сенсус

ЦИФРОВОЙ МАРКЕТПЛЕЙС

Цифровые решения – 2026 · аналитика по направлениям

Искусственный интеллект: от доступа к моделям – к экономике процесса

Как на форуме «Цифровые решения – 2026» обсуждали переход от пилотов ИИ к корпоративным системам: эффект и стоимость токенов, ответственность за агентов, суверенные модели, ЦОДы и закон об ИИ – с цифрами компаний.

Содержание

Ключевые показатели

Кратко

1. От пилотов к корпоративной системе

2. ИИ-агенты: экономика делегирования и контроль

3. Эффект: промышленность, телеком и разработка

4. Токены и окупаемость

5. Суверенные модели и инфраструктура

6. Регулирование ИИ

7. Безопасность ИИ: суверенная не значит безопасная

8. ИИ в госуправлении и городе

9. ИИ в торговле: где помощь становится подменой выбора

10. Барьеры и предложения

11. Ключевые игроки темы

Выводы

Источники

Ключевые показатели

порядка 10 млрд руб. в год

Эффект ИИ на обогатительных фабриках

Тестин Алексей, «Норникель»

3 млрд руб.

Эффект ИИ в контакт-центре МТС за прошлый год

Филиппов Денис, MWS AI

400%

Рост операций закупочного органа при росте штата на 4%

Гаранин Евгений, Росатом; за год

в 3 раза выше

Подтверждённый эффект ИИ к инвестициям

Кутузов Станислав, Банк «Санкт-Петербург»

1,1–1,2 млрд руб.

Годовой эффект Нейрошлюза от роста производительности

Халитов Дарий, Ростелеком; оценка

9 200

ИИ-агентов создали сотрудники Ростелекома за год

Халитов Дарий, Ростелеком

70%

Процессы, где агентная автоматизация не окупается

Щербаков Виталий, МегаФон; по итогам анализа процессов

более 600

Доступы к ИИ-инструментам в НЛМК, не давшие эффекта

Долгов Александр, НЛМК; выданы в 2024 году

более 75%

Инженеры Яндекса, использующие агентскую разработку

Атрепьев Григорий, Yandex Cloud

до 5 раз

Разброс расхода токенов на одну и ту же задачу

Фетисов Алексей, Альфа-Банк

4–8 месяцев

Отставание российских моделей от открытых зарубежных

Алутин Игорь, Московская биржа; оценка

менее 10 из более 130

Проекты ЦОДов, получившие возможность реализации

Степанов Константин, РТК-ЦОД; оценка

8–12 трлн руб.

Потенциальный эффект ИИ к 2030 году

Титов Виталий, «Яков и Партнёры»; прогноз

6

Постановления правительства в развитие закона об ИИ

Лебедев Иван, Минцифры России; по план-графику

11%

Рост загрузки самосвалов с компьютерным зрением

Желтухин Вадим, «Алроса»

96%

Москвичи, пользовавшиеся ИИ-сервисами за последний год

Корчежинская Софья, ДИТ Москвы; исследование

Кратко

На форуме «Цифровые решения – 2026» ИИ обсуждали как производственный инструмент: вопрос «внедрять ли» участники считали закрытым. Спорили о том, как превратить личное использование моделей в корпоративную систему, как считать эффект, кто отвечает за действия агентов и сколько суверенности нужно заказчику. Обзор опирается на 24 сессии с участием Яндекса, Сбера, Ростелекома, Билайна, НЛМК, «Норникеля», Росатома, Минцифры России и других организаций.

Главные выводы. Раздача доступов сама эффекта не даёт: НЛМК выдал более 600 доступов и получил только рост затрат (Долгов Александр, НЛМК). Крупнейший подтверждённый результат показала промышленность – порядка 10 млрд руб. в год на фабриках «Норникеля» (Тестин Алексей, «Норникель»). Токены стали статьёй бюджета: расход на одну и ту же задачу различается до 5 раз (Фетисов Алексей, Альфа-Банк). Инфраструктура ограничена: из более 130 проектов ЦОДов реализуемы менее 10 (Степанов Константин, РТК-ЦОД).

1. От пилотов к корпоративной системе

1.1 Массовый доступ или платформа: спор о методе

Главная развилка корпоративного внедрения – с чего начинать: с массового доступа сотрудников к моделям или с единой платформы. Александр Долгов (НЛМК) описал провал модели «раздать всем инструменты»: в 2024 году компания выдала более 600 доступов к ИИ-инструментам и не получила эффекта, кроме роста затрат. Перелом дала собственная агентная платформа, на которую перевели весь цикл разработки. Теперь крупный проект ведут 2–3 соло-инженера и 25–30 параллельно работающих агентов; e-commerce-систему компания переписывает силами 2 соло-инженеров при заявленной стоимости 50 млн руб. и сроке 7 месяцев. Цель – снизить себестоимость поставки ИТ-решений в 10 раз (Долгов Александр, НЛМК).

> Я выдал более 600 доступов всем сотрудникам. И единственный эффект, который получили – это рост затрат. Другого эффекта не было вообще. – Александр Долгов, НЛМК

Станислав Кутузов (Банк «Санкт-Петербург») возразил: когда доступ получили все сотрудники, они принесли кейсы, которые команда не могла придумать сама. Подтверждённый финансовой службой эффект в банке в 3 раза превышает инвестиции, на этап промышленного использования выходят более 130 ИИ-проектов. В первом квартале банк рассчитывает привлечь первую 1 000 цифровых сотрудников на агентной платформе. Само внедрение Кутузов считает прежде всего культурным сдвигом: «Мы верим в то, что это больше про смену культуры».

