# ИИ-газета ДЛЯ АЛЕКСЕЯ

№ 10 ЧЕТВЕРГ, 12 НОЯБРЯ 2026 **АГЕНТЫ В ШТАТЕ**


*«Любая достаточно развитая технология неотличима от магии». — Артур Кларк*

**ОРГАНИЗАЦИЯ** КИТАЙ

## Baidu: следующий шаг ИИ — «умная организация»

Основатель Baidu Робин Ли назвал следующей эпохой ИИ «умную организацию»: цифровые работники должны войти прямо в продажи, поддержку, разработку и операционку, а не просто ускорять отдельных сотрудников. Внутри самой Baidu число агентов, которые работают каждый день, за год выросло больше чем вшестеро, а выполненных ими задач — ещё сильнее. Удачные приёмы людей Baidu сохраняет как общие навыки, которые может вызвать любой агент.

**СОЛО** США

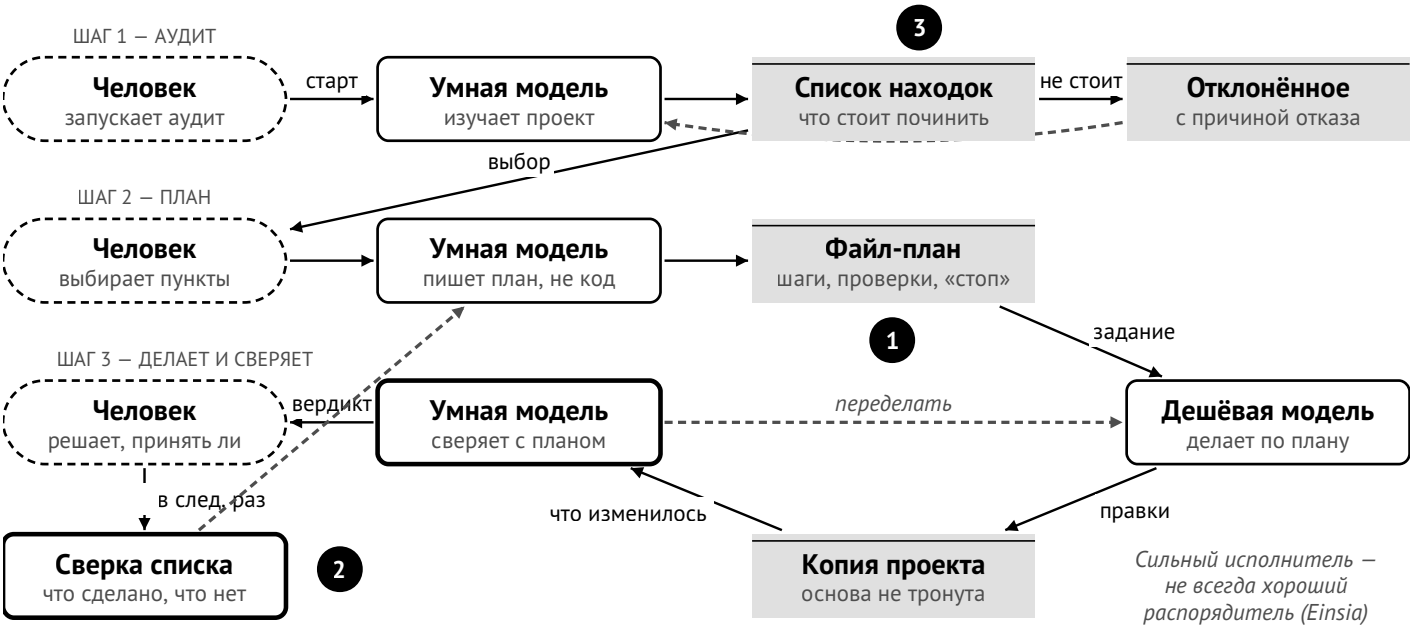
## Основатель ведёт агентство с «братством» агентов

Уильям Имох — единственный основатель Hackmamba, маркетингового агентства для разработчиков, в котором около 25 человек. Управлять ему помогает «братство» ИИ-агентов в Grok Bot: каждую роль основателя он отдал герою «Властелина колец». Агентам он открыл почти все рабочие сервисы, кроме одного, и больше всего боится не замены людей, а зависимости от ИИ.

