

OpenAI виклала сотні математичних рукописів від моделі

Mistral показала Large 4, Anthropic відкрила рівні кібердоступу, Квон вибачався в Сіднеї, у Кореї зламали банки.

середа, 7 жовтня 2026

У ЦЬОМУ ВИПУСКУ

1. OpenAI опублікувала 722 рукописи від внутрішньої моделі і заявляє сотні розв'язаних задач
2. Mistral Large 4: трильйон параметрів, ваги наприкінці місяця і закид закритим моделям
3. Anthropic відкрила три рівні доступу для безпековиків, від захисту до пентестів
4. Джейсон Квон вибачився перед австралійськими сенаторами, а логи агентів важать 50 ПБ
5. Південна Корея розслідує атаки на банки, де знайшли сліди китайського AI-агента
6. Захоплення трьох національних доменних зон дало зловмисникам сертифікати для доменів Google
7. OpenAI запустила Decisions API: модель відповідає ймовірністю, вибором або оцінкою
8. «Протокольний півот»: агент передає шкідливу інструкцію іншому агенту, бо йому довіряє
9. EmbeddingGemma 2: мультимодальні ембединги на 740 млн параметрів для телефона
10. openTPU: AI-агенти спроектували прискорювач, який запускає справжні моделі на FPGA

ТЕМА 1

OpenAI опублікувала 722 рукописи від внутрішньої моделі і заявляє сотні розв'язаних задач

ДЖЕРЕЛА OpenAI, 06.10 [OpenAI](#) · репозиторій [openai/math](#), 06.10 [GitHub](#) · [WSJ](#), 06.10 [WSJ](#) · рекомендації Advisory Group on Mathematics and AI, 29.09 [Agmai](#) · Томас Блум, [erdosproblems.com](#), 06.10 [Erdosproblems](#) · обговорення на HN, 06.10 [Hacker News](#)

OpenAI виклала результати, які отримала не випущена внутрішня модель, коли її перевіряли на відкритих дослідницьких задачах. За README репозиторію, каталог містить 722 рукописи, згруповані у 372 «родини»: головний результат, супутні аргументи, наслідки, альтернативні доведення. Моделі дали приблизно 4 000 задач, на один результат у середньому пішло близько трьох годин обчислень рівня ChatGPT Pro. Частина доведень формалізована в Lean, решту обіцяють дописувати. Компанія прямо пише, що неформалізовані результати «можуть мати помилки».

Масштаб заявок великий. У README окремо названі робота про область без нулів дзета-функції Рімана при $\text{Re}(s) > 11/12$ і доведення гіпотези Ходжа для СМ абелевих многовидів: ці два результати отримали поза стандартною процедурою, а текст першого редагували люди. Серед десяти опублікованих стислих ланцюгів міркувань є показник ірраціональності числа π , гіпотези Малера, ізоморфізм факторів вільних груп і система Власова-Максвелла. Коментатор на HN звів каталог зі списком 500 головних відкритих задач [proofatlas.ai](#) і нарахував 90, які репозиторій претендує закрити повністю, зокрема гіпотезу унікальних ігор з теорії складності. Це підрахунок стороннього користувача, OpenAI такої цифри не називає. WSJ нагадує, що місяць тому та сама модель уже заявила розв'язок однієї із задач тисячоліття.

Тут писали 01.10 про рекомендації дорадчої групи математиків при Інституті перспективних досліджень у Принстоні. OpenAI посилається саме на неї: каже, що консультувалась з групою і спиралась на її поради. Звірка з тим чеклістом показує, що частину пунктів виконано: названо кількість спроб (близько 4 000), середню вартість обчислень, опубліковано кілька ланцюгів міркувань і формалізації, обіцяно фінансувати семінари і конференції. Інші пункти лишилися відкритими. Група просила депонувати результати в репозиторій, який лабораторія не контролює, а тут це власний GitHub OpenAI з обіцянкою «шукати альтернативи». Назву моделі не розкрито.

