ИИ-АГЕНТЫ · УЧЁТНЫЕ СИСТЕМЫ · БЕЗОПАСНОСТЬ

Как обеспечить агентам доступ к учётным данным

Меры безопасности и необходимая инфраструктура



ДОСТУП У ИИ УЖЕ ЕСТЬ

ВОПРОС — ЧЕРЕЗ ЧТО

Девять из десяти пилотов ИИ не доходят до результата

95 %

пилотов генеративного ИИ не дали измеримого эффекта

MIT NANDA, 2025

88 %

пилотов не дошли до внедрения: из 33 — только 4

IDC и Lenovo, 2025

ОШИБКИ ПОДХОДА

1. Купили всем подписку — и ждут эффекта
2. Меряют сожжёнными токенами, а не результатом
3. Внедряют ИИ ради ИИ — без задачи и метрики
4. Ставят агента в середину неразобранного процесса
5. Перепрыгивают через данные

Причина не в моделях: пилот сделать легко, внедрить — нет.

Кто мы и почему пошли этим путём

ГК «КИБЕРНЕТИКА»

Интегратор учётных систем

- ✓ 100+ проектов внедрения
- ✓ Около 50 инженеров

Учётные системы на 1С · хранилище данных · ввод документов с ИИ · обвязка для агентов

1. **Нас просят: «просто подключите базу к чату»**
   Всё чаще и всё настойчивее.

2. **«Да» сказать нельзя**
   Это данные заказчиков: зарплаты, цены, договоры.

3. **«Нет» не работает**
   Без нас это сделают сами — и сделают хуже.

Третий путь — слой между агентом и базой. Как он устроен и на чём мы споткнулись.

Самый быстрый способ — и что он включает

Работает за вечер. Вот что при этом включилось

Чат с ИИ
Сотрудник задаёт вопрос

→

Готовый сервер-посредник
Подключается за вечер

→

База выставлена наружу
Иначе чат до неё не дотянется

Конфиденциальность

Всё, что вернула база, уходит в контекст модели — на серверы за рубежом

Целостность

Запрос с ошибкой даёт правдоподобную, но неверную цифру

Доступность

Тяжёлый запрос в рабочее время останавливает бухгалтерию

Персональные данные хранятся в базе на территории Казахстана — Закон РК «О персональных данных и их защите», статья 12.

Какая учётная запись у сотрудника: три контура

Личная или бесплатная

- ⚠ Будут ли учить модель на ваших данных — зависит от настроек
- ⚠ Договора с компанией нет
- ⚠ Журнала для проверки нет
- ⚠ Данные обычно обрабатываются за рубежом

Корпоративный тариф или доступ по договору

- ✓ Обучение на данных, как правило, отключено и закреплено договором
- ✓ Договор с юридическим лицом
- ✓ Журнал есть
- ⚠ Где обрабатываются данные — смотреть в договоре

Модель в своём контуре

- ✓ Данные не покидают периметр
- ✓ Обучения на ваших данных нет
- ✓ Журнал свой
- ⚠ Нужны свои серверы и люди

Вопрос не «каким ИИ вы пользуетесь», а «в каком контуре».

Один агент под администратором

Рано или поздно все будут знать о компании всё

Кладовщик спрашивает у агента зарплату директора — и получает ответ.

Закрытые данные

Агент ходит в базу под учётной записью с полными правами

Недоверенный текст

Комментарий в документе для агента — такая же команда, как ваша

Канал наружу

Агент может записать, отправить или показать прочитанное

Опасно сочетание трёх. Уберите одно — и атака не складывается.

Безопасность — свойство обвязки, а не модели

Не просите модель не делать — не давайте возможности

Инструменты
Что агент может вызвать

Права
Под чьими правами он ходит

Ключи
Где лежат и кто их видит

Журнал
Что записано о каждом действии

Инструкция в промпте — пожелание, а не граница. Модель сменится через полгода; права, шлюз и журнал останутся.

Обвязка — это проект, а не вечер с Claude

НАША ПЕРВАЯ ВЕРСИЯ

500 000+
строк кода

4/5
кода — за девять недель

30
дефектов нашёл аудит

ПЯТЬ САМЫХ ВАЖНЫХ

1. Ограничение описано, а код исполняет его слабее
2. Ошибка настройки песочницы выдавалась за успех
3. Неизвестный исход записывался как «не выполнено»
4. Предпросмотр почты писал в данные
5. Согласование не привязано к версии того, что исполнится

Нет заявленного без исполняемого

Отказывать при сомнении

У каждого действия есть тип

Чтение: путь одного вопроса

«Какая дебиторка у контрагента?» — шесть шагов от сотрудника до базы и обратно

1
Кто спросил
Вход по корпоративной учётной записи

2
Кто куда стучится
Наружу ходит только сервер обвязки; база — внутри сети

3
С чьими правами
С правами спросившего, не под общей учётной записью

4
Чем спрашивает
Проверенные инструменты, только чтение

5
Откуда данные
Хранилище с описанием, а не рабочая база

6
Что уходит модели
Обезличенные данные; всё записано в журнал

Логин и ключи агента — в хранилище секретов, а не в инструкции и не в файле настроек.

Права учётной системы в хранилище данных сами не переезжают — их строят заново.

Кто куда стучится: три схемы подключения

Чат в облаке — прямо к базе

Базу или сервер перед ней открывают из интернета

Быстро, но точка входа — снаружи

Агент на компьютере сотрудника

Наружу ничего не открыто, но ключи и контроль разбросаны по рабочим местам

Каждый компьютер — отдельная точка риска

Сервер обвязки внутри сети

Наружу ходит только он — и только к модели. База опубликована лишь внутри сети

Агент входит в базу под своей учётной записью

Публиковать базу придётся в любом случае. Вопрос — кому она видна.

Права каждого пользователя: три слоя

Агент не должен знать больше того, кто его спросил

1

Запрос — с правами спросившего

База сама не отдаёт лишнего, как бы ни был задан вопрос

Это граница

2

Слой контроля запросов

Проверяет вопросы пользователей и замечает попытки получить чужое

Второй слой: фильтр можно обойти

3

Журнал и проверка

Кто спросил и что получил; тест на двух пользователях с разными правами

Так это доказывается

Кладовщик спрашивает зарплату директора — база отвечает отказом, а попытка остаётся в журнале.

Если агент сам пишет запросы

Ошибка в условии

Не включил последний день периода — итог неверный, но правдоподобный

Зависание базы

Тяжёлый запрос в рабочее время останавливает работу пользователей

Не тот источник

Взял не тот регистр — цифра не сходится с отчётом

Навык получения данных пишет аналитик

И сверяет результат с отчётом учётной системы. Агент выбирает проверенный инструмент и подставляет параметры.

Пределы на каждый запрос

Число строк, время выполнения, один запрос за раз. В ответе — период, источник и признак «данные неполные».

ETL и хранилище: анализ без риска для рабочей базы

Базы 1С
Работают как работали

→

ETL
Выгружает данные отдельно, не мешая пользователям

→

Хранилище данных
Данные проверены и приведены к одному виду

→

Описание данных
Что где лежит и как правильно считать

→

Агент
Сам строит запросы и анализирует

Нагрузка

Тяжёлый запрос не остановит бухгалтерию

Правильность

Правила расчёта записаны в описании; итоги сверяются с учётной системой

Оговорки

Права строятся заново; данные отстают — агент называет дату актуальности

Персональные данные в хранилище для агента можно просто не выгружать — это самое надёжное обезличивание.

Запись: только через конвейер

1 Найти
Сначала поиск в справочниках, потом создание

→

2 Уточнить
Недостающее спросить у человека, а не придумать

→

3 Проверить
Арифметику, итог и дубли проверяет код

→

4 Черновик
Документ не проведён; проводит человек

СТУПЕНИ АВТОНОМИИ

Советует
Человек решает и делает сам

Готовит черновик
Человек проверяет и проводит

Выполняет по кнопке
Человек подтверждает каждое действие

Действует сам
Только мелкое и безопасное

Деньги, договоры и приём на работу — никогда без человека. Это не настройка, а архитектура.

Необходимая инфраструктура: шесть слоёв

Вход
Корпоративные учётные записи

Агенты
Обвязка с правами и журналом

Свой RAG
Поиск по документам внутри контура

Обезличивание
Персональные данные — не в облако

Шлюз моделей
Ключи, лимиты и журнал в одном месте

Модели
Локальные и облачные

Локальная модель — для чувствительного

Персональные данные и коммерческая тайна не покидают периметр.

Обезличить, отправить, вернуть

Локальная модель заменяет имена и номера; в облако уходит обезличенный текст; в ответ данные подставляются обратно.

Свой RAG, а не личный NotebookLM

Удобно, но документы компании оказываются в личной учётной записи.

Личная бесплатная учётная запись — это публикация в интернете: ни договора, ни журнала.

Обезличивание: туда и обратно

Данные из базы
С именами и номерами

→

Локальная модель
Заменяет имена и номера метками

→

Облачная модель
Видит «Контрагент 17», а не имя

→

Обратная подстановка
Метки заменяются настоящими значениями

→

Ответ
Пользователь видит реальные данные

Структурные поля — правилом
Известно, в каком реквизите ФИО и ИИН

Свободный текст — локальной моделью
Комментарии, письма, сканы

Таблица соответствия — внутри
За периметр она не выходит

Это снижает риск, а не снимает его: человека выдают должность, подразделение и сумма.

ИИ пишет код, а не трогает данные

Лучший способ защитить данные от модели — не показывать их модели

1

Модель предлагает

Распознать, понять, сопоставить — на минимальном фрагменте

2

Код проверяет

Сверяет со справочниками и считает арифметику

3

Человек подтверждает

И отвечает за результат

При разработке — ИИ пишет код обмена

Его можно прочитать, проверить тестом и повторить. Данные через модель не проходят.

В работе — только эвристика

Модель нужна там, где нельзя написать правило. Её ответ — структура, которую проверяет код.

Внедрять ИИ — как внедрять ERP

ОПЫТ ВНЕДРЕНИЙ ERP

70–80 %

внедрений ERP и цифровых трансформаций заканчиваются неудачей

Оценка, которую приводит Эрик Кимберлинг, Third Stage Consulting, 2024

ПЯТЬ ПРИЧИН — ПО КИМБЕРЛИНГУ

1. Завышенные ожидания
2. Спешка: от выбора — сразу к внедрению
3. Технология ради технологии, без видения у руководства
4. Слабое управление изменениями
5. Не определено, что считать успехом

С ИИ причины те же. Поэтому внедрение — это проект: обследование, роли, данные, этапы.

С чего начать

1. **Разрешённый путь для сотрудников**
   Корпоративные учётные записи и правило «что куда можно»
2. **Агент — отдельная учётная запись**
   Минимальные права, сначала только чтение
3. **Запрос — с правами спросившего**
   Проверка: два пользователя, разные ответы
4. **Проверенные инструменты и хранилище**
   Частые вопросы — инструментами, аналитика — не в рабочей базе
5. **Запись — только черновиком**
   С подтверждением человека

ВОЗГЛАВИТЬ АВТОМАТИЗАЦИЮ

Дать разрешённый путь, который удобнее теневого

Семён Литвинов
Сооснователь и технический директор ГК «Кибернетика»

20+ лет в корпоративной автоматизации · 60+ проектов

+7 (701) 729 05 51
webinfo@cybernetica.kz

cybernetica.kz