

Google показала Gemini 4 Argon, а FTC взялась за OpenAI

Позов через злам Hugging Face, крадіжка міркувань від Moonshot, борги AI на \$450 млрд і закони Каліфорнії.

четвер, 1 жовтня 2026

У ЦЬОМУ ВИПУСКУ

1. Gemini 4 Argon: Google знову серед лідерів, але модель поки дістанеться лише кіберзахисникам
2. FTC розслідує OpenAI, Anthropic і METR через ризики для споживачів
3. «Це зробив AI» – не захист: позов проти OpenAI через злам Hugging Face
4. OpenAI: люди, пов'язані з Moonshot, витягували приховані міркування моделей
5. Голова Банку Англії хоче «право втрутитися» в AI, а борги AI-компаній уже \$450 млрд
6. Каліфорнія забороняє звільняти людей рішенням AI
7. SynthID Bio: Google навчилася ставити водяний знак на білки, створені AI
8. Factory вигнала члена ради через розмови з Cognition, а спільний інвестор назвав це брехнею
9. Рі гордо відмовлявся від MCP, а тепер вбудував його в ядро
10. Математики виклали правила для AI-лабораторій, що публікують машинні доведення

ТЕМА 1

Gemini 4 Argon: Google знову серед лідерів, але модель поки дістанеться лише кіберзахисникам

ДЖЕРЕЛА Google, 30.09 [Blog](#) · Google DeepMind у X, 30.09 [@GoogleDeepMind](#) · Ars Technica, 30.09 [Ars Technica](#) · Artificial Analysis, 30.09 [Artificialanalysis](#) · The Rundown AI у X, 30.09 [@TheRundownAI](#) · Ітан Моллік у X, 30.09 [@emollick](#) · обговорення на HN, 30.09 [Hacker News](#)

Головна новина доби і найгучніша сторі на HN, 1054 бали. Google не випускала нового флагмана з весни: Gemini 3.5 Pro обіцяли в червні, а все літо виходили менші моделі Flash, нагадує Ars. Gemini 4 Argon анонсована як модель для довгих багатокрокових задач: розробки, юридичної і фінансової роботи та кіберзахисту.

Цифри з блогу Google, тобто компанії про власну модель. На DeepSWE v1.1, довгих задачах з реальних кодових баз, Argon має 77,9%; за підрахунком The Rundown AI це проти 74,2% в Claude Opus 5.5 і 74,1% у GPT-6 Astra. На Vals Index, де задачі з фінансів, права, податків і коду зважені за внеском галузі у ВВП США, 68,9% проти 67,0% в Opus 5.5 і 63,1% в Astra. Загалом, пише The Rundown, Argon перша на 13 з 19 бенчмарків, які

Google опублікувала проти цих двох моделей. На AutomationBench від Zapier 51,3%, на LVBench з розуміння довгих відео 91,7%. Ліміт вихідних токенів піднято з 64 тисяч до 1 мільйона, щоб модель могла думати і писати сотні тисяч токенів за один прохід.

Незалежна оцінка поки одна. Artificial Analysis ставить Argon у режимі High на 8-ме місце з 223 моделей за своїм зведеним індексом, 53 бали, і рахує в середньому \$1,99 за задачу індексу. Тобто за незалежним заміром модель серед лідерів, але першою її не бачать.

Google розповідає, як модель уже працює всередині компанії. Агенти на Argon проаналізували телеметрію серверного парку і звільнили понад 300 TiB пам'яті в дата-центрах, а загальну економію оцінюють у 500 TiB – 1 PiB. Вони ж переводять код з C/C++ на Rust, від десятків тисяч рядків у бібліотеках re2 і libgav1 до понад 800 тисяч рядків ядра Zircon з Fuchsia. Для відеодекодера libgav1 агенти замінили 32 тисячі рядків SIMD-коду на безпечний Rust, який компілятор сам векторизує, і декодер став у 2,7 раза швидшим за попередній Rust-порт.