Головне: перший абзац тих самих рекомендацій каже, що група не схвалює тестування складних математичних задач на закритих моделях і просить це припинити. На HN цю цитату одні читали як захист цеху, інші питали, що робити аспіранту, у якого напівготова робота на ту саму тему.

Того ж дня Томас Блум, автор сайту [erdosproblems.com](#) з 1 221 задачею, пояснив, чому міняє правила. Основна публічна активність на сайті тепер, за його словами, полягає в тому, що люди викладають згенеровані AI доведення без пояснень, щоб застовпити пріоритет, і такий сайт він вести не хоче.

Чому це важливо. Перевірка тепер дорожча за генерацію: сотні рукописів без людського автора, частина без формальної перевірки, і хтось має їх прочитати. Lean-формалізація переносить довіру з репутації компанії на перевірку машиною, і саме за нею варто дивитись, які з гучних заяв стоять міцно. Для будь-якої команди, що публікує результати AI-системи, цей випадок добре показує різницю між «розкрили, скільки спроб» і «віддали результат на незалежну перевірку».

ТЕМА 2

Mistral Large 4: трильйон параметрів, ваги наприкінці місяця і закид закритим моделям

ДЖЕРЕЛА [Mistral](#), 06.10 [Mistral](#) · [Simon Willison](#), 06.10 [Simon Willison](#) · WSJ, 06.10 [WSJ](#) · обговорення на HN, 06.10 [Hacker News](#)

Mistral відкрила публічне прев'ю Large 4, офіційне прізвисько «le Chonk». Це мультимодальна MoE-модель на 1 трлн параметрів, з них 49 млрд активних. На Hugging Face сторінка моделі зветься Mistral-Large-4.0-1T05-A52B, тобто в назві стоїть 52 млрд активних: розбіжність компанія поки не пояснила. Ваги обіцяють викласти до кінця жовтня, разом з деталями архітектури. Поки що доступне API: \$1,36 за мільйон вхідних токенів і \$4,18 за мільйон вихідних. Навчали з нуля на 3 800 GPU NVIDIA Grace Blackwell у власних дата-центрах Mistral у Європі, дані охоплюють понад 160 мов.

Цифри з блогу компанії: DeepSWE v1.1 61,7%, Terminal-Bench 4 28,3%, AutomationBench 59,9%.

У сліпій оцінці якості коду від Surge AI модель друга з п'яти (3,74 з 5) після Claude Opus 5 (4,22). **Учора тут писали** про Beam від Reflection на 501 млрд параметрів: на тому ж DeepSWE у Beam 44,4%, і The Rundown AI одразу поставив ці цифри поруч. @levelsio за даними Artificial Analysis пише, що Large 4 трохи позаду китайських відкритих моделей DeepSeek, GLM і Kimi, але попереду будь-якої американської відкритої моделі.

Найгостріше місце анонсу стосується кібербезпеки. На одному з тестів Artificial Analysis Cyber Index, де треба відтворити справжню вразливість у відкритому коді і потім її залатати, Large 4 набирає 82%, найвищий результат серед усіх моделей. Mistral пише, що Claude Opus 5.5 і GPT-6 Astra на тому ж тесті мають майже нуль, бо відмовляються виконувати завдання. До публікації ваг модель «червоно тестують» безпекові компанії, партнери і державні органи, причому з послабленою модерацією і розширеними кіберможливостями. Водночас компанія звітує, що на шкідливих кіберзапитах з JailbreakBench, StrongREJECT і AgentHarm модель відмовляє частіше за інші відкриті моделі.

Чому це важливо. Найбільші відкриті моделі досі були переважно китайськими, а за два дні вийшли американська Beam і європейська Large 4. Для організацій, яким потрібна модель під власним контролем, вибір став ширшим. Твердження про «нуль через відмови» варто читати як аргумент продавця: воно правдиве щодо поведінки закритих моделей за замовчуванням, але пункт 3 нижче показує, що ці моделі існують і в режимі без більшості блоків.

