

КОД **ИБ** ЕКАТЕРИНБУРГ · 15 ОКТЯБРЯ 2026

15:00–15:20

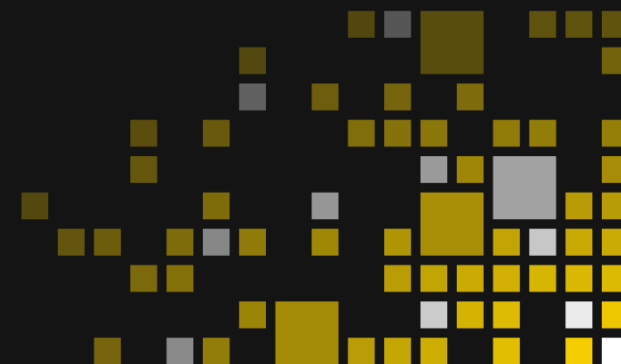
ЗАЛ 2

ИИ в закрытом контуре

Никита Дунов

Руководитель группы цифровой трансформации

IT-компания «Метраникс», ГК «Метран»

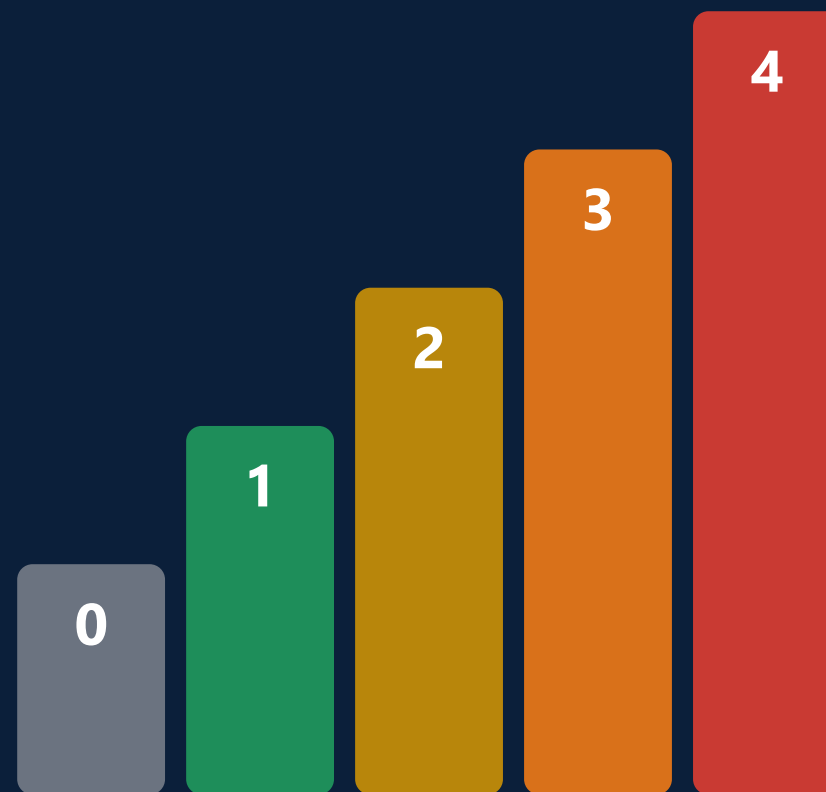


ИИ в закрытом контуре

Как пустить нейросети в компанию и не отдать наружу её данные. Опыт производственной группы — с граблями

Никита Дунов

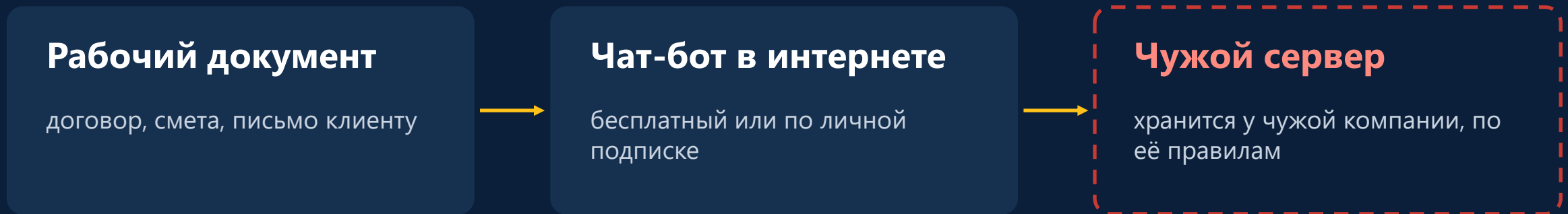
Руководитель группы цифровой трансформации
IT-компания «Метраникс», ГК «Метран»



от публичного — к коммерческой тайне

Кто вставлял рабочий документ в чат-бот?

За последний месяц — поднимите руку



Любой разговор с нейросетью остаётся на чужом компьютере

Сегодня — как мы сами через это прошли, что сломали и как устроили по-другому

20% организаций с утечками связали их с ИИ вне утверждённых процессов. Год назад — около 12% «Информзащита», июль 2026

Завод с 1992 года и команда из четырёх



ГК «Метран», Челябинск

С 1992 года. Первые в России интеллектуальные датчики давления. Сегодня — приборы и системы автоматизации для всей промышленности

4 человека

Один эксперт с ИТ-опытом и три джуна без образования программиста

3 года

От первых гипотез до сервисов, которыми пользуется вся группа

10 млн ₽ за всё

Весь фонд оплаты труда команды за три года — все затраты эксперимента

Ни одного нанятого программиста: эксперт задаёт направление, джун в связке с ИИ делает

The screenshot displays a terminal window with three main sections: Explorer, Terminal, and Chat.

Explorer: Shows a file tree with folders like 'scripts', 'plugins', and 'statements'. The 'scripts' folder contains files like 'setup-weekly-reboot.sh' and 'setup-weekly-reboot.sh'. The 'plugins' folder contains files like 'bank_stat' and 'bank_stat'. The 'statements' folder contains files like 'statements-mount' and 'statements-mount'.

Terminal: Shows the execution of various commands to set up the container. The commands include creating directories, setting permissions, and installing dependencies. The output shows the successful execution of these commands.

Chat: Shows a conversation with an AI assistant. The assistant provides instructions and code snippets for setting up the container. The instructions include creating a Dockerfile, setting up the container, and running the container. The code snippets show the commands to create the Dockerfile, set up the container, and run the container.

Код пишем в связке с ИИ

СВОИ СЕРВЕРЫ

Гипотезы — на своём железе

Проверили зрение, расшифровку и синтез речи

ОБЩИЙ ЧАТ

Один ИИ-чат на всю компанию

Открытое решение: используем как есть, обновляет сообщество

Честно: тогда мы думали, работает ли это. А не куда уходят данные

Получилось — и пошло само

Не заставляли, а показывали пользу: вебинары, посты во внутреннем портале, свои «чемпионы» в отделах

ИНЖЕНЕРНЫЙ ЦЕНТР + 1С

2 → 14

Показали двум сотрудникам. Через месяц ИИ пользуются 12 инженеров и 2 программиста 1С

2 мес → 2 нед

типовой проект инженерного центра

×2

скорость разработки в 1С

+150%

в месяц — рост аудитории общего ИИ-чата

Разрешения никто не спрашивал. Для бизнеса — отлично. Для безопасности — **тревожно**

И начало приносить деньги

Сэкономленный час — ещё не деньги. Деньги — это найденный заказ и не нанятый подрядчик

ТЕНДЕРНЫЙ БОТ

70%

тендеров в работе компании находит бот

- ~200 тендеров в сутки: собирает, оценивает, рекомендует
- Первый же тендер, который пропустил человек, окупил бота в 4 раза
- Продан внешнему заказчику

QR-КОДЫ НА ПРОДУКЦИИ

3,5 млн ₽

продано внутри группы

- Паспорт и инструкция изделия по скану
- В работе больше года
- Сделали двое, без разработчиков



Раз работает — значит, пойдёт дальше. Вместе с данными компании

И тут стало не по себе

Мы оглянулись и увидели, куда на самом деле уходят данные и деньги

01 Запрещать не стали

Многие запрещают — и люди уходят в личные аккаунты и телефоны. Мы это знали и сразу сделали свой сервис

02 Ключи доступа по отделам

Каждый ключ — отдельная дверь наружу. Никто не знал, сколько их и кто ими пользуется

03 Бюджет без лимитов

Большую часть счёта съедали одна дорогая модель и пара самых активных сотрудников

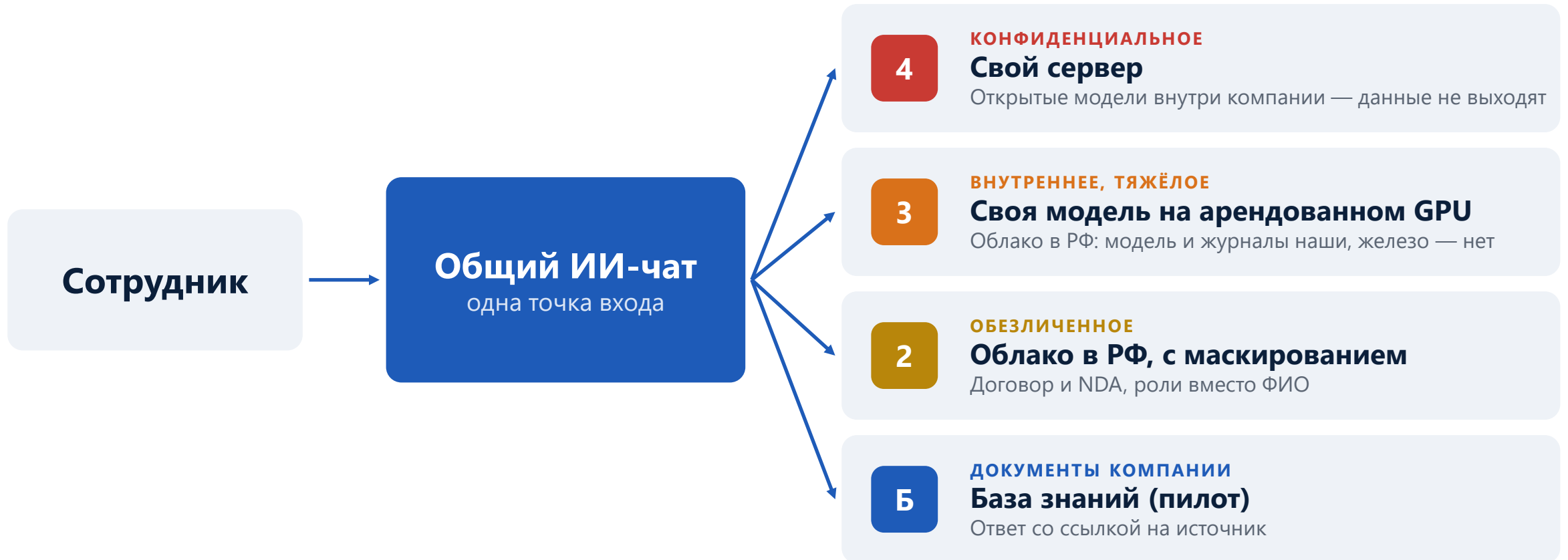
04 Агент «со всеми правами»

Удобно на демо, опасно в работе: ошибка агента становится ошибкой администратора

Всё это — наш собственный опыт, а не цифры из чужих отчётов

Не запрещать, а дать официальный путь

Одна дверь для всех сотрудников. Куда пойдёт запрос — решает класс данных, а не привычка



Когда есть удобная официальная дверь, в личные аккаунты уходить незачем

Каждой задаче — своя ступень

Наша рабочая схема, а не стандарт. Чем ценнее данные, тем ближе к себе их держим



ПРАВИЛО КУРИЛКИ

Что нельзя сказать вслух в курилке — не отправляем в чат-бот

Сильная модель тянет людей — и счёт

Привлекательность общего чата растёт вместе с моделями, которые мы в него добавляем

ОБЩИЙ ИИ-ЧАТ КОМПАНИИ

+ Opus 4.8

Добавили дорогую и сильную модель — люди потянулись в чат и стали пользоваться им заметно чаще

Это видно по статистике

Чат — для общих вопросов: там он недорогой

Следим не только за чатом, но и за тем, что и куда отдают программисты

ПРОБЛЕМА

~20 000 ₽

в месяц на программиста: код через прокси в дорогую модель

ЧТО СДЕЛАЛИ

Лимит токенов

в общем чате — не отключили, а ограничили

АЛЬТЕРНАТИВА

DeepSeek + VS Code

для обычного кода — так работают все наши программисты

КОНФИДЕНЦИАЛЬНЫЙ КОД

Qwen 3.8 локально

вместо DeepSeek: код не покидает наши серверы

Не отключать, а давать разумную альтернативу. Каждой задаче — свой инструмент

Сколько стоит закрытый контур

Три вопроса, которые стоит задать до покупки сервера — вместе с безопасниками

1 Какие данные?

Задают минимальную ступень.
Ниже нельзя, даже если дешевле

2 Как часто?

Загрузка постоянная — свой сервер. Эпизодическая — аренда GPU в облаке по часам

3 Сколько стоит?

Подписка, аренда GPU или покупка. Считаем цену контура, а не цену модели

≈40 тыс ₽

в месяц — облачные модели для общего ИИ-чата
всей группы компаний

**Свой сервер нужен не для всего,
а для ступени 4**

Тяжёлое и разовое — арендуем GPU. Остальное —
подпиской, с договором и маскированием

Где риски остаются, даже когда всё настроено

Маскирование прячет, о ком речь. Но не прячет всё остальное

Метаданные

Облако видит сам факт работы

Когда, сколько, какие задачи и какие отделы активнее. Это мы знаем, принимаем и держим под наблюдением

Права

База знаний не помнит прав

В папке документ видят ролям, в ИИ-поиске — все. Права нужно проектировать заново

3 из 3

Документ может «командовать» ИИ

На изолированном тестовом стенде агент трижды из трёх выполнил команду, спрятанную в безобидном документе

Инструмент

Сам ИИ-инструмент — тоже точка атаки

Март 2026: в популярный ИИ-шлюз LiteLLM подложили версии, которые крали ключи и пароли

Идеала нет. Есть понимание, что и куда уходит

Стоять на месте — тоже риск

«Здесь, знаешь ли, приходится бежать со всех ног, чтобы только остаться на том же месте»

Льюис Кэрролл, «Алиса в Зазеркалье»

РИСК ОТДАТЬ

Часть данных уходит в облако по договору

Только «конфиденциальное для нас». Персональные данные и коммерческая тайна — на своих серверах



РИСК НЕ ОТДАТЬ

Конкуренты делают ту же задачу в разы быстрее

И мы отстаём. Этого риска не видно в отчётах ИБ

Баланс решает владелец данных — явно и под свою ответственность, а не ИТ и не ИБ. Наша задача — дать ему понятный выбор и цену каждого варианта

Где мы сейчас

От «на коленке» к корпоративному контуру — по шагам

СДЕЛАНО

- Общий ИИ-чат — одна дверь для всех
- Облако в РФ: договор, NDA, маскирование
- Аренда GPU для тяжёлых задач
- Свои модели для конфиденциального
- Ступени: данные → инструмент

ДЕЛАЕМ

- ИИ-шлюз: единая панель управления ИИ
- Лимиты по деньгам и выбор модели под задачу
- Журнал: кто, что и сколько
- Перенос сервисов на инфраструктуру группы

ДУМАЕМ

- Права в базе знаний = права источника
- Безопасники на старте, а не на приёмке
- Проверка кода, написанного с ИИ
- Реестр агентов и MCP: что есть и что им разрешено
- Фиксация версий ИИ-компонентов

У ИИ в компании должен быть хозяин

Сам по себе контур не управляется: модели, цены и угрозы меняются каждые пару месяцев

ЧТО ЗА ЭТИМ СТОИТ

- Выбирает модели и ступени под задачи
- Держит счёт и лимиты под контролем
- Ведёт журнал, права агентов и плагинов
- Следит за обновлениями и уязвимостями
- Учит людей и собирает обратную связь

1

МИНИМУМ

Один ответственный

Человек, у которого это — работа, а не «по совместительству»

2

ПО МЕРЕ РОСТА

Своё подразделение

Когда ИИ во всех отделах. У нас — команда из четырёх человек

Нет своих людей или времени разбираться? Не обязательно начинать с нуля: есть команды, которые прошли этот путь на своём опыте и помогают другим. Мы — одна из них

Пять вопросов своему ИТ в понедельник

- 1 Какие наши данные уходят в нейросети — и куда именно?
- 2 Есть ли у сотрудников удобный официальный ИИ — или они в личных аккаунтах?
- 3 Видим ли мы, кто что спрашивает и сколько это стоит?
- 4 Какие ИИ-агенты и плагины у нас работают — и что им разрешено?
- 5 Позвали ли безопасников до пилота, а не на приёмку?

Сфотографируйте слайд. Полный чек-лист пришлю — контакт по QR-коду на следующем слайде

ИИ не запрещают — его маршрутизируют

Наши маршруты пока неидеальны.
Но мы знаем, что и куда уходит

А как это решаете вы? Давайте обсудим

Спасибо! Никита Дунов
nikita.dunov@metran.ru



Контакт одним сканом. Чек-лист
пришлю, с контуром — поможем