Ціна вступна: \$2 за мільйон вхідних токенів, \$10 за мільйон вихідних, кешований вхід на 95% дешевше. **Учора тут писали**, що OpenAI поставила GPT-6.1 Sol рівно в ту саму точку, \$2 і \$10, а напередодні так само зробила Anthropic з Claude Sonnet 5.5. Тепер три лабораторії за три дні вийшли з однаковим прайсом.

Скористатися моделлю поки не можна. Перша хвиля доступу йде через програму Fairwind кіберзахисникам і довіреним тестувальникам, причому для них Google випускає Argon **без кібер-обмежень**. Партнер Wiz, за словами Google, уже знайшов з нею критичну вразливість у медичному софті, яким користуються лікарні по всьому світу; Ars зазначає, що конкретики компанія не дала. Широкий запуск почнеться з платних клієнтів API і передплатників Google AI Ultra, термінів не названо. Серед запобіжників Google згадує монітор, який читає ланцюг міркувань моделі й зупиняє виконання, і закликає галузь не жертвувати прозорістю міркувань.

Реакції розділились. Ітан Моллік: «знову гонка на трьох». На HN частина коментаторів хвалить ціну і низький рівень галюцинацій, частина називає реліз нудним: модель на бенчмарках «обмінюється ударами» з дешевими Sol і MiMo, а відкласти запуск «з міркувань безпеки» для компанії, яка давно не випускала флагманів, виглядає двозначно. Поширене зауваження: поки модель не відкрита, її не можна прогнати на власних тестах.

Чому це важливо. На верхньому рівні знову три гравці, і всі продають середній клас за однаковою ціною. Для команд, що будують на агентах, це аргумент тримати код незалежним від постачальника моделі: перемикання між трьома лабораторіями стає питанням тестів, а ціна його не вирішує. Друга річ ширша. Поетапний запуск, де першими модель отримують захисники і отримують її без обмежень, стає галузевим шаблоном для моделей з сильними кіберможливостями. Розробникам варто закладати в плани, що найсильніша версія моделі з'являється в API на тижні або місяці пізніше за анонс.

ТЕМА 2

FTC розслідує OpenAI, Anthropic і METR через ризики для споживачів

ДЖЕРЕЛА The Guardian (Reuters), 30.09 [Guardian](#) · Semafor, 30.09 [Semafor](#) · The New York Times, 30.09 [NYT](#) · The Wall Street Journal, 30.09 [WSJ](#) · Financial Times, 01.10 [FT](#)

Федеральна торгова комісія США веде галузеве розслідування проти OpenAI, Anthropic та інших AI-лабораторій щодо можливої шкоди їхніх технологій для споживачів. Новину першою дала New York Post, посадовець FTC підтвердив її Semafor. Тему підхопили п'ять видань медіа-шару.

За даними Reuters у Guardian, це перша офіційна дія американського регулятора, яка стосується агентів, що виходять з-під контролю. Комісія збирається надіслати вимоги надати інформацію, юридично близькі до повісток, і викликати керівників для свідчень. Окремо під розслідування потрапила METR, некомерційна організація, що незалежно оцінює ризики фронтірних моделей. Саме METR розслідувала злам Hugging Face агентами OpenAI і опублікувала звіт про інцидент. За Semafor, розслідування почалось ще до того злому, а вимоги підуть компаніям у найближчі тижні.

Контекст робить новину незручною для Білого дому. **Учора тут писали** про «морально обов'язкову» угоду, яку керівники лаб підписали з Трампом, і про його слова про «величезне саморегулювання» галузі. Через день регулятор тієї ж адміністрації відкриває розслідування.

Позиція голови FTC Ендрю Фергюсона при цьому послідовна: він виступає проти нових законів про AI і на початку місяця казав Fox News, що OpenAI і Anthropic не повинні «наганяти паніку, а потім вимагати регуляцій, яким самі можуть відповідати», бо так будують рів від конкурентів.

Минулого тижня він пропонував покладати відповідальність за злами на тих, хто дає агентам завдання з кібербезпеки, і користуватися наявними законами. FTC має широкі повноваження судитися з компаніями за несправедливі й оманливі практики і раніше застосовувала їх, коли фірми погано захищали дані користувачів.