Компромиссную схему показал Росатом. Требования информационной безопасности, выбор платформы и оркестратора стандартизированы централизованно, а идеи прикладных задач поступают из подразделений и заводов через конвейер гипотез, рассказала Заяна Ачинова («Гринатом»). На 2027 год Росатом ставит цель сократить сроки разработки на 40% с помощью ИИ (Ачинова Заяна, «Гринатом»). Билайн выбрал похожую модель: конструктор агентов, среда разработки и каталог MCP-серверов, а обмен агентами поощряется корпоративными баллами (Оганесян Ашот, Билайн).

1.2 Теневой ИИ и конкуренция с внешними сервисами

Корпоративные спикеры признали, что внутренние ИТ-службы конкурируют с внешними ИИ-подписками по скорости и удобству. Вадим Желтухин («Алроса») описал, как без корпоративного доступа сотрудники фотографируют рабочие документы и отправляют их во внешние модели. Владимир Нелюб («Группа Астра») назвал личные аккаунты неконтролируемым каналом утечки данных. Ответ, на котором сошлись спикеры: не запрещать, а давать доверенные инструменты с сопоставимым пользовательским опытом. Сергей Карпович (Т1) предупредил, что чрезмерно сложные ограничения безопасности сами вытесняют сотрудников во внешние сервисы. Ашот Оганесян (Билайн) сформулировал это так: «Самое главное, чем может конкурировать корпоративный ИИ с некорпоративным – это просто интеграции».

У Билайна опыт показал и обратную сторону массового доступа: после перегрузки серверов большой моделью компания перешла к лимитам потребления, а ночью лимиты ослабляют, чтобы равномернее загружать мощности. Оганесян ожидает, что объём доступных токенов станет частью предложения работодателя сотруднику.

1.3 Данные, процессы и люди как предпосылка

Вторая линия – готовность самой организации. Сергей Голицын (Т1) назвал базовым критерием готовности наличие оцифрованных данных и предупредил, что пилот может прекратиться после ухода единственного энтузиаста. Карен Казарян (АНО «Цифровая экономика») привёл проект с медицинскими данными, где существующие записи оказались непригодны для ИИ и сбор пришлось выстраивать заново. По его словам, «если не структурируются данные и не сохраняется институциональное знание в организации, то никакая ИИ-шка не поможет». Участники той же дискуссии призвали до внедрения проводить аудит процессов: где-то достаточно базовой автоматизации.

Отдельно обсуждали людей. Ачинова отметила страх замены на производственных площадках, Анна Петухова («Семантика») – саботаж на местах без предварительного вовлечения сотрудников. Петухова выступила против увольнения младших специалистов: без них компания лишится будущих сотрудников среднего и старшего уровня. Виталий Щербаков (МегаФон) напомнил, что ответственность за качество процесса с ИИ должна оставаться у бизнес-руководителя, а не перекладываться на ИТ.

2. ИИ-агенты: экономика делегирования и контроль

2.1 Агент как новый канал продаж

Агенты меняют отношения компании с клиентом: они сами становятся покупателями и пользователями сервисов. Игорь Алутин (Московская биржа) рассказал об эксперименте, в котором управляющая компания из агентов создала индекс и объясняет инвестиционные рекомендации; всего агенты выполнили 17 000 операций. На «Финуслугах» реализован MCP-доступ, позволяющий агенту открыть счёт в финансовой организации. Биржа тестирует собственный MCP данных и призывает компании адаптировать сайты под агентов (Алутин Игорь, Московская биржа). Свою позицию Алутин сформулировал коротко: «Если тебя не будет видеть поисковик именно агентный, да, то тебя просто нет на этом рынке».

«ВкусВилл» через MCP позволяет агенту подбирать продуктовую корзину с учётом состава питания, а в следующем релизе добавит персонализацию и безопасную оплату. Компания ожидает около 5% транзакций через агентный канал на старте и 13–15% в течение 3 лет, сообщил Александр Абрамов («ВкусВилл»). Никита Старичков («1С») обозначил ограничение: заказчику нужна запись и автоматизация бизнес-процессов, а не только чтение данных, при этом не все коннекторы к решениям «1С» поддерживают запись. Голицын предложил рассмотреть наличие MCP как обязательный критерий включения решений в реестр ПО.

2.2 Ответственность и границы автономии

Ответственность за действия агента участники оставляют за компанией и человеком. Михаил Мишустин (Правительство России) призвал государство и бизнес вместе определить границы полномочий и ответственности агентов, чтобы обеспечить предсказуемую работу экосистем. Абрамов привёл пример ошибочного продуктового заказа, за который перед клиентом отвечает компания, и выступил против правосубъектности агентов: «Невозможно всё списать на машину». Голицын предложил связывать права агента с правами сотрудника, функцию которого он выполняет. Сергей Анохин (Билайн) предложил паспорт агента, фиксирующий создателя и ответственного, Алутин – реестр агентных сделок, доступный человеку.

