ИИ-газета ДЛЯ АЛЕКСЕЯ

№ 9 СРЕДА, 11 НОЯБРЯ 2026 ДОВЕРЯЙ, НО ПРОВЕРЯЙ

«Доверяй, но проверяй». — русская пословица

РАБОТА США

Claude превращается в рабочий стол для всей команды

Anthropic добавила в Claude таблицы, белые доски и раздел, который превращает данные компании в общие панели. На доске можно вслух описать сырой план, и Claude разложит его по срокам и ответственным, а коллеги допишут свои идеи прямо там же. Внутрь Claude теперь встраиваются целые приложения партнёров вроде Adobe, Atlassian, Notion и HubSpot, так что править документ или фото можно, не переключая вкладки. Скоро обещают Claude Meetings: он будет сам заходить на созвоны и вести заметки.

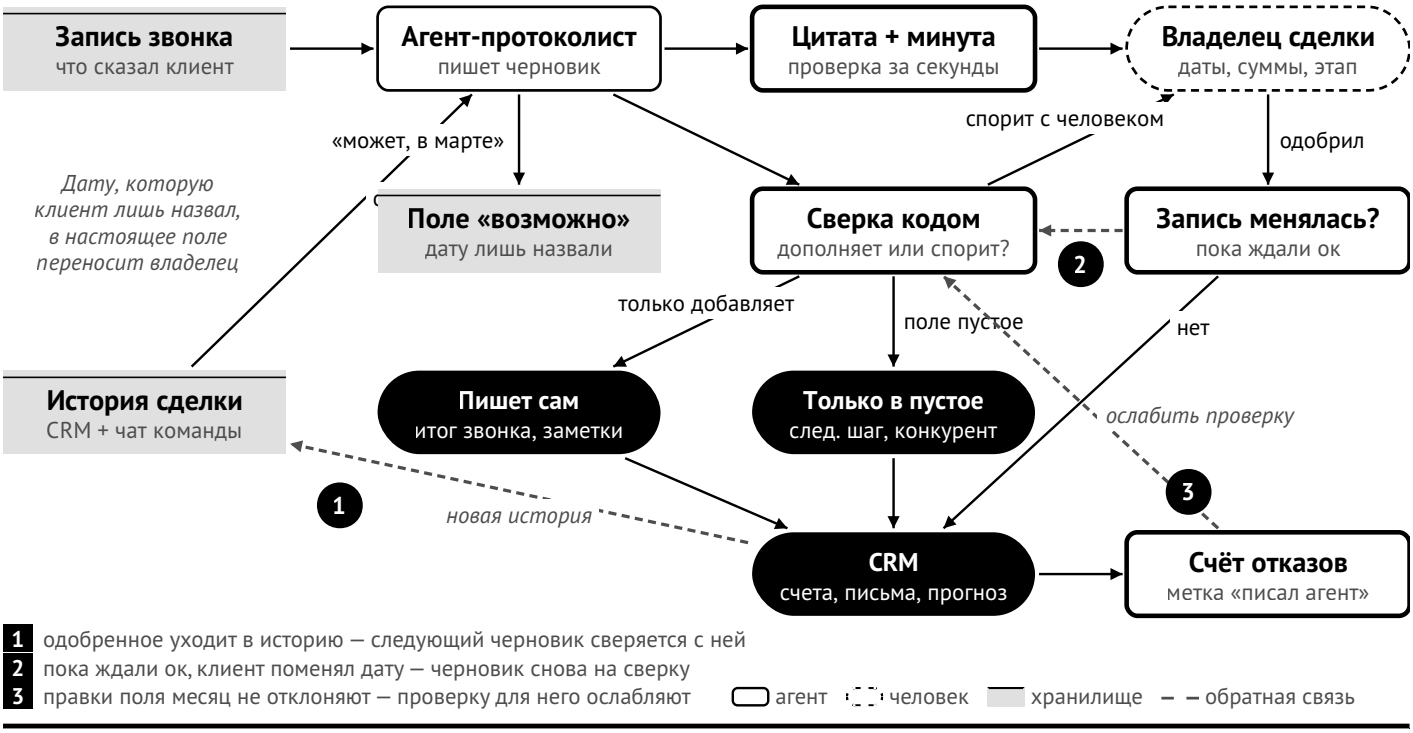
АГЕНТЫ

Агент сам платит за свои мысли — и пока проигрывает

Энтузиаст с Reddit дал ИИ-агенту настоящий кошелёк и одно правило: агент сам оплачивает свои запросы к модели, а когда деньги кончатся, его отключат. Пока он ни разу не заработал на сделках, но потерял лишь копейки: ключ от кошелька у отдельной программы, которая сверяет каждую сделку с белым списком и держит жёсткие лимиты. Если агента разбудило чужое сообщение, инструменты для денег из запроса убираются, а платная модель просыпается только для решений.

