



Ай-ТИ Фреш

ТЕХНИЧЕСКИЙ РАЗБОР

Дайджест ИИ: Cursor, Runway, Qwen и Tilda AI — как мы внедряем

Наш регламент пилота ИИ-инструментов у клиентов:
контур данных, доступ из РФ, бюджет, контроль

Июль 2026

itfresh.ru · ИТ-аутсорсинг для юридических лиц

Суть проблемы

Клиенты приносят ИИ-сервисы «с рынка»: разработка хочет Cursor, маркетинг — Runway и Tilda AI, бэк-офис — «скормить документы» Qwen. Без регламента это утечка клиентских данных в облако, счета за токены без лимитов и процессы на сервисах, доступ к которым из РФ не гарантирован. Мы решаем это единым циклом: контур данных → пилот 14 дней → внедрение с лимитами и ревью.

Почему это важно бизнесу

- Утечка ПДн клиентов или коммерческой тайны в облачную модель — это 152-ФЗ, штрафы и потеря клиента; отданные данные не вернуть
- Агентские ИИ-сессии без лимитов расхода превращают «дешёвый инструмент» в непредсказуемую статью бюджета
- Процесс, построенный на зарубежном сервисе без резерва, останавливается вместе с его доступностью из РФ
- Непроверенный сгенерированный код и контент уходит в прод и ломает то, что работало, — простой и репутационный ущерб

Ключевые параметры реализации

1М токенов

контекст Qwen3.8-Max — пакет договоров или вся переписка проекта в один запрос, без RAG-обвязки

по докам Alibaba Model Studio

Privacy Mode

принудительно на всю организацию в Cursor: код не идёт в обучение, у провайдеров zero-retention

по докам Cursor Enterprise

2-30 с

длительность клипа на правку в Runway Aleph 2; выход до 1080p с сохранением пропорций кадра

по докам Runway API

14 дней

наш цикл пилота: неделя на обезличенных данных, неделя на боевой задаче с замером эффекта

наш стандарт

x10

стоимость токена Composer 2.5 ниже флагманских моделей уровня Orus — повод пересчитать бюджет...

по докам Cursor Models & Pricing

100%

генераций проходят проверку человеком до продакшена: код — через PR, контент — через согласова...

наш стандарт



Контур данных: подготовка до первого промпта

Что настраиваем

Все облачные ИИ (Cursor, Qwen, Runway, Tilda AI) на рабочих местах клиента до 50 PM; узлы — админ-панели сервисов и шлюз доступа

Как мы это делаем

- 1 Заводим сервисы только на корпоративные учётки домена клиента; доступы — в парольный менеджер компании, а не в личные аккаунты сотрудников
- 2 В Cursor включаем Privacy Mode на уровне организации (админка Team/Enterprise) и сверяем по документам zero-data-retention у модель-провайдеров
- 3 Утверждаем регламент AI-Usage-Policy: что можно в промпт (обезличенное), что нельзя (ПДн, коммерческая тайна, доступы); знакомим сотрудников под подпись
- 4 Для зарубежных сервисов настраиваем стабильный сетевой маршрут и резервный способ оплаты; фиксируем дату проверки доступности в паспорте сервиса
- 5 Ведём реестр ИИ-инструментов клиента: версия, тариф, лимит расходов, владелец, дата пересмотра

РЕЗУЛЬТАТ

Любой новый ИИ-инструмент попадает в работу через одну и ту же процедуру за 1–2 дня: данные не утекают, расходы под лимитом, а увольнение сотрудника не уносит доступ к сервису вместе с личным аккаунтом.

КЛЮЧЕВОЙ НЮАНС

В документации первым смотрим раздел про data usage и retention: у Cursor это отдельные страницы Privacy and Data Governance и LLM Safety and Controls — режимы обучения на данных отличаются по тарифам.