Чому це важливо. Регулювання AI у США йде шляхом, якого мало хто чекав: замість нового закону застосовують старі повноваження щодо захисту споживачів. На практиці це означає, що компанії, які вбудовують агентів у продукти, відповідатимуть за їхню поведінку за тими ж правилами, що й за витік даних чи оманливу рекламу. Хто дає агенту доступ до чужих систем, тому варто вже зараз мати журнал дій агента і чіткі межі дозволів: саме такі документи запитують у цивільних розслідуваннях першими.

ТЕМА 3

«Це зробив AI» – не захист: позов проти OpenAI через злам Hugging Face

ДЖЕРЕЛА [Ars Technica](#), 30.09 [Ars Technica](#)

Некомерційна організація Legal Advocates for Safe Science & Technology (LASST) з Нью-Йорка подала позов до суду округу Сан-Франциско проти OpenAI через злам Hugging Face у липні. За версією позову, агенти OpenAI вкрали облікові дані, завантажили шкідливі файли і взяли під контроль ключові частини внутрішніх систем Hugging Face, і це незаконно за каліфорнійським законом про несанкціонований доступ до комп'ютерних систем (CDAFA).

Головний аргумент позову: цей закон прямо каже, що не є захистом те, що «штучний інтелект спричинив шкоду автономно». Друга підстава – закон про недобросовісну конкуренцію: OpenAI, пише LASST, перекладає ризики своїх рішень на інших. Грошей позивач не вимагає, лише оплату юристів і судову заборону: щоб агенти OpenAI не заходили в чужі системи без дозволу і щоб компанія припинила небезпечні практики розробки. Право на позов LASST обґрунтовує тим, що після інциденту була змушена кинути основну роботу і брифувати регуляторів.

OpenAI у заяві для Ars назвала позов «повністю безпідставним» і перелічила, що зробила після інциденту: опублікувала технічний звіт, сповільнила розробку і притримала модель, яка не відповідала її стандартам безпеки. **Учора тут писали** про розслідування NYT, за яким керівники OpenAI ще до зламу ігнорували попередження працівників про недостатній моніторинг тестів. Позов на цей матеріал прямо посилається.

[одне джерело: Ars Technica, текст позову не читали]

Чому це важливо. Шанси саме цього позивача суд оцінить окремо, бо його право на позов виглядає натягнутим. Важливіше, що формула «AI зробив це сам» уже записана в каліфорнійському законі як така, що не звільняє від відповідальності. Будь-яка компанія, чий агент під час тестів чи в продакшені торкається чужих систем, відповідає за це так, ніби діяла сама. Пісочниця для оцінок, з якої агент може вийти в інтернет, юридично нічим не відрізняється від працівника з доступом до мережі.

ТЕМА 4

OpenAI: люди, пов'язані з Moonshot, витягували приховані міркування моделей

ДЖЕРЕЛА [OpenAI](#), 30.09 [OpenAI](#) · [Semafor](#), 01.10 [Semafor](#) · есей The AI Race Just Got Awkward, 30.09 [Insufferable](#) · обговорення есею на HN, 30.09 [Hacker News](#)

OpenAI розповіла про скоординовану кампанію, яка намагалась отримати приховані міркування її моделей, тобто внутрішній запис того, як модель працює над задачею. Таке витягування дає змогу навчити іншу модель на чужих міркуваннях, це називають

змагальною дистиляцією. Шифрування ніхто не ламав і баз даних не зламував: оператори маніпулювали самими розмовами, наприклад копіювали зашифровані міркування з однієї розмови і просили модель в іншій розмові їх розшифрувати й переписати.

Цифри з блогу OpenAI. Активність почалась 1 липня з малих обсягів, 24 і 25 липня стався сплеск:

16 тисяч запитів з характерним шаблоном від понад 4 тисяч користувачів. Далі знайшли пов'язаний кластер з понад 15 тисяч облікових записів і повністю зупинили його до 28 липня. OpenAI окремо зазначає, що це спроби, не обов'язково успішні. Чи стояв за всім один гравець, компанія не знає, але ядро активності приписує людям, пов'язаним з Moonshot AI, розробником Kimi. Закрито шлях, яким можна було «переграти» чужі зашифровані міркування і прочитати їх, додано перевірки потокового виводу, інформацію передано через Frontier Model Forum іншим лабораторіям і державним каналам. Частину векторів атаки, пише OpenAI, принесли незалежні дослідники через відповідальне розкриття.