> Описать, кто где, на каком этапе несёт ответственность, как это регулируется и где сделки будут записываться – это вот сейчас самое важное. – Игорь Алутин, Московская биржа

Автономность предлагают расширять постепенно. Дмитрий Никишов (Банк ДОМ.РФ) считает, что агенту в кредитном процессе можно поручить сбор данных, но решение об изменении условий клиента следует оставлять человеку. Т1 при внедрении агентов-андеррайтеров сохраняет участие человека: агент готовит решение для кредитного комитета (Голицын Сергей, Т1). Щербаков предлагает до запуска оценивать в деньгах

наихудший ущерб и масштаб распространения ошибки. Новый вопрос поднял Константин Куликов (Альфа-Банк): кому принадлежат агенты, созданные сотрудником на собственном оборудовании, и что с ними происходит при увольнении автора.

2.3 Защитная обвязка агента

Практики безопасности агентов подробно описала «Лаборатория Касперского». Для облачных агентов разработки компания внедрила отдельные учётные записи с ограниченными правами, песочницу и шлюз фильтрации запросов и ответов, рассказал Александр Лискин («Лаборатория Касперского»). Модель при проектировании защиты он предложил считать недоверенным вероятностным ядром. Анна Кулашова («Лаборатория Касперского») добавила, что агентам нужны идентичности и привилегии с контролем их повышения и отзывом прав. По данным исследования компании, около 38% российских компаний активно разрабатывают и используют ИИ-решения для внутренних процессов, а зрелость процессов ИБ за этим не успевает (Кулашова Анна, «Лаборатория Касперского»). Запреты Кулашова считает бесполезными, «потому что тогда появляется теневой искусственный интеллект».

Юрий Максимов (Positive Technologies) описал полигон, где человеку предлагают 100 млн руб., если он заставит агента выйти за пределы порученной задачи. Никишов отметил, что успешной аттестации систем с агентами в его опыте пока не встречалось.

3. Эффект: промышленность, телеком и разработка

3.1 Промышленность и телеком: подтверждённые результаты

Наиболее конкретные цифры эффекта прозвучали от промышленных компаний. Алексей Тестин («Норникель») сообщил, что обогатительные фабрики находятся под управлением ИИ несколько лет, а эффект составляет порядка 10 млрд руб. в год. ИИ при этом работает надстройкой над АСУ ТП в физически изолированной сети, а несогласие оператора разбирают и используют для обучения системы. Внедрение Тестин предложил оценивать по трём ступеням: «Первая ступень – это искусственный интеллект видит, вторая ступень – это он советует, и третья управляет».

«Алроса» с помощью компьютерного зрения контролирует загрузку самосвалов и получила рост загрузки техники на 11% (Желтухин Вадим, «Алроса»). В закупочном процессе Росатома после применения ИИ объём операций уполномоченного органа за год вырос на 400%, а численность – на 4%, сообщил Евгений Гаранин (Росатом). СИБУР применяет агента для микроаукционов, дающих дополнительную скидку в несколько процентов, рассказал Денис Юдаков (СИБУР). НЛМК полностью переписал участок MES-системы на собственной агентной платформе и внедрил его в цехах (Долгов Александр, НЛМК).

В телекоме эффекты измеряют масштабом. В Т-Мобайл 99% мошеннических звонков не доходят до абонентов, их среднемесячное число снизилось с примерно 65 млн до 45 млн, сообщил Антон Никольский-Волконский (Т-Мобайл). ИИ-инженер Билайна с начала года

обработал порядка 570 000 событий, 28% из них – без участия человека (Анохин Сергей, Билайн). База пользователей ИИ-продуктов МТС для звонков с начала года выросла в 4 раза, по словам Андрея Бийчука (МТС). Денис Филиппов (MWS AI) оценил эффект ИИ в контакт-центре МТС за прошлый год в 3 млрд руб.; проект охватывает более 400 сценариев обслуживания при нагрузке 6 млн звонков в месяц, а в развитие своей ИИ-платформы MWS AI инвестирует более 1,5 млрд руб. в год.

3.2 Агентная разработка: скорость кода не равна ценности

Доля кода, написанного с помощью ИИ, стала популярным показателем, но ряд спикеров поставил под сомнение саму метрику. В НЛМК с помощью ИИ пишется 30% кода (Долгов Александр, НЛМК). В Яндексе более 75% инженеров регулярно используют агентскую разработку, и с ней создаётся более 75% кода в изменениях, сообщил Григорий Атрепьев (Yandex Cloud). В Сбере у отдельных команд объём генерируемого кода вырос в 8–10 раз, рассказал Рафаел Тонаканян (Сбер). В Yandex Cloud агентная система анализа кода ускорила аудиты безопасности в 6 раз (Сидоров Евгений, Yandex Cloud).

Сергей Висленев (РЖД) сослался на исследование, по которому 30% действий разработчиков с агентами относятся к работе, которую без агентов они не выполняют вовсе. Изменения кода могут не пройти слияние и не дойти до заказчика. Игорь Маслов (Т-Банк) признал, что массовое применение ИИ для кода пока не дало банку значимого общего прироста эффективности. Антон Шмаков («Группа Астра») предложил измерять принятую заказчиком функциональность и релизы. Нелюб привёл оценку: точечное внедрение повышает производительность конвейера разработки не более чем на 5%, методологический подход – около 50%.

> Невозможно не применять агентную разработку в 2026 году, даже не потому, что без этого вы не получаете прирост производительности, а потому, что ваши сотрудники считают вас динозаврами и не хотят у вас работать. – Сергей Висленев, РЖД

Кирилл Меньшов (Сбер) объяснил разброс отчётов об ускорении «перекрёстками» – взаимодействием команд в крупном enterprise. Для выравнивания практик создан Совет по генеративной разработке: в него вошли около 30 компаний, у Совета 5 ключевых направлений, включая токеномику и оптимизацию инференса (Меньшов Кирилл, Сбер). Будущее ручного программирования Меньшов оценил жёстко: «Вручную кодирующие программисты будут выглядеть примерно так же, как сейчас протыкающие дырки в перфокартах».