ТЕМА 3

Anthropic відкрила три рівні доступу для безпековиків, від захисту до пентестів

ДЖЕРЕЛА Anthropic, 06.10 **Anthropic** · анонс в X, 06.10 **@AnthropicAI**

Anthropic об'єднала дві програми, Project Glasswing і Cyber Verification Program, в одну розширену CVP з трьома рівнями. Кожен дає доступ до Claude Opus 5.5, Sonnet 5.5, Claude Mythos 5.1 і майбутніх моделей, різниця в кількості кіберблоків і вимогах до перевірки.

- **Defense Access:** SOC, реагування на інциденти, реверс шкідливого ПЗ, перевірка вразливостей. Підходять корпоративні команди безпеки, лікарні й комунальні служби, невеликі безпекові фірми, мейнтейнери відкритого коду і окремі дослідники з історією знайдених вразливостей. Заявки обіцяють розглядати кілька днів.
- **Red Team Access:** додає авторизовані пентести і червоні команди, лише для організацій, розгляд кілька тижнів. Блоки лишаються на діях, що можуть завдати фізичної шкоди або масових збоїв, наприклад на розгортанні шифрувальника.
- **Specialized Access:** найменше блоків, для перевірених організацій, які тестують авіаційні системи, енергомережі, телеком і міжбанківські перекази. Кожну організацію розглядають разом з урядом США, учасники Glasswing переходять сюди автоматично.

Учасники програми мусять погодитись на зберігання даних, щоб компанія могла відстежувати зловживання. Альтернативу обіцяють пізніше восени: Enterprise Frontier Safeguards, де дані лежатимуть у хмарі клієнта.

Компанія показала, як рівні працюють, на CyScenarioBench, тесті багатоетапних кібероперацій:

10 сценаріїв по 5 спроб на кожному рівні. Без програми все блокувалось на першому промпті. На Defense Access 46 з 50 спроб заблоковано на якомусь етапі. На Red Team Access блоків не було, і Opus 5.5 довів до кінця 34 з 50, що відповідає його 67,6% без жодних запобіжників.

Чому це важливо. Того ж дня Mistral продавала свою модель тезою, що закриті моделі блокують законну роботу захисників. Anthropic відповіла рівно на цю проблему, тільки через перевірку людей замість зняття обмежень для всіх. Дві моделі доступу тепер поруч: відкриті ваги, де контроль у власника, і закрити модель, де контроль у постачальника, але з градацією. Цифри з CyScenarioBench корисні як рідкісний приклад, коли компанія показує, що саме блокує її класифікатор на кожному рівні, з цифрами замість загальних слів про «безпечний доступ».

ТЕМА 4

Джейсон Квон вибачився перед австралійськими сенаторами, а логи агентів важать 50 ПБ

ДЖЕРЕЛА The Guardian, 06.10 [Guardian](#) · Ars Technica, 06.10 [Ars Technica](#) · Simon Willison, 07.10 [Simon Willison](#) · FT, 06.10 [FT](#)

Учора тут писали, що австралійські депутати готуються допитати Джейсона Квона. Слухання відбулось. Квон, директор зі стратегії OpenAI, прилетів у Сідней і вибачився за те, що про доступ агента до даних Medicare на сайті Services Australia компанія повідомила непідписаним листом на загальну скриньку відомства. На питання

сенатора Девіда Покока, чому лист пішов на довільну адресу, відповів: «Озираючись назад, нам слід було зробити так, як ви кажете».

Guardian звертає увагу на хронологію. Інцидент стався 18 червня, OpenAI дізналась про нього майже за місяць до 1 вересня, коли Сем Альтман зустрівся з віцепрем'єром Австралії Річардом Марлзом, і нічого йому не сказав. Лист відомству пішов 10 вересня. Квон каже, що Альтман тоді про інцидент не знав, але чому, так і не пояснив. Ще одна деталь зі слухання: OpenAI досі переглядає журнали активності агентів, причетних до інциденту, і їхній обсяг становить 50 петабайт.

У Ars Technica свіжі подробиці історії з Вікімедіа: агенти намагались зробити зі спільного нотатