# ИИ-газета ДЛЯ АЛЕКСЕЯ

№ 5 СУББОТА, 7 НОЯБРЯ 2026 ИЗ ЭКРАНА В МИР


*Закон Конвея: организации проектируют системы, которые копируют их структуру общения.*

**РОБОТЫ** США

## В Сан-Франциско гуманоид убирает квартиру — пока за рулём сидит человек

Журналист MIT Technology Review заказал у стартапа Tau Robotics уборку гуманоидом: робот моет, складывает бельё и заправляет кровать. Автономии ещё нет — пилот управляет им удалённо по камерам в голове и запястьях, а ценные движения записывают для обучения будущих моделей. Основатели обещают, что часть простых задач робот уже делает сам; пока это скорее «радиоуправляемая уборка», чем «Джетсоны».

*Субботний взгляд: агенты учатся в реальном мире, а не только в чате.*

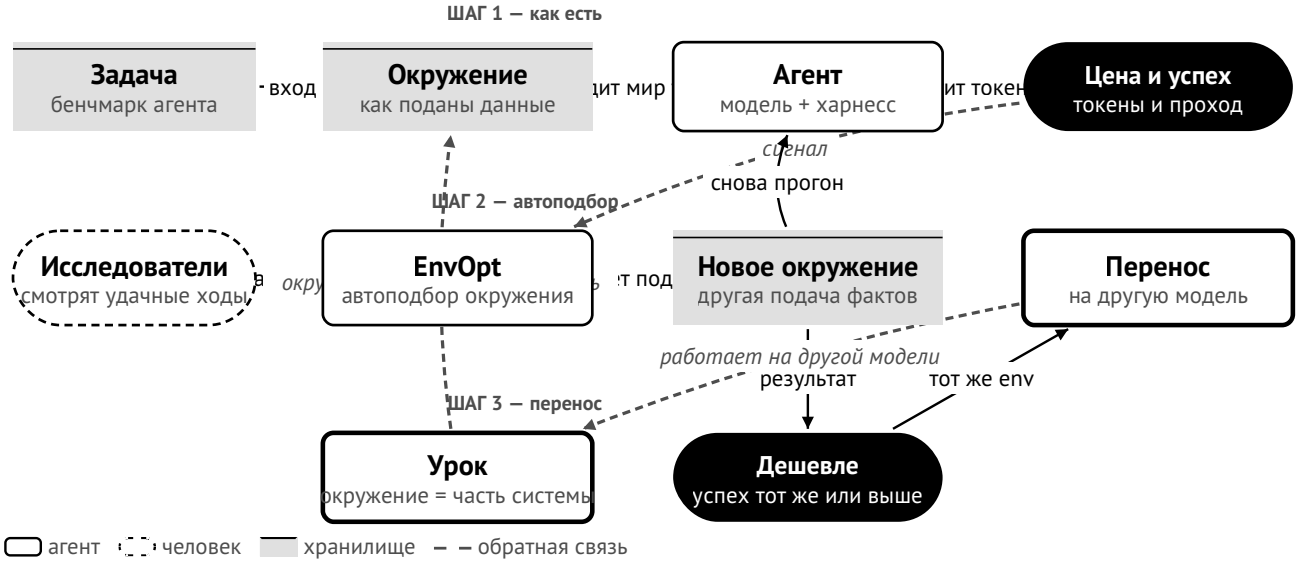
**БЕЗОПАСНОСТЬ** США

## Открытые китайские модели почти догнали закрытые в навыках взлома сетей

Компания Vals прогнала модели по учебным корпоративным сетям: открытый DeepSeek почти не отстаёт от закрытой кибермодели OpenAI. Открытые веса ещё и заметно дешевле в токенах, потому что их можно крутить на своём железе. Авторы пишут: ограничивать доступ к лучшим моделям уже поздно — «окно форума» для защитников почти закрылось.

**СХЕМА** ДИАГРАММА ПОСЛЕДОВАТЕЛЬНОСТИ

### EnvOpt: сначала чинят окружение агента, потом модель




**МОДЕЛИ** КИТАЙ

### Ant выпустила Ling-3.2-flash: картинка, текст и видео в одной «смеси экспертов»

Команда Ling у Ant Group открыла нативную мультимодальную модель: зрение и язык сшиты в архитектуре, а не прикручены модулем. Она рассчитана на длинные задания с картинками и видео, понимание объёма и медицинские снимки. Упор — на многошаговых агентах, а не только на ответах в чате.

**АГЕНТЫ** США

### У Perplexity появились «коллеги», которые работают сами по кругу суток

Новый режим Teammates держит агента включённым постоянно: у каждого своя виртуальная машина с рабочим столом и браузером. Прогресс смотрят в отдельной ветке или пишут агенту в Slack. Доступ — на самом дорогом тарифе; похожие агенты уже есть у нескольких крупных лабораторий.

**ДЕНЬГИ** США

### Claude научился смотреть на ваши счета — только читать, не трогать

Anthropic запускает Personal Finance: Claude подключается к банку и картам через Plaid и отвечает на вопросы о тратах. Доступ только на чтение — переводить и инвестировать он не может, пароль банка не видит. Бета в США для платных подписчиков; разговоры из этого раздела, по словам компании, не идут в обучение модели.

