ANALYTICS & COMPLIANCE

Локально или в облако: архитектура B2B AI в условиях 152-ФЗ

Что реально требует закон от B2B AI в 2026 году. Фреймворк для C-level: где нужен on-premise, а где облако абсолютно легально.

14 МАЯ 2026 — TEMADEV NOTES

РЕАЛЬНОСТЬ 2025–2026

до 500 млн ₽

Оборотный штраф
за повторную утечку ПДн.

>600

Уголовных дел по ст. 272.1
(неправомерный доступ) за год.

РЕАКЦИЯ РЫНКА

Юристы и интеграторы
массово советуют
изолировать AI:

~~Делать всё только on-premise~~

Понятно, но некорректно как универсальное правило.

ДАННЫЕ ЮРЛИЦ ≠ ПЕРСОНАЛЬНЫЕ ДАННЫЕ

152-ФЗ защищает физических лиц, а не организации. ИНН, название компании, корпоративный email и должность — не попадают под ограничения.

Главный вопрос: не «облако или сервер?», а «что обрабатывает AI и кому это принадлежит?»

ЗеЛЁНАЯ ЗОНА (СВОБОДНО)

Реквизиты юрлиц (ИНН, ОГРН), операционные данные (парк техники, прайсы), публичная информация, обезличенные агрегаты.

ОБЛАКО БЕЗ ОГРАНИЧЕНИЙ

ЖЁЛТАЯ ЗОНА (УМЕРЕННЫЙ РИСК)

Имена и телефоны контактных лиц (ЛПР), записи деловых переговоров, формы с адресами доставки.

ОБЛАКО ЧЕРЕЗ ДПО И МАСКИРОВАНИЕ

КРАСНАЯ ЗОНА (КРИТИЧНО)

Биометрия (штрафы 15-20 млн ₽), диагнозы, кредитные истории, необезличенные физлица. Трансграничная передача в США.

ТОЛЬКО ON-PREMISE

ОТРАСЛЬ	ТИП ДАННЫХ	ОБЛАКО ЗАКОННО?	МИНИМАЛЬНЫЕ ТРЕБОВАНИЯ
Спецтехника	Данные юрлиц + заявки	Да	ДПО + обезличивание ФИО ЛПР.
Оптовая торговля	Юрлица + корп. контакты	Да	ДПО + стандартная политика ПДн.
Строительство	Юрлица + субподрядчики	Частично	Кадровые данные строго отдельно.
E-commerce	ПДн физлиц	С оговорками	ДПО + уведомление РКН.
Медицина	Медицинские данные (УЗ-1)	Нет	On-prem + интеграция с ЕГИСЗ.
Банки	Банковская тайна (395-1 ФЗ)	Нет	On-prem + требования ЦБ РФ.

КРАСНАЯ ЗОНА: КОГДА ON-PREMISE НЕИЗБЕЖЕН

Банки и финансы

Запрет на передачу данных о клиентах третьим лицам без согласия. Claude/OpenAI напрямую невозможны.

ПОЛОЖЕНИЕ ЦБ РФ № 787-П, 395-1 ФЗ

Медицина (УЗ-1)

AI-ассистенты для медкарт обязаны работать в аттестованной МИС. Облачные API полностью исключены (спец. категории ПДн).

ПРИКАЗ МИНЗДРАВА № 911Н

Гостайна и Госзакупки

Единые защитные меры с 1 января 2026 года. Ни один публичный облачный провайдер не имеет нужного уровня допуска.

СЕРТИФИКАЦИЯ ФСТЭК / ФСБ

Массовый B2C (Без обезличивания)

Передача необезличенных ПДн в зарубежные API в 2026 году запрещена (США вне перечня разрешенных направлений РКН).

ТРАНСГРАНИЧНАЯ ПЕРЕДАЧА ПДН

B2B СЕРВИСЫ

Маскирование ФИО контрагентов снимает 90% юридических рисков.

ГОЛОСОВОЙ AI

Уведомление в начале звонка + обезличивание транскрипта + сервер РФ для сырой записи.