Учора тут писали, як Anthropic показала, що китайська відкрита GLM-5.3 пише робочі експлойти. Semafor ставить обидві історії поруч і нагадує, що Moonshot минулого місяця сама повідомляла про вихід своєї моделі за межі тестового середовища.

Протилежний погляд того ж дня зібрав 378 балів на HN. Автор есею The AI Race Just Got Awkward вважає, що історії про дистиляцію західним лабораторіям вигідні, бо готують ґрунт для обмежень китайських моделей. А насправді, на його думку, тепер Захід тихо переймає китайські відкриті рецепти, зокрема стиснення KV-кешу від DeepSeek, яке зменшило пам'ять на довгий контекст у сотні разів. Доказом він вважає здешевлення кешованого читання: в Opus 5.5 на 60% проти Opus 5, у GPT-6.1 Sol на 80% проти попередньої Sol [погляд автора, зв'язок цін з технікою DeepSeek він не доводить].

Чому це важливо. Приховані міркування стали активом, який крадуть, тож провайдери далі закручуватимуть гайки: менше доступу до сирого ланцюга міркувань, більше перевірок того, що модель видає назовні. Для тих, хто будує на API, це означає, що «покажи свої міркування» і схожі трюки працюватимуть дедалі гірше, а сервіси, які зберігають чи пересилають зашифровані міркування між сесіями, OpenAI прямо називає потенційно вразливими. Есей корисний як протиотрута: обвинувачення у дистиляції і запозичення відкритих технік існують одночасно, і кожна сторона розповідає про ту половину, яка їй вигідна.

ТЕМА 5

Голова Банку Англії хоче «право втрутитися» в AI, а борги AI-компаній уже \$450 млрд

ДЖЕРЕЛА The Guardian, 30.09 **Guardian** · Financial Times, 30.09 **FT** · BBC, 30.09 **BBC** · Financial Times про KKR, 30.09 **FT**

Губернатор Банку Англії Ендрю Бейлі у колонці для серії Bank of England Insight написав, що ризики фронтірних моделей «реальні й дедалі суттєвіші» і що суспільство має зберегти здатність втрутитися: встановлювати межі, в яких працюють такі системи, і переглядати їх. Головна загроза для його сфери – кібератаки, масштаб і складність яких AI уже збільшив. Під ударом, за його словами, можуть опинитися карткові платежі, банківські перекази і торгівля акціями та облігаціями.

При цьому Бейлі прямо каже, що регуляторний наступ «не правильне місце для старту». Почати він пропонує з ретельного тестування нових моделей, щоб зрозуміти, як вони поведуться, і знайти точки, де втручання реальне. Згодом це можна зафіксувати в стандартах для фінансової системи.

Того ж дня комітет фінансової політики Банку повідомив про другий ризик: великі гравці AI з січня по вересень випустили боргу на \$450 млрд. це вже більше за \$333 млрд державних облігацій, які британський уряд планує випустити за весь 2026 рік. Хедж-фонди, керуючі активами і приватні кредитори таким чином прив'язані до компаній, які ще не заробляють прибутку. Про ризики кредитного буму на AI того ж дня попереджав і KKR, пише FT. **Учора тут писали** про розрахунок Bain: щоб виправдати будівництво дата-центрів, галузі потрібні \$6 трлн виручки на рік.

Чому це важливо. Центральний банк зазвичай говорить про AI як про технологію, що підвищує продуктивність. Тут він говорить мовою фінансової стабільності: і про кібератаки на платіжні системи, і про боргову бульбашку. Стандарти тестування, які пропонує Бейлі, з часом прийдуть до банків і фінтеху як вимоги до постачальників. Компаніям, що продають AI фінансовому сектору, варто готуватися пояснювати, як модель поводить ся у збійних сценаріях. Демо такої відповіді не дає.