Cursor Composer в разработке клиента

Что настраиваем

Команды разработки 2–10 человек; узлы — Cursor Team/Enterprise, Git-репозитории клиента, CI

Как мы это делаем

- 1 Разворачиваем Cursor Team: в админке включаем pooled usage и лимит расходов на участника, модельный доступ ограничиваем списком (Composer 2.5 + резервная модель)
- 2 MCP-контроли: разрешаем только серверы из allowlist админки, системные agent-rules задаём централизованно (Enterprise)
- 3 В репозиторий кладём правила проекта (.cursor/rules): стек, запрет секретов в коде, обязательные тесты — агент следует им в каждой сессии
- 4 Composer 2.5 отдаём типовые задачи (CRUD, тесты, рефакторинг), флагманскую модель оставляем на архитектуру — так и получается экономия x10 на токенах
- 5 Весь сгенерированный код — только через pull request с ревью; прямые коммиты агента в main запрещены защитой ветки

РЕЗУЛЬТАТ

Разработка ускоряется на рутине без роста бюджета: дешёвая модель закрывает большинство задач, дорогая включается точно, расходы видны в админке по каждому участнику команды.

КЛЮЧЕВОЙ НЮАНС

Дешёвая модель провоцирует «стрелять очередями»: без лимитов на участника и ревью PR счёт и техдолг растут быстрее продуктивности. Лимиты ставим до выдачи доступов, а не после первого счёта.



Qwen для документов и Tilda AI для сайта

Что настраиваем

Бэк-офис (анализ документов) и маркетинг (лендинги); узлы — Alibaba Model Studio API и редактор Tilda

Как мы это делаем

- 1 Qwen3.8-Max подключаем через Model Studio (OpenAI-совместимый API); на пилоте — только обезличенные документы, качество меряем на 10 эталонных вопросах
- 2 Длинный контекст (до 1М токенов) используем вместо RAG-обвязки на старте: пакет договоров грузим целиком, ответы требуем с цитатой и номером пункта
- 3 Tilda: блоки генерируем Вайб-блоком (Библиотека блоков → раздел «Другое»), итеративно уточняем описание в чате редактора; лимит генераций — 5-50 запросов за 12 часо...
- 4 Перед AI-правками публикуемой страницы делаем её копию в проекте Tilda — откат за минуту, если блок сломал вёрстку; после генерации проверяем рендер 375px и скорость

РЕЗУЛЬТАТ

Юрист или бухгалтер получает разбор пакета документов за минуты вместо часов, маркетолог сам собирает лендинг без верстальщика — при этом ни один персональный документ не ушёл в облако без обезличивания.

КЛЮЧЕВОЙ НЮАНС

Ответы по длинному контексту обязательно проверяем на «середину» документа: качество на больших окнах неравномерно, поэтому требуем точные цитаты и сверяем их с оригиналом.



Подводные камни

✗ ПДн и тайна в облачном промпте

Сотрудники грузят реальные договоры «как есть». Обходим: Privacy Mode, регламент AI-Usage-Policy и обезличивание реквизитов до отправки в модель.

✗ Пилот на личных аккаунтах

Уволился сотрудник — ушли и доступ, и история. Заводим сервисы на корпоративный домен, доступы храним в парольном менеджере компании.

✗ Красивое демо приняли за прод

Генерация стабильна на демо и сыпется на боевых данных. Пилотируем 14 дней на своих задачах с метриками до/после — и только потом покупаем тариф.

✗ Нет лимитов на токены

Агентские сессии жгут бюджет незаметно. В админке ставим лимит расходов на участника и алерт на 80% лимита — до выдачи доступов.

✗ Критичный процесс на зарубежном API

Доступ из РФ не гарантирован никому. Для каждого ИИ-процесса держим резерв (Tilda, Qwen, локальная модель) и описанный план переключения.

✗ Модель вывели из эксплуатации без нас

Провайдеры отключают модели: Gen-4 Aleph убран из Runway API 30.07.2026. Фиксируем версию модели в конфиге и раз в квартал сверяем changelog и депрес...

✗ Вайб-блок ломает мобильную вёрстку

Сгенерированный блок красив на десктопе и едет на телефоне. Проверяем рендер на 375px и скорость страницы до публикации; копия страницы — заранее.

✗ Слепое доверие длинному контексту

На сотнях страниц модель «теряет» середину документа. Требуем цитаты с указанием пункта и сверяем их с оригиналом перед принятием решения.