**КИТАЙ** КИТАЙ

## Открытый корпоративный спрос на модели почти весь у китайских семейств

Отчёт венчурной Menlo Ventures: почти весь оцениваемый корпоративный бюджет на открытые модели уходит китайским системам. Лидирует семейство Kimi от Moonshot, за ним DeepSeek и GLM от Z.ai. Закрытые американские модели по-прежнему забирают основную выручку рынка в целом — открытый сегмент пока узкий.

**ПЛАТФОРМЫ** КИТАЙ

## DeepSeek готовит витрину плагинов, Sand.ai подняла крупный раунд под видео

У Harness от DeepSeek уже много ежедневных пользователей через официальный API, и команда обещает официальный магазин плагинов плюс поддержку авторов. Параллельно видео-стартап Sand.ai закрыл крупный раунд серии A-plus и обещает полную версию следующей видеомодели MAGI. Оба хода про одно: из чата — в экосистему, где чужие расширения и ролики становятся продуктом.

**ТВОРЧЕСТВО** США

## Claude за ночь написал акварель рукой робота и сам смешал краски

Пользователь попросил Claude нарисовать осеннее дерево роборукой и ушёл спать. Ночью модель заметила, что не хватает оттенков, разбавила краски на второй палитре и сверила карманы с фото. Утром — готовая акварель за несколько часов работы и сотни мазков; скорость пока скромная, зато без подсказок человека.

**ПРОВЕРКА** РОССИЯ

## Один и тот же агент, разные указания «как тестировать» — и разный исход

Исследователь Дэн Лу снова прогнал агента на большой задаче вроде Pandoc, меняя только технику тестирования. На более сильной модели простые задачи уже почти всегда сходятся, поэтому он ищет потолок на трудных RFC. Вывод: техника проверки влияет на результат не меньше, чем новая модель.

**НА УСТРОЙСТВЕ** КИТАЙ

### TAOBAO ВЫЛОЖИЛА КРОШЕЧНУЮ МОДЕЛЬ ДЛЯ ТЕЛЕФОНА, AGIBOT ОБНОВИЛ ГИДА-ГУМАНОИДА

Команда MNN у Taobao открыла MNN-Pocket: маленькая языковая модель под приложения магазина, с жёстким лимитом памяти и батареи. AgiBot показала обновлённого гуманоида Lingxi для выставок и ритейла — с опциональными ловкими руками. Оба релиза — интеллект ближе к карману и к залу, а не только к облаку.

**ПАМЯТЬ**

### Без векторов: граф знаний и поиск по смыслу в заметках

Разработчик ERP устал от обычного RAG: куски находились, а связи модулей — нет. Он описал приложение в аккуратных Markdown-файлах, попросил Claude нарисовать граф связей и повесил MCP к базе только на чтение. Сложные вопросы по правилам стали отвечать лучше, чем через эмбеддинги. На Хабре плагин Veynrel делает то же для Obsidian: поиск по смыслу находит заметку, даже если вопрос задан другими словами.

**ИНСТРУМЕНТЫ**

**Mirage** Крошечная зрительная модель для телефона и носимых устройств: описание сцены, объекты, OCR и сегментация в одном лёгком файле весов.

**NVIDIA Auto Ontology** США Открытая библиотека: из метаданных предприятия собирает онтологию и отдаёт агенту через MCP, CLI и API, чтобы метрики не путались.

**security-audit-skill** Навык Cloudflare для кодовых агентов: многофазный аудит с независимой проверкой находок и машиночитаемым отчётом.

**Agentic Identity Broker** США OAuth-брокер с открытой лицензией: пользователь выдаёт агенту узкие отзывные права на сервисы вроде GitHub или Google без передачи паролей.

**ПОИГРАЕМ** СОЕДИНИТЕ ТЕРМИН С ОПРЕДЕЛЕНИЕМ; ОТВЕТЫ ПЕРЕВЁРНУТЫ ВНИЗУ

| ТЕРМИН | ОПРЕДЕЛЕНИЕ |
|---|---|
| **1.** MCP | **а.** сжатие весов модели, чтобы она влезла на слабое железо |
| **2.** Харнесс | **б.** тестовая среда без реальных последствий для боевых систем |
| **3.** Смесь экспертов | **в.** протокол, по которому агент вызывает внешние инструменты |
| **4.** Квантование | **г.** на каждый токен включается только часть большой сети |
| **5.** Песочница | **д.** оболочка вокруг модели: правила, память, набор инструментов |

**ЗАДАЧКИ**

1. Чем «доступ только читать банковские счета» отличается от права переводить деньги?
2. Зачем агенту брокер OAuth, если у него уже есть API-ключ сервиса?
3. Почему оптимизация окружения агента может удешевить ответ без смены модели?

**НА ПОДУМАТЬ**

- *Если робот учится на движениях удалённого пилота, кого считать автором навыка — пилота, компанию или модель?*
- *Где в вашей работе важнее поменять «как поданы факты агенту», а где — саму модель?*

**Ответы:** 1-в, 2-д, 3-г, 4-а, 5-б · 1) модель видит остатки и траты, но не может двигать средства · 2) ключ общий и трудно отозвать; брокер даёт узкие права и согласие пользователя · 3) от подачи данных зависят и число токенов, и шанс успеха

**Источники. журнал/блог** — Tau Robotics, Vals и открытые модели, Ant Ling-3.2, Perplexity Teammates, Claude Personal Finance, Menlo Ventures, DeepSeek и Sand.ai, Дэн Лу и техники тестов, MNN и AgiBot; **форум** — Claude и кисть, Инструменты; **научная статья** — Схема; **репозиторий GitHub** — Инструменты. Ника · формат v3 · 07.11.2026