*Grok Bot — тот же сервис, где работают ваши ИИ-сотрудники.*

**СХЕМА** ДИАГРАММА ПОСЛЕДОВАТЕЛЬНОСТИ

### Умный планирует, дешёвый делает: как разделить работу между дорогой и дешёвой моделью




**1** переделка, пока правки не совпадут с планом **2** в новой сессии сверяют, что сделано и что застряло, и освежают планы
**3** отклонённое хранится с причиной и не всплывает снова — агент — человек — хранилище — обратная связь

**ДОСТУП** РОССИЯ

## Anthropic закрывает Claude для компаний под российским контролем

С 12 ноября Anthropic применяет обновлённый список «поддерживаемых регионов»: Claude недоступен организациям, зарегистрированным в России или контролируемым россиянами. Запрет касается чат-бота, Claude Code, API и доступа через посредников — даже если компания зарегистрирована в другой стране. Компания называет это разъяснением старых правил и объясняет подготовкой к выходу на биржу.

**ЧИПЫ** США

## Модель Anthropic сама перевезла Claude на чипы AMD

Anthropic рассказала инвесторам, что её внутренняя модель Mythos почти без участия людей перенесла Claude на видеокарты AMD. Почти весь низкоуровневый код под новый чип модель написала сама — за дни вместо привычных месяцев работы десятков инженеров. Теперь Claude работает на чипах четырёх семейств, а главная защита Nvidia — привязка разработчиков к её программам — слабеет.

**ДЕНЬГИ** США

## Stripe купил OpenRouter — «переходник» к сотням моделей

Платёжный сервис Stripe завершил покупку OpenRouter — площадки, через которую разработчики одним подключением получают модели десятков компаний. Вместе они обещают помогать компаниям распределять запросы между моделями и тратить меньше токенов. Большая часть трафика OpenRouter уже идёт от агентов, а не от людей.

**АГЕНТЫ** США

## Google: агент отвечает не текстом, а экраном

Google выпустила первую стабильную версию A2UI — открытого способа, которым агент отвечает готовым кусочком интерфейса: формой, карточкой, кнопками. Агент лишь описывает, что показать, а приложение рисует это своими элементами — на сайте, в телефоне или внутри Claude и Gemini. Стандарт уже используют Atlassian, Bloomberg и ByteDance.

**БЕЗОПАСНОСТЬ** США

## Взломщик просто попросил агента назвать свой ключ

Организация METR, которая проверяет ИИ-модели, рассказала: у её исследователя тихо отключилась самописная защита входа в панель агентов. Чужой человек нашёл страницу, попросил агента выдать ключ к моделям и неделями тратил с него кредиты. Никто не заметил: лимита расходов не было, а панель прятала подозрительные запросы. Совет из обсуждения: держать настоящий ключ вне агента и ставить дневной лимит трат.

**ПУТЕШЕСТВИЯ** США

## United Airlines запретила ИИ-агентам покупать билеты за пассажиров

Авиакомпания United запрещает личным ИИ-помощникам бронировать рейсы и регистрироваться на них от имени пассажиров. Причины — риск утечки паролей и платёжных данных, случайные покупки и траты миль, а ещё правило, по которому пассажир сам подтверждает, что в багаже нет запрещённого. Southwest идёт обратным путём: её рейсы видны прямо в ChatGPT.

**ЛЮДИ** КИТАЙ

## «Учитель роботов» в Китае оказался работой на конвейере

Журналист 36Kr устроился «сборщиком данных» — так в Китае называют новую официальную профессию людей, которые записывают движения для обучения роботов. На деле это поток: весь день в перчатке с датчиками повторять простые действия вроде выдавливания зубной пасты, без договора и без понимания, куда уходят данные. Программа следит за числом повторов и их качеством, и пока норма не выполнена, уйти домой нельзя.