Как правильно

МИНИМУМ

- Регламент AI-Usage-Policy подписан: что можно и что нельзя отправлять в облачный ИИ
- Все ИИ-сервисы — на корпоративных учётках, доступы в парольном менеджере
- Privacy Mode / отказ от обучения на данных включён везде, где настройка есть
- Любая генерация проходит проверку человеком до продакшена

НОРМАЛЬНО

- Пилот 14 дней с метриками до/после для каждого нового инструмента
- Лимиты расходов и алерты на токены в админках (Cursor, Model Studio)
- Реестр ИИ-инструментов: версия, тариф, владелец, дата пересмотра
- Обезличивание документов перед загрузкой в облачные модели

ХОРОШО

- Централизованные admin-controls: список моделей, MCP-allowlist, agent-rules
- Резервный инструмент и план переключения для каждого ИИ-процесса
- Фиксация версий моделей + квартальная сверка changelog и deprecation-дат
- Правила проекта в репозитории (.cursor/rules) и обязательный PR-ревью кода агента



Чек-лист самопроверки

- | | |
|--|--|
| ☐ Известно ли, какие ИИ-сервисы сотрудники уже используют и на каких учётках? | ☐ Есть ли резервный инструмент на случай недоступности зарубежного сервиса из РФ? |
| ☐ Включён ли Privacy Mode / запрет обучения на ваших данных во всех подключённых сервисах? | ☐ Зафиксированы ли версии моделей и отслеживаются ли даты их вывода из эксплуатации? |
| ☐ Есть ли подписанный регламент, что можно и что нельзя отправлять в облачный ИИ? | ☐ Обезличиваются ли документы перед загрузкой в облачную модель для анализа? |
| ☐ Стоят ли лимиты расходов и алерты на токены в админках ИИ-сервисов? | ☐ Делается ли копия страницы Tilda перед AI-правками и проверяется ли мобильный рендер? |
| ☐ Проходит ли сгенерированный код через pull request с ревью, а контент — через согласование? | |

Если хотя бы на два вопроса ответ «нет» или «не знаю» — тема требует внимания.



Как поможет ITFresh

ITFresh — ИТ-аутсорсинг для юридических лиц до 50 рабочих мест в Москве и области. 15+ лет практики, собственная инфраструктура в дата-центре МТС (8 серверов Dell Xeon Platinum).

- Аудит «теневого ИИ»: находим, что сотрудники уже используют, и переводим в управляемый контур
- Пилот под ключ за 14 дней: Cursor / Qwen / Tilda AI на ваших задачах с замером эффекта
- Контур данных: Privacy Mode, корпоративные учётки, регламент, лимиты расходов
- Внедрение Cursor в разработку: админ-политики, правила проекта, PR-процесс
- Сопровождение стека: мониторинг доступности, сверка deprecation, план перехода на резерв

15+

лет в ИТ-поддержке

50

рабочих мест — наш профиль

МТС

дата-центр, Москва



КОНТАКТЫ

Обсудить вашу задачу

Сайт **itfresh.ru**

Телефон **+7 903 729-62-41**

Telegram **@ITfresh_Boss**

Бесплатно посмотрим вашу инфраструктуру по этому чек-листу и скажем, где тонко — без обязательств.



itfresh.ru



Техническая база

- 01** Cursor Docs — Enterprise: Privacy and Data Governance (cursor.com — 2026)
- 02** Cursor Docs — Models & Pricing; Enterprise: LLM Safety and Controls (cursor.com — 2026)
- 03** Runway API Docs — Aleph 2 (video-to-video), API Changelog (docs.dev.runwayml.com — 2026)
- 04** Alibaba Cloud Model Studio — Models, Qwen API Reference (alibabacloud.com — 2026)
- 05** Справочный центр Tilda — Вайб-блок: создание блоков с помощью ИИ (help-ru.tilda.cc — 2026)
- 06** Наш шаблон регламента AI-Usage-Policy и паспорта ИИ-сервиса (itfresh.ru — v2)

Основано на официальной документации продуктов и нашей практике внедрения.