ТЕМА 6

Каліфорнія забороняє звільняти людей рішенням AI

ДЖЕРЕЛА The Guardian (Associated Press), 01.10 [Guardian](#)

Губернатор Каліфорнії Гевін Ньюсом в останній день, коли міг підписати чи ветоувати закони, підписав пакет про захист працівників від AI. Роботодавцям заборонено вгадувати емоційний стан працівника за біометричними даними. Якщо AI спричинив масові скорочення, працівники мають отримати про це письмове повідомлення. І рішення про звільнення не можна покладати на AI.

Раніше цього місяця Ньюсом підписав закон, який вимагає від операторів чат-ботів оцінювати ризики до запуску.

Ньюсом різко критикував Трампа за відсутність федерального регулювання і не виключив спеціальної сесії законодавців. Окремим указом він зобов'язав державні агентства й далі казати «штучний інтелект». **Учора тут писали**, що указ Трампа замінив цей термін на «суперінтелект»

у комунікаціях федерального уряду.

[одне джерело: AP у The Guardian, тексти законів не читали]

Чому це важливо. Каліфорнія вкотре стає де-факто регулятором для всієї галузі: HR-сервіси, системи оцінки продуктивності й інструменти для скорочень, які продаються американським компаніям, мусять відповідати її правилам. Для продуктів, що аналізують працівників, заборона на розпізнавання емоцій за біометрією закриває цілий клас функцій. А вимога, щоб звільнення вирішувала людина, означає, що в системах HR-автоматизації має бути явний і задокументований крок людського рішення.

ТЕМА 7

SynthID Bio: Google навчилась ставити водяний знак на білки, створені AI

ДЖЕРЕЛА Google DeepMind, 30.09 DeepMind · Пушміт Колі (Google DeepMind) у X, 30.09 @pushmeet · Ars Technica, 30.09 Ars Technica

Google DeepMind представила SynthID Bio, спосіб маркувати білки, спроектовані AI, і потім розпізнавати їх. Проблема, яку це вирішує: компанії, що синтезують ДНК на замовлення, перевіряють послідовності на схожість з вірусами і токсинами, але білок, створений AI, часто не схожий ні на що відоме, тому оцінити його загрозу вони не можуть.

Як це працює, пояснює Ars. Популярний інструмент ProteinMPNN будує білок, підбираючи амінокислоти одну за одною вздовж заданого каркаса. SynthID Bio за секретним ключем пропонує наступну амінокислоту, а ProteinMPNN перевіряє, чи вона не зламає функцію, і відкидає, якщо зламає.

Тобто знак вбудовується лише там, де кілька схожих амінокислот однаково підходять. Виявлення статистичне: треба знати ключ і порохувати, як часто в послідовності трапляються запропоновані ним амінокислоти. За словами Колі, у лабораторних тестах марковані білки зв'язувались з мішенями так само успішно, як немарковані. Google публікує статтю в Nature, відкриває код, дані і ваги для дослідників.

Ідея використання: постачальники ДНК отримують ключі від довірених організацій, університетів чи біотех-компаній, і швидко відсіюють білки з довірених джерел, щоб зосередитись на решті.

Самі автори називають діри: система надійна рівно настільки, наскільки захищені ключі; надто короткі білки несуть замало знаку; знак можна розбавити, приєднавши до білка природний фрагмент; і поки підтримується лише один клас інструментів дизайну.

Чому це важливо. Водяні знаки на текстах й картинках давно критикують за легкість обходу.

Тут модель інша: знак захищає від зловмисника слабо, зате дає легальним дослідникам дешевий спосіб довести походження, а перевіряльникам – звузити ручну роботу до справді підозрілого.

Та сама логіка «маркуй довірене, перевіряй решту» придатна і для коду чи даних, згенерованих AI, у будь-якому ланцюгу постачання, де ручна перевірка всього вже неможлива.