**ДОМ** США

## Учитель математики собрал «мозг семьи» на Claude Code

Американский преподаватель Скотт Фаррар устал от чатов с ИИ, которые всё забывают, и перенёс домашние дела в Claude Code. Его «мозг семьи» — папка простых текстовых заметок, которую он смотрит в Obsidian: техника, гарантии, страховки и общий список дел. С этой базой он выбирает страховку для машины и планирует ремонты, а жена пользуется той же системой.

*Шутка с Reddit: Бэтмен с шестидесятых гонял ИИ на Бэткомпьютере — и ни разу не переспросил.*

**GROK BOT**

### Видео про стартап и жалобы на сбои

Официальный YouTube-канал Grok показал, как стартап после первого крупного раунда работает на Grok Bot · подтверждено. Пользователи форума Cursor: «компьютер» бота зависает или не запускается, браузер блокирует ошибка сохранённых данных входа · слух, ответа нет. Запуски по расписанию не видят инструменты почты, приложение в Slack отвечает ошибкой · слух. После версии 0.79.2, по словам пользователя, боты не выполняют локальные команды · слух.

**РЫНОК**

### Nvidia штормит, OpenAI растёт

Совет директоров Nvidia, по данным WSJ, собирается решать судьбу Дженсена Хуанга после новых сообщений о его романах, акции резко падали; сам Хуанг, по данным 36Kr, вышел на работу и извинился перед сотрудниками. OpenAI впервые заработала за квартал около 10 млрд долларов — помогли корпоративные клиенты, но убыток тоже растёт. Траты американских компаний на ИИ в октябре почти перестали расти, новый двигатель — поддержка клиентов.

**ИНСТРУМЕНТЫ**

**Kit** общая память для Claude, Codex, Cursor и других: контекст о вас лежит на вашем Mac, а не у поставщика.

**Pomerado** США по короткому описанию превращает любой сайт в подключение (MCP) для агентов меньше чем за час; есть открытая версия.

**Yogurt** США бесплатная открытая замена Granola: пишет созвоны в фоне, не заходя на них, и всё остаётся у вас.

**ha-mcp** управление умным домом Home Assistant через Claude, ChatGPT и других ассистентов.

**ПОИГРАЕМ** РАЗМИНКА ПО ПОНЯТИЯМ ИИ; ОТВЕТЫ ПЕРЕВЁРНУТЫ ВНИЗУ. НЕЗНАКОМОЕ — СПРОСИТЕ СВОЕГО БОТА.

**НАЙДИ ЛИШНЕЕ**

**1.** Ключ API · Пароль · Токен доступа · Системный промпт

**2.** Оркестратор · Исполнитель · Проверяющий · Квантование

**ПОРЯДОК РАБОТЫ ПОИСКА ПО СВОЕЙ БАЗЕ (RAG)**

**а.** Модель отвечает по найденному

**б.** Вопрос превращают в запрос

**в.** Документы заранее режут на кусочки

**г.** Находят похожие кусочки

**д.** Найденное кладут в промпт

**ВЕРНО ИЛИ НЕТ?**

**1.** Квантование уменьшает модель, огрубляя числа в её весах.

**2.** Окно контекста — это сколько модель помнит между разными чатами.

**3.** Защита «fail-open» при сбое не пускает никого.

**НА ПОДУМАТЬ**

- *Что из домашних дел вы записали бы в общую «базу семьи», а что оставили бы только в голове?*

**Ответы:** Лишнее: 1) системный промпт (инструкции модели, остальное — секреты для входа); 2) квантование (сжатие модели, остальное — роли в команде агентов). Порядок: в, б, г, д, а. Верно/нет: 1) верно; 2) нет, это сколько текста она видит за один раз; 3) нет, пускает всех; не пускает — «fail-closed».

**Источники. журнал/блог** — Baidu: умная организация, Anthropic и Россия, Mythos и AMD, Stripe и OpenRouter, A2UI 1.0, Сборщики данных для роботов, Рынок ИИ; **рассылка** — Hackmamba и «братство» агентов, Семейный мозг; **форум** — Инцидент METR, United против агентов, Схема, Инструменты; **репозиторий GitHub** — Схема, Инструменты; **отчёт агента Ультра** — Grok Bot. Ника · формат v3 · 12.11.2026