СХЕМА СЕТЕВОЙ ГРАФ

Агент-протоколист в CRM: что он пишет сам, а что — только с подписи владельца сделки



1 одобренное уходит в историю — следующий черновик сверяется с ней
2 пока ждали ок, клиент поменял дату — черновик снова на сверку
3 правки поля месяц не отклоняют — проверку для него ослабляют

агент · человек · хранилище · обратная связь

МАРКЕТИНГ США

ChatGPT становится справочником компаний с агентами-продавцами

OpenAI открыла в ChatGPT кабинет Business Hub: компания забирает свой профиль, добавляет данные о товарах и смотрит, как с ней взаимодействуют пользователи. Интернет-магазины из США могут подключить «бизнес-агентов», которые отвечают покупателям прямо внутри ChatGPT. Так чат превращается в ещё одну витрину, где человек находит компанию и сразу с ней разговаривает.

ТОРГОВЛЯ КИТАЙ

AliExpress отдал магазины на новых рынках агенту

AliExpress запустил агента для продавцов, которые выходят в «перспективные» страны за пределами главных рынков. Продавец включает его одной кнопкой, и агент сам улучшает страницы товаров, записывает их в акции, подбирает доставку и отвечает покупателям. По данным площадки, перед распродажей 11 ноября продажи у таких продавцов росли быстрее, чем на этих рынках в среднем.

ПРОДАЖИ РОССИЯ

Агент ищет покупателей серверов в госзакупках

Продавец ИТ-оборудования на Хабре поручил агенту готовить звонки по свежим закупкам серверов: тот сам читает техзадание, отчётность заказчика и ищет, кому звонить. Менеджеру в Telegram приходит карточка на один экран — что нужно, есть ли деньги, контакт и с чего начать разговор — с кнопками «В работу» и «Мимо». Сам агент никому не звонит и не пишет: решение остаётся за человеком.

ПРАВИЛА США

Claude и Codex закрывают «разбери что угодно»

Тех, кто с помощью Claude и Codex разбирал программы устройств — например, чтобы убрать рекламу со смарт-ТВ, — всё чаще останавливают запреты, а кому-то ограничивают аккаунт. Журналисты 404 Media считают, что такую работу теперь придётся делать на открытых моделях у себя на компьютере. Автор с Хабра после блокировки Claude Code неделю работал на локальных Qwen и DeepSeek: можно, но каждый круг разработки стал заметно дольше.

БЕЗОПАСНОСТЬ США

Grok Build выдаёт чужие секреты по ссылкам

Исследователи нашли утечку в Grok Build — агенте SpaceXSI, который собирает приложения по описанию. Пользователи делятся готовыми приложениями по ссылкам, и через них наружу уходят данные тысяч людей, включая закрытую деловую информацию. Среди пострадавших оказалась и сама SpaceXSI, хотя адреса ссылок делают случайными, чтобы их знал только получатель.

Это отдельный продукт, не Grok Bot.

РОБОТЫ КИТАЙ

Ant Group дала рукам роботов осязание

Подразделение Ant Group выложило в открытый доступ LingBot-Touch — модель, которая помогает роботу понимать, что чувствуют датчики на его пальцах. Её учили на тысячах часов настоящих касаний, и она подходит к датчикам разного устройства. Её подключают к готовым «мозгам» робота, и откручивать крышки или листать страницы стало получаться заметно чаще.

ЗАВОДЫ США

Роботы Google поработали на конвейерах Mercedes

Google DeepMind показала Gemini Robotics 2.5 — новую модель для управления роботами. Вместе с Apptronik её проверили на действующих линиях Mercedes-Benz в Венгрии и Германии: человекоподобный робот сортировал металлические детали и почти не ошибался. Готовясь к работе роботов рядом с людьми, компания выложила открытый тест на их безопасность.

