multimodal Research Group, multimodal.dev

18 Eastgate Software. Multi-Agent AI Systems: Frameworks, Use Cases & Trends 2025, eastgate-software.com

19 Билайн назвал главные тренды развития ИИ-агентов в России. РИА Новости, ria.ru

20 Huawei Technologies Co., Ltd. 智能世界2035, huawei.com

21 Alibaba Cloud. Artificial Intelligence Solutions, alibabacloud.com

22 Гонка гиперскейлеров. Коммерсантъ Технологии, kommersant.ru

23 Андриянова А. Битва за железо: как российский бизнес выстраивает ИИ-инфраструктуру в условиях нехватки чипов, computerra.ru

24 ScienceDirect / Elsevier. Next-generation Agentic AI for Transforming Healthcare. Journal of Medical Systems, sciencedirect.com

25 3GPP. Study on Management and Security of AI/ML in 5G Systems (TR 23.700). 3GPP, 3gpp.org

26 ИИ-агенты: правовой вакуум, ФЗ-152 и ответственность бизнеса в РФ. РБК Компании, companies.rbc.ru