4. Токены и окупаемость

4.1 Токены как статья расходов

Стоимость вычислений перестала быть технической деталью и встала в один ряд с затратами на персонал. Атрепьев сообщил, что в Яндексе бюджет на токены рассматривают вместе с бюджетом на персонал: «Для нас это теперь уже одна строка: условно говоря, фонд оплаты труда и токены». Желтухин предложил тот же подход финансовым службам: затраты на персонал и токены – единая стоимость ресурсов для получения бизнес-эффекта.

Именно на этом уровне видны риски. Алексей Фетисов (Альфа-Банк) сообщил, что расход токенов агентами на одну и ту же задачу различается до 5 раз, что ломает бюджетный цикл; группа по токеномике до конца года подготовит 2 блюпринта – по оценке стоимости генеративной разработки и по экономике эксплуатации. Алексей Макин (Red_mad_robot) констатировал, что большая часть бизнес-кейсов ИИ в разработке при подсчёте экономики оказывается убыточной. Во «ВкусВилле» расходы на ИИ-подписки одного разработчика оказались сопоставимы с затратами ещё на одного разработчика; при этом агенты в аналитике сократили срок принятия решений с 3 недель до 1 недели (Абрамов Александр, «ВкусВилл»).

4.2 От эффекта к финансовому результату

Массовость внедрения не гарантирует окупаемости. По опросу более 150 крупных российских компаний, свыше 70% внедрили генеративный ИИ хотя бы в один бизнес-процесс, а потенциальный эффект ИИ к 2030 году оценивается в 8–12 трлн руб., сообщил Виталий Титов («Яков и Партнёры»). При этом Щербаков рассказал, что по итогам анализа МегаФона для 70% рассмотренных процессов агентная автоматизация оказалась ненужной и неокупаемой.

Дарий Халитов (Ростелеком) показал, как трудно перевести эффект в финансовый результат. Нейрошлюз компании оценивают примерно в 1,1–1,2 млрд руб. годового эффекта от роста производительности, но влияние на финансовые показатели требует отдельной оценки. За год сотрудники создали в Нейрошлюзе 9 200 агентов, однако пока не определено, как учитывать агентов в модели численности; Халитов предложил включать цифровых сотрудников в организационную структуру.

5. Суверенные модели и инфраструктура

5.1 Свои модели как резерв

Суверенные модели участники рассматривают как резерв, а не как обязанность для всех. Александр Крайнов (Яндекс) назвал собственные модели страховкой на случай полного прекращения доступа к лучшим зарубежным моделям. Он допустил, что через несколько лет доступность моделей может определяться гражданством пользователя, а передовые

китайские модели могут перестать быть открытыми. Алутин оценил отставание российских моделей от открытых зарубежных в 4–8 месяцев, Кулашова – отставание России от Китая в 4–6 месяцев. Критерий суверенности Крайнов связал с результатом: «Суверенность – это не только как это было сделано. Суверенность – это ещё то, что в результате получилось».

Разработчики выступили против обязательности. Крайнов считает, что бизнес не следует обязывать использовать суверенные модели, а применение стоит стимулировать. Андрей Кутуков (Сбер) ограничил востребованность суверенных моделей госсектором, КИИ и отраслями с чувствительными данными. Мишустин оставил выбор за компаниями, но обозначил исключение.

> Выбор здесь, конечно, за ними, но в случаях, когда речь идёт о критически значимой инфраструктуре или других чувствительных сферах, правительство станет определять, когда возможно использование только суверенных или национальных фундаментальных моделей. – Михаил Мишустин, Правительство России

Алутин предложил различать операционную и технологическую независимость: локально развёрнутая зарубежная модель без обновлений может привести к технологическому тупику через полгода или год. Обе крупнейшие российские модели доступны открыто: суверенные модели Яндекса выложены для бесплатного использования (Крайнов Александр, Яндекс), GigaChat доступен для использования и дообучения (Кутуков Андрей, Сбер).

5.2 Мультимодельная и гибридная архитектура

Ставку на одну модель спикеры отвергли. Нейрошлюз Ростелекома объединяет более 20 малых и больших языковых моделей, 75% пользователей ИИ-продукта работают в локальном контуре, ежедневно используются 1 400 агентов (Халитов Дарий, Ростелеком). Билайн запускает 4 open-source модели на собственных мощностях (Оганесян Ашот, Билайн). По оценке Глеба Облонского (Just AI), 40–60% рассматриваемых компанией кейсов можно эффективно и безопасно решать на облачных моделях.

Гибридная схема стала нормой: «Алроса» обрабатывает конфиденциальные данные внутри, основную массу – у российских облачных операторов (Желтухин Вадим, «Алроса»); пользователи агентской платформы Сбера держат платформу в своём контуре, а инференс – в облаке (Кутуков Андрей, Сбер). Крайнов отметил, что дообученная компактная модель может давать качество, сопоставимое с большими: компактная открытая модель Яндекса для поиска по внутренним базам содержит меньше 10 млрд параметров. Дмитрий Марков (VisionLabs) напомнил, что для задач высокой точности генеративный ИИ в основном механизме не нужен: «Есть класс задач, где не нужно обязательно использовать генеративку».