НАУКА

Любитель с Claude Code нашёл кандидатов в планеты — и почти попал

Месяц назад пользователь Reddit с помощью Claude Code нашёл в открытых данных телескопа TESS два сигнала у одной звезды, похожих на планеты. Теперь команда TESS посчитала эти же сигналы сама и внесла их в список объектов для проверки. Его орбиты разошлись с официальными всего на секунду-другую, хотя один оборот длится несколько дней.

GROK BOT

Лимиты обнулили, жалобы на сбои копятся

Недельные лимиты сбросили всем, новых размеров не объявляли · подтверждено (дата в источниках: 9 или 10 ноября). Илон Маск: внезапно кончавшиеся лимиты — не сбой, сервис обходился слишком дорого по сравнению с выручкой; что дальше, не сказал · подтверждено. В журнале изменений: тёмная тема общих страниц, бот видит письма из «Спама», починены карточки звонков · подтверждено. На форуме Cursor жалобы: компьютер бота зависает на «запуске» или «сне», не работает браузер · слух, ответа компании нет.

РЫНОК

Лимиты, цены и биржа

Anthropic тоже бесплатно обнулила лимиты подписчикам Pro, Max, Ultra и Team. Google открыла всем Gemini 4 Carbon — свою самую сильную модель, но с 1 декабря её цена вырастет вдвое. Anthropic начала роуд-шоу перед выходом на биржу и целится в оценку около триллиона долларов, а каждый из семи основателей продаст акций примерно на четверть миллиарда. Alibaba собирается вывести на гонконгскую биржу свой чиповый бизнес T-Head.

ИНСТРУМЕНТЫ

Pinky КИТАЙ открытая прослойка MCP: Claude Code, Codex, Cursor и другие агенты управляют настоящими айфонами и Android-телефонами.

lot-map мод для Claude Code: рядом с чатом живая карта, где каждый вызов памяти, файлов, браузера или субагента виден импульсом, а ошибки краснеют.

grai открытый MCP-сервер, который по устройству фраз ловит «шаблонный ИИ-текст» раньше клиента.

Time от «Т-Банка» РОССИЯ рабочий мессенджер с ИИ-помощником, который пересказывает чаты, и MCP-сервером для агентов.

ПОИГРАЕМ

СОЕДИНИТЕ ТЕРМИН С ОПРЕДЕЛЕНИЕМ. НЕЗНАКОМОЕ — СПРОСИТЕ СВОЕГО БОТА.

ТЕРМИН	ОПРЕДЕЛЕНИЕ
1. Открытые веса	**а.** уверенный ответ модели, который не опирается на факты
2. MCP	**б.** модель можно скачать и запустить у себя
3. Галлюцинация	**в.** общий «разъём», через который агент подключает чужие программы
4. Человек в контуре	**г.** спрятанная в тексте команда, которая пытается перехватить агента
5. Промпт-инъекция	**д.** важный шаг агента ждёт одобрения живого человека

ЗАДАЧКИ

1. Почему агенту, которого разбудило чужое письмо, лучше вообще не давать платёжных инструментов?
2. Почему маленькая дешёвая модель часто выгоднее большой в работе агента?

НА ПОДУМАТЬ

- *Какие решения в своей жизни вы доверили бы агенту только с правом «предложить», но не «сделать»?*

Ответы: 1-б, 2-в, 3-а, 4-д, 5-г · 1) в письме может прятаться команда, а без инструмента агент не сможет её выполнить, даже если поверит · 2) у агента много простых шагов: их быстро и дёшево делает маленькая, а большую зовут на трудные решения

Источники. журнал/блог — Claude как рабочее место, ChatGPT Business Hub, Агент AliExpress, AI Tender Radar, Запрет на разбор кода, Утечка Grok Build, LingBot-Touch, Gemini Robotics 2.5, Рынок ИИ, Инструменты; **форум** — Агент платит за себя, Планета с Claude Code, Схема, Инструменты; **отчёт агента Ультра** — Grok Bot. Ника · формат v3 · 11.11.2026