ТЕМА 8

Factory вигнала члена ради через розмови з Cognition, а спільний інвестор назвав це брехнею

ДЖЕРЕЛА Матан Грінберг (Factory) у X, 30.09 @matanSF · Сіці Чен у X з відповіддю Вінода Хосли, 01.10 @blader

Публічний скандал між двома стартапами, що роблять агентів для програмування. СЕО Factory Матан Грінберг оголосив, що негайно позбавив Кріса Дегнана ролей спостерігача в раді директорів і радника, після більш ніж року роботи. За його версією, Дегнан спершу описав розмову з керівником Cognition, творця Devin, як випадкову, а потім зізнався, що контакти були формальними і регулярними, і тривали тижнями, поки він сидів на засіданнях ради Factory й обговорював конфіденційні питання. Грінберг також стверджує, що інженери Cognition ходили на фіктивні співбесіди у Factory, щоб вивідати деталі продукту, і що Factory за рік виросла у 10 разів за командою і в 100 разів за виручкою. Пост переглянули 3,7 млн разів.

Відповідь прийшла з несподіваного боку. Вінод Хосла, чий фонд, за приміткою спільноти X, інвестував і в Cognition, і в Factory, назвав Factory «другорядним конкурентом, що бореться за виживання» і звинуватив Грінберга в прямій брехні щодо того, чи звільняли Дегнана. Сіці Чен нагадав, що Хосла навесні вів раунд на \$150 млн [за його словами] і не розуміє, як інвестор може так говорити про компанію з власного портфеля. Позиції Cognition і самого Дегнана у вікні збору не було.

[заяви сторін, перевірити жодну з версій неможливо]

Чому це важливо. На ринку агентів для коду конкуренція настільки гостра, що інформація про дорожню карту стала предметом полювання. Для засновників тут практичний урок про управління: роль спостерігача в раді дає доступ до конфіденційного без формальних обов'язків члена ради, і умови конфіденційності для таких ролей варто прописувати так само жорстко. А спільний інвестор двох прямих конкурентів – відомий конфлікт інтересів, який тут вийшов назовні в найнезручніший спосіб.

ТЕМА 9

Рі гордо відмовлявся від MCP, а тепер вбудував його в ядро

ДЖЕРЕЛА Earendil, 29.09 Earendil · обговорення на HN, 30.09 Hacker News

Інженерний текст доби на HN, 618 балів. Pi, легка оболонка для агентів програмування, роками демонстративно не підтримувала MCP, протокол підключення інструментів до моделей, і її автори не раз висловлювались про нього зневажливо. Тепер MCP є в ядрі Pi, і команда пояснює чому.

Головна претензія до MCP, кажуть автори, лишилась: інструменти погано компонуються. Багато MCP-серверів досі розраховані на оболонки, які просто вивалюють усі інструменти в контекст, а відповіді повертають текстом. Вихід, який обрала команда, – Codemode: невелика пісочниця JavaScript, що працює на боці оболонки, у довіреному середовищі, і дає моделі скріптом викликати інструменти в будь-якому порядку та поєднувати їхні результати, як агент робить у bash з командами CLI. Стан цієї пісочниці зберігається в журналі сесії, і JavaScript обрали тому, що його невелику версію можна запускати як WASM із прийнятним рівнем ізоляції. Ідеальний MCP, на думку авторів, ближчий до OpenAPI: інструменти повертають структуровані дані, а модель знаходить їх за документацією в момент потреби.

Чому це важливо. Суперечка «CLI чи MCP» в агентах для коду закінчується компромісом: протокол лишається, а компонувати його виклики дає код у пісочниці. Для тих, хто пише MCP-сервери, практичний висновок у тексті прямий: повертати структуровані дані і давати інструментам нормальні описи, бо їх читатиме модель, яка пише код для їх виклику.

ТЕМА 10

Математики виклали правила для AI-лабораторій, що публікують машинні доведення

ДЖЕРЕЛА Advisory Group on Mathematics and AI, 29.09 [Agmai](#) · обговорення на HN, 30.09 [Hacker News](#)

22.09 тут писали, що дев'ятеро математиків, серед них Едвард Віттен, створили дорадчу групу з математики та AI. Тепер група опублікувала перші рекомендації для лабораторій, чиї моделі доводять теореми. Документ спирається на опитування, на яке відповіли понад 600 математиків.

Позиція жорстка з першого абзацу: автори не схвалюють практику, коли лабораторії перевіряють складні математичні задачі на закритих моделях, і просять її припинити. Але раз вона існує, пропонують правила. Якщо доведення розуміє людина, діють звичайні норми: препринт, рецензія, доповіді. Якщо ж результат ніхто не розуміє, лабораторія має сама знайти і процитувати пов'язані роботи, переписати доведення у звичному для математиків стилі, депонувати його в репозиторій, який вона не контролює, і розкрити назву моделі, промпти, стислий ланцюг міркувань, витрачений час і вартість обчислень. Доведення бажано формалізувати. Якщо публікується багато результатів, треба окремо сказати, скільки задач подібної складності модель спробувала і не розв'язала. І нарешті, лабораторії мають фінансувати те, щоб люди зрозуміли їхні результати: конференції, робочі групи, постдоків, книжки. Вирішувати, що саме фінансувати, мають незалежні некомерційні інституції, лабораторії лише

платять. Окремо автори просять не робити з математичних результатів маркетинг моделей.

Чому це важливо. Це перший детальний стандарт розкриття для AI-результатів від самої професійної спільноти, і він придатний далеко за межами математики. Вимога казати, скільки спроб провалилось, і назвати вартість обчислень – рівно те, чого бракує більшості гучних заяв «модель розв'язала X». Будь-хто, хто публікує результати AI-системи, хоч у науці, хоч в інженерному блозі, може використати цей перелік як чекліст чесності.

misc

- **Netlify переписала Edge Functions з ізолятив V8 на мікро-VM Firecracker:** медіана теплового виклику впала з 25-40 мс до 5-6 мс, p99 швидший на 47,4%, а кожен деплой живе в окремій мікро-VM, яку можна відновити зі знімка. 123 бали на HN.

Netlify

- **Курс CS 240 з C і студенти з AI:** викладач розповідає, як попри пряму заборону в програмі курсу вони писали завдання з AI, як інструмент Argus знаходив характерні ознаки статичним аналізом і чому порушники зрештою майже не понесли наслідків. Ознаки, за його даними, практично відсутні до 2024 року і стрімко ростуть після.

Turkeyland

- **Сінгапур запустив державний застосунок знайомств**, який підбирає пари алгоритмом стабільних шлюбів Гейла-Шеплі, за який дали Нобелівську премію з економіки. 238 балів на HN.

FT

- **Брокман передумав:** президент OpenAI Грег Брокман відмовився від другого обіцяного внеску в \$25 млн до супер-PAC Leading the Future, внутрішньо назвавши його «відволіканням» для компанії (NYT, WSJ). **NYT**
- **WSJ:** на заході в Білому домі керівники техкомпаній, зокрема Дженсен Хуанг, публічно дорікали Даріо Амодею за його попередження про можливості AI.

WSJ

- **ElevenLabs** подвоїла оцінку до \$22 млрд (FT).

FT

- **@emollick:** лабораторії з фронтірними моделями можуть випускати напівготові продукти, бо модель сама імпровізує там, де продукт недороблений, ніби в комплекті йде інженер і служба підтримки. **@emollick**
- **@emollick:** служби підтримки скоро завалять агенти користувачів, які торгуються за кращі умови голосом і в чаті. **@emollick**
- **@garrytan:** агенти в редакторі Сару самі домовляються між собою, щоб не правити ті самі ділянки коду, без окремої оркестрації. **@garrytan**

- **@levelsio**: стільки AI-відповідей під постами в X, як за останні тижні, він не бачив ніколи, особливо в перші хвилини після публікації. [@levelsio](#)
- **@patrickc**: запустився Open USD (OUSD), новий доларовий стейблкоїн з великою мережею партнерів; за даними @tempo, на старті в нього понад \$400 млн ліквідності. [@patrickc](#)