5.3 Вычисления, ЦОДы и энергия

Инфраструктурная часть дискуссии свелась к дефициту и загрузке. По замерам Rubytech, при разрозненном внедрении загрузка процессоров не достигает 35–40%, при консолидации на платформе поставщика – 70–80%, сообщил Игорь Ведёхин (Rubytech). Крайнов указал, что при необлачном использовании оборудование может простаивать 50% времени или больше. «Алроса» по текущему расчёту считает покупку токенов дешевле собственной инфраструктуры при масштабе менее ста GPU-серверов (Желтухин Вадим, «Алроса»).

Строительство мощностей сдерживается сроками и экономикой. По оценке Константина Степанова (РТК-ЦОД), дисконтированный срок окупаемости ЦОДа – 10–15 лет, а из более 130 проектов на согласовании возможность реализации получили менее 10. Халитов сообщил, что с конца 2025 года отдельные категории оперативной памяти подорожали в 3–3,5 раза. Макин оценил стоимость генерации токена на российских кластерах более чем в 2 раза выше, чем у китайских, и ожидает роста дефицита доступа к оборудованию. Кутуков и Крайнов вывели ограничение на следующий уровень: развитие ИИ может упереться в нехватку электроэнергии, что требует изменения многолетнего планирования в энергетике.

6. Регулирование ИИ

6.1 Закон об ИИ: от рамки к подзаконным актам

Закон об ИИ вступил в фазу подзаконных актов. Иван Лебедев (Минцифры России) сообщил, что по утверждённому план-графику к закону принимаются 6 постановлений правительства – в том числе о сферах применения и доступе к данным. Объектом регулирования выбраны фундаментальные модели как основа множества отраслевых сервисов (Лебедев Иван, Минцифры России).

Артем Шейкин (Совет Федерации) описал рамку: требования становятся строже по мере роста вероятности вреда. Часть операционных норм начнёт действовать с 1 марта 2027 года. Платформы с аудиторией более полумиллиона пользователей в сутки обязаны дать пользователям техническую возможность маркировать ИИ-контент (Шейкин Артем, Совет Федерации).

> Закон закрепляет простой принцип: где выше вероятность вреда человеку, обществу, там должно быть регулирование гораздо жёстче. – Артем Шейкин, Совет Федерации

Бизнес оценил закон положительно. Крайнов назвал ключевым результатом отсутствие ограничений, способных остановить развитие технологии. Алексей Шпильман (Т-Технологии) призвал смелее открывать медицинские и финансовые данные, но и бизнесу – приходить к регулятору с конкретными запросами: какие данные нужны, где они и как будут защищены.

6.2 Маркировка, отрасли и регионы

Маркировку ИИ-контента выбрали добровольной как исполнимую стартовую модель; быстрого перехода к обязательной Шейкин не ожидает. Михаил Рыженков (Авито) пояснил, что на платформе размещается или изменяется 20 млн объявлений в сутки, а повсеместная маркировка даже небольших ИИ-правок вызовет баннерную слепоту. Крайнов предложил регулировать введение пользователя в заблуждение, а не способ создания контента. Против мошенников с поддельными лицами и голосами, по словам Шейкина, маркировка не работает: они её не применяют.

Олег Ли (Правительство Башкортостана) поднял тему распределения полномочий: регионам предложено разрешить регулирование малых моделей с числом параметров менее 1 млрд. Лебедев ответил формулой трёх уровней – федеральная архитектура, отраслевые требования и региональные особенности. Крайнов выступил за то, чтобы правила для каждой отрасли писали её специалисты, а не единый регулятор.

7. Безопасность ИИ: суверенная не значит безопасная

7.1 Происхождение модели и доверие к ней

Специалисты по безопасности развели понятия происхождения и доверия. Дмитрий Служеникин (НТЦ ЦК) подчеркнул, что национальная модель не равна доверенной, а доверенная – безопасной; отвечает тот, кто подписал акт приёмки. Готовятся изменения к приказу ФСТЭК № 117 с требованиями к безопасности ИИ в ГИС, в эксперименте консорциума по оценке защищённости участвуют 13 регионов (Служеникин Дмитрий, НТЦ ЦК).

> Национальная и суверенная модель не равно доверенная и не равно безопасная. – Дмитрий Служеникин, НТЦ ЦК

Андрей Белеванцев (ИСП РАН) описал проект ГОСТа по безопасной разработке с ИИ как компромисс между американским «можно всё» и европейским «нельзя ничего». Требований к агентам в нём нет: пока неясно, как проверять их безопасность. Защищать, по его словам, нужно окружение модели – сопутствующее ПО, фреймворки и инструменты агентов. Шпильман привёл пример НПЗ, где между управляющей ИИ-системой и аварией стояли 7 барьеров.

7.2 Угрозы дешевеют

Угрозы со стороны ИИ стали доступнее. Марков сообщил о примерно 2 000 бесплатных инструментов создания дипфейков; отдельный детектор отражает от 90% до 95% атак и полной защиты не даёт (Марков Дмитрий, VisionLabs). Лидия Виткова («Газинформсервис») отметила, что генеративный ИИ снизил порог входа для атакующих. Денис Баранов (Positive Technologies) описал тот же сдвиг: модель угроз смещается от квалифицированного хакера

к человеку среднего уровня, усиленному ИИ. Рынок защиты ИИ-систем только складывается: по оценке аналитиков Yandex Cloud, которую привела Анна Устинова («Ведомости»), на сентябрь 2026 года он составлял от 1 до 4 млрд руб.

8. ИИ в госуправлении и городе

8.1 Аппарат правительства и ИИ-офис

Госуправление переходит от чатов к агентам, а госслужащий становится проверяющим их решений. Дмитрий Григоренко (Правительство России) рассказал, что в аппарате правительства внедряют порядка 40 самостоятельных ИИ-сервисов на решениях Сбера и Яндекса, умышленно дублируя их для сравнения эффективности. Запрос пользователей, по его наблюдению, смещается к ИИ, встроенному в рабочую функцию и выполняющему операции незаметно.

Минцифры России реализует проект ИИ-офиса: решения Сбера и Яндекса упаковываются в единый чат для госслужащих; к концу года планируется 1 000 пользователей хотя бы в пилоте, сообщил Георгий Евстафьев (Минцифры России). Регионам безвозмездно передают размеченные наборы данных – сейчас их 100, к концу года будет 150. По его оценке, «госслужащие скорее становятся валидатором решения искусственного интеллекта». Через Макса на Госуслугах в диалоговом режиме оказывается 116 услуг, добавил Антон Радужан (Минцифры России).

8.2 Регионы: запросы и метрики

Исследование потребностей регионов опиралось на более 400 решений портала «Цифровой регион»; 90% из них фиксируют эффект оптимизации труда и времени, сообщил Юрий Кабанов (НИУ ВШЭ – Санкт-Петербург). Он указал на отсутствие методики перевода экономии рабочего времени в финансовый эффект и предложил включать в обоснование проекта измеримые эффекты и способ их проверки.

На демодне регионам предложили пилоты с заранее зафиксированными метриками. В Пензенской области, по словам участников демодня, агент анализирует закупочную документацию на соответствие законодательству, а окончательное решение принимает человек.

8.3 Граждане, доверие и граница решения

По исследованию ДИТ Москвы, 96% москвичей пользовались ИИ-сервисами за последний год, но осознавали это только 74%: разрыв между фактическим использованием и его осознанием составляет 22 пункта, сообщила Софья Корчежинская (ДИТ Москвы). 89% заявляют, что проверяют результаты генеративного ИИ. Проще всего жители делегируют ИИ мониторинг среды, труднее – задачи, связанные с образованием детей (Корчежинская Софья, ДИТ Москвы).

Петр Отоцкий (Президентская академия) разложил применение ИИ в госуправлении на 4 квадранта и отметил, что сложные внутренние задачи – стратегия, нормотворчество, контроль закупок – пока почти нигде не автоматизированы, хотя эффект там наибольший. Граница решения остаётся за человеком. Марина Ким (Госдума) сформулировала это так: «Вот всегда искусственный интеллект – это второе мнение».

9. ИИ в торговле: где помощь становится подменой выбора

9.1 Рекомендации, эффект и конфликт интересов

В торговле ИИ уже влияет на оборот, и спор идёт о том, чьи интересы защищает алгоритм. Сергей Лобанов (Минпромторг России) заявил, что ИИ в торговле перестал быть только инструментом операционной эффективности: он меняет архитектуру бизнеса, роли и распределение ответственности. По его словам, X5 оценивает эффект ИИ в прогнозировании и управлении остатками в 5 млрд руб., а у ИИ-ассистента «Самоката» каждый 10-й запрос – поиск готового решения, а не конкретного товара. Лобанов считает, что агенты, помогающие выбирать товар, не должны играть в пользу конкретных производителей.

Артём Соколов (АКИТ) привёл среднюю оценку по рынку: рекомендательные технологии дают до 12% дополнительного оборота. Границу он провёл так: помощь превращается в подмену, когда система перестаёт помогать выбирать по характеристикам и незаметно выбирает за человека. Главный риск – скрытый конфликт интересов, когда покупателю обещают наиболее подходящий товар, а система оптимизирует другой показатель (Соколов Артём, АКИТ).

9.2 Полномочия агента и интересы продавцов

Агент отличается от рекомендательной системы тем, что действует: собирает корзину и инициирует покупку. Соколов предложил правило: «Полномочия агента должны быть явно заданы, ограничены и доступны для отзыва». Если агент увеличивает бюджет или оформляет подписку, он должен заново получить подтверждение человека. Начинать, по мнению Соколова, стоит с добровольных отраслевых стандартов, а не с закона. Владимир Волошин (Минэкономразвития России) назвал целевым уровнем для агента в колл-центре около 997 удачно решённых обращений из 1 000 и предложил оставлять в сервисах «красную кнопку» – возможность поговорить с человеком.

Мария Заикина (Ozon) сообщила, что ИИ-генерация контента сокращает расходы продавца на контент в четыре-пять раз, бесплатным генератором пользуются больше 260 000 предпринимателей, а 95% продавцов площадки – малый и микробизнес. Проблемы создают сторонние универсальные агенты: продавцы поручают им распределение товаров по складам и не перепроверяют результат (Заикина Мария, Ozon). Евгений Этин (RWB) сравнил агента с мерчендайзером, который одни товары ставит наверх, а другие не выставляет вовсе, и предупредил, что новые бренды могут не попасть на рынок, если модель не будет дообучаться. Валерия Воробьева (Альянс в сфере ИИ) сообщила, что

эксперименты с агентами идут во всех 22 компаниях Альянса, но в тяжёлой промышленности внедрение идёт медленнее: ошибку в физическом процессе нельзя откатить, как финансовую транзакцию. Итог дискуссии подвёл Этин: агент «должен нам помогать, но не подменять».

10. Барьеры и предложения

Барьеры, которые называли участники, сводятся к четырём группам: метод внедрения, ответственность за агентов, экономика и регулирование. В таблице – кто назвал барьер и что предложено.

Барьер	Кто называет	Что предлагают (адресат)
Раздача ИИ-инструментов не даёт промышленного эффекта	Александр Долгов, НЛМК	Платформа на весь цикл разработки; открытый код, документация и MCP у вендоров (вендоры ПО)
Теневое использование внешних ИИ-сервисов	Владимир Нелюб, «Группа Астра»; Вадим Желтухин, «Алроса»	Доверенные корпоративные инструменты и доступ к моделям на рабочем месте (работодатели, ИТ-службы)
Неподготовленные данные и нет базы знаний	Сергей Карпович, Т1	RAG-базы, базы знаний и интеграции в составе ИИ-платформы (корпоративные ИТ)
Ответственность за операции агента не определена	Дмитрий Никишов, Банк ДОМ.РФ	Заранее договориться бизнесу, ИТ и ИБ; ограничить полномочия агента (компании)
Нет нормативного описания сделок через агента	Игорь Алутин, Московская биржа	Подтверждение распоряжения человеком, реестр агентных сделок (финансовые организации)
Нет готовых коннекторов, внедрение дорожает	Сергей Голицын, Т1	MCP-коннекторы от вендоров, MCP как критерий реестра ПО (вендоры, операторы реестров)
Расход токенов непредсказуем	Алексей Фетисов, Альфа-Банк	Блюпринты оценки стоимости генеративной разработки (участники Совета)
Нет методики перевода экономии времени в финансовый эффект	Юрий Кабанов, НИУ ВШЭ – Санкт-Петербург	Измеримые эффекты и методика проверки в обосновании проекта (разработчики госрешений)
Не определено, как учитывать агентов в численности	Дарий Халитов, Ростелеком	Включать цифровых сотрудников в оргструктуру (руководители компаний)

Барьер	Кто называет	Что предлагают (адресат)
Правовой вакуум в региональном применении	Олег Ли, Правительство Башкортостана	Право регионов регулировать малые модели (федеральные законодатели)
Неясно, как проверять безопасность агентов	Андрей Белеванцев, ИСП РАН	Добавить требования при пересмотре ГОСТа (разработчики стандартов)
Скрытый конфликт интересов в рекомендациях агента	Артём Соколов, АКИТ	Явные и отзываемые полномочия агента, отраслевые стандарты (площадки, отраслевые ассоциации)

11. Ключевые игроки темы

Повестку направления определяли разработчики моделей, операторы связи, промышленные заказчики и регуляторы.

- **Яндекс и Yandex Cloud** – Александр Крайнов отстаивал суверенные модели как резерв без принуждения; Григорий Атрепьев сообщил, что фонд оплаты труда и токены стали одной строкой бюджета.
- **Сбер** – Андрей Кутуков говорил о суверенных моделях для КИИ и гибридном инференсе; Кирилл Меньшов представил Совет по генеративной разработке из около 30 компаний.
- **Ростелеком** – Дарий Халитов: Нейрошлюз с более чем 20 моделями, 9 200 агентов, эффект 1,1–1,2 млрд руб. в год.
- **Билайн** – Сергей Анохин и Ашот Оганесян: около 10 000 сотрудников постоянно работают с платформой экзоинтеллекта (Анохин Сергей, Билайн), предложены паспорт агента и лимиты токенов.
- **МТС и MWS AI** – Денис Филиппов: 3 млрд руб. эффекта в контакт-центре, более 400 сценариев при 6 млн звонков в месяц.
- **НЛМК** – Александр Долгов: от 600 доступов без эффекта к соло-инженерам и цели снизить себестоимость ИТ-решений в 10 раз.
- **Банк «Санкт-Петербург»** – Станислав Кутузов: эффект в 3 раза выше инвестиций, более 130 ИИ-проектов на пути в промышленное использование.
- **Росатом и «Гринатом»** – Евгений Гаранин и Заяна Ачинова: 400% роста операций при 4% роста численности, конвейер гипотез.
- **«Норникель»** – Алексей Тестин: ИИ управляет фабриками, порядка 10 млрд руб. в год, модель «видит – советует – управляет».
- **«Алроса»** – Вадим Желтухин: рост загрузки самосвалов на 11%, гибридное облако и сравнение токенов с собственными GPU.
- **Московская биржа** – Игорь Алутин: агентный эксперимент на 17 000 операций, MCP на «Финуслугах», реестр агентных сделок.

- **«Лаборатория Касперского»** – Анна Кулашова и Александр Лискин: защитная обвязка агентов, песочницы и шлюзы фильтрации, около 38% компаний используют ИИ внутри.
- **T1** – Сергей Голицын и Сергей Карпович: права агента по правам сотрудника, MCP как критерий реестра ПО.
- **Минцифры России** – Иван Лебедев о 6 постановлениях; Георгий Евстафьев об ИИ-офисе на 1 000 госслужащих и 150 наборах данных для регионов.
- **ДИТ Москвы** – Софья Корчежинская: 96% москвичей пользуются ИИ, разрыв осознания в 22 пункта.
- **Ozon и RWB** – Мария Заикина и Евгений Этин: ИИ-инструменты для продавцов и риски агентов, которые выбирают за покупателя.

Выводы

- **Доступ к моделям сам по себе эффекта не даёт.** НЛМК выдал более 600 доступов и получил только рост затрат; результат появился после перевода разработки на агентную платформу (Долгов Александр, НЛМК). Банк «Санкт-Петербург» описывает обратный опыт: массовый доступ принёс кейсы, а эффект в 3 раза превысил инвестиции (Кутузов Станислав, Банк «Санкт-Петербург»).
- **Самые крупные подтверждённые эффекты – в промышленности.** «Норникель» заявляет порядка 10 млрд руб. в год от ИИ на фабриках (Тестин Алексей, «Норникель»), Росатом – рост операций закупочного органа на 400% при росте численности на 4% (Гаранин Евгений, Росатом).
- **Эффект считают по процессу, а токены – вместе с фондом оплаты труда.** Расход токенов на одну задачу различается до 5 раз (Фетисов Алексей, Альфа-Банк), а для 70% рассмотренных МегаФоном процессов агентная автоматизация не окупается (Щербаков Виталий, МегаФон).
- **Агент становится клиентом, но отвечает за него компания.** Московская биржа провела эксперимент на 17 000 агентных операций и предлагает реестр агентных сделок (Алутин Игорь, Московская биржа); «ВкусВилл» ждёт 13–15% транзакций через агентный канал за 3 года (Абрамов Александр, «ВкусВилл»).
- **Суверенная модель нужна как резерв, обязательной она будет только в чувствительных сферах.** Отставание российских моделей от открытых зарубежных оценено в 4–8 месяцев (Алутин Игорь, Московская биржа); случаи обязательного использования суверенных моделей определит правительство (Мишустин Михаил, Правительство России).
- **Вычисления и энергия ограничивают рост.** Из более 130 проектов ЦОДов возможность реализации получили менее 10 (Степанов Константин, РТК-ЦОД), генерация токена на российских кластерах более чем в 2 раза дороже китайской (Макин Алексей, Red_mad_robot).
- **Регулирование переходит к подзаконным актам и отраслевым стандартам.** К закону об ИИ готовятся 6 постановлений (Лебедев Иван, Минцифры России), часть норм начнёт

действовать с 1 марта 2027 года (Шейкин Артем, Совет Федерации); в торговле предлагают начать с добровольных стандартов для агентов (Соколов Артём, АКИТ).

Источники

- Сессия «Главная пленарная сессия „Результаты. Возможности. Перспективы“», Форум «Цифровые решения – 2026»
- Сессия «ИИ-агенты под контролем: как управлять рисками и строить доверенную инфраструктуру», Форум «Цифровые решения – 2026»
- Сессия «ИИ-фабрика как основа безопасного и эффективного развития предприятия», Форум «Цифровые решения – 2026»
- Сессия «Регулирование ИИ: поиск баланса между развитием технологий и защитой интересов граждан», Форум «Цифровые решения – 2026»
- Сессия «Эффекты применения ИИ в системах управления ресурсами: метрики, кейсы, масштабирование», Форум «Цифровые решения – 2026»
- Сессия «ИИ для решения государственных задач: приоритеты, эффекты и критерии успеха», Форум «Цифровые решения – 2026»
- Сессия «ИИ на распутье: как выбор инфраструктуры определит эффективность и выгоду на годы вперёд», Форум «Цифровые решения – 2026»
- Сессия «От ускорителя к ИИ-сервису: как сделать корпоративную ИИ-инфраструктуру управляемой», Форум «Цифровые решения – 2026»
- Сессия «Отечественные генеративные модели: путь к технологическому суверенитету», Форум «Цифровые решения – 2026»
- Сессия «От локальных инициатив к корпоративной системе: как внедрять ИИ в бизнесе», Форум «Цифровые решения – 2026»
- Сессия «Пленарная сессия. Государство как цифровой сервис: где остановиться?», Форум «Цифровые решения – 2026»
- Сессия «Доступ разрешен: повышение эффективности ИИ-агентной экономики и новые стандарты ПО», Форум «Цифровые решения – 2026»
- Сессия «Конференция билайн. Дискуссионное шоу. Красная зона ИИ: технология готова – готовы ли мы?», Форум «Цифровые решения – 2026»
- Сессия «Конференция билайн. Облака в эпоху ИИ-атак: выжить, выстоять и восстановиться», Форум «Цифровые решения – 2026»
- Сессия «Демодень ИЦК „Мобильная связь“: ИИ и трансформация отрасли связи», Форум «Цифровые решения – 2026»
- Сессия «Скрытые резервы: как превратить накопленный цифровой опыт компании в реальные бизнес-результаты», Форум «Цифровые решения – 2026»
- Сессия «Суверенный ИИ: сколько независимости нужно заказчику», Форум «Цифровые решения – 2026»

- Сессия «Искусственный интеллект в телекоме и коммуникациях: как технологии влияют на наше общение», Форум «Цифровые решения – 2026»
- Сессия «В диалоге с ИИ: как жители Москвы и других умных городов взаимодействуют с технологией», Форум «Цифровые решения – 2026»
- Сессия «Доверенная генеративная разработка: единые правила для отрасли», Форум «Цифровые решения – 2026»
- Сессия «Безопасность ИИ-моделей: угрозы, методы защиты и подходы к регулированию», Форум «Цифровые решения – 2026»
- Сессия «Пленарная сессия. ИТ-достояние России: победы, за которыми стоят люди», Форум «Цифровые решения – 2026»
- Сессия «Цифровой контур госслужбы: технологии, безопасность, образование», Форум «Цифровые решения – 2026»
- Сессия «ИИ решит за вас? Где заканчивается помощь и начинается подмена выбора», Форум «Цифровые решения – 2026»