СТРОИТЕЛЬСТВО

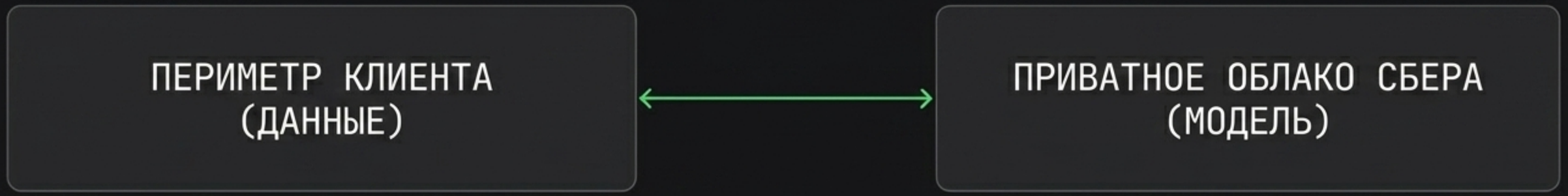
Безопасно, пока AI координирует заявки юрлиц, а не ведет кадровый учет 115-ФЗ.

Input:
Иван Иванов (ИНН 7701234567) просит скидку.

ПРИКАЗ РКН № 996

Output to LLM:
[PERSON_1] (ИНН 7701234567) просит скидку.

ВЫБОР LLM-СТЕКА ДЛЯ ENTERPRISE



GigaChat 2 Pro (500 ₽ / 1 млн токенов — в 10x дешевле Claude).
GigaChat 3.1 Lightning (Self-hosted GGUF).

LATENCY	FUNCTION CALLING	CONTEXT WINDOW	OBSERVABILITY
Гибрид добавляет задержку к ответам.	Обязательное тестирование длинных цепочек инструментов.	Сверка актуальных лимитов токенов по документации.	Необходимость строить кастомный logging-слой.

МИНИМАЛЬНЫЙ LEGAL STACK

ДПО (Договор поручения обработки)

Фиксирует оператора (клиент) и обработчика (разработчик), категории данных, срок хранения. Цена адаптации: 25–40 тыс. ₽.

Политика конфиденциальности

Обновление раздела клиента об AI-обработке.

Уведомление РКН

Подается клиентом через Госуслуги до начала сбора данных.

Уведомление пользователя

Стандартный дисклеймер в начале чата или звонка об автоматической обработке.

РЕГУЛЯТОРНЫЙ ГОРИЗОНТ: ЗАКОН ОБ ИИ (С 1 СЕНТЯБРЯ 2027)

Обязанность информировать

Чат-бот, выдающий себя за человека — вне закона. Информирование об AI до контакта становится строгим требованием.

Распределение ответственности

Разработчик → Оператор → Пользователь. Договор обязан явно фиксировать за AI-вывод, суд решит по степени вины.

Обязанность информировать

Чат-бот, выдающий себя за человека — вне закона. Информирование об AI до контакта становится строгим требованием.

Реестр доверенных моделей

Государственные и критические ИС потребуют сертифицированных AI. Создаст давление и на частный B2B сектор.

Распределение ответственности

Разработчик → Оператор → Пользователь. Договор обязан явно фиксировать ответственность за AI-вывод, иначе суд решит по степени вины.

Экспресс-диагностика архитектуры

> Какие категории данных физлиц видит модель до маскирования?
[ЕСЛИ НИКАКИЕ] → ЗЕЛЕНАЯ ЗОНА

> Есть ли подписанный ДПО с каждым клиентом?
[ЕСЛИ НЕТ] → КРИТИЧЕСКИЙ РИСК

> Куда физически уходят данные к API?
[ЕСЛИ ЗА РУБЕЖ С ПДН] → ТРЕБУЕТСЯ УВЕДОМЛЕНИЕ РКН

Метод Temadev: Мы не консультируем, мы строим AI-native контуры за 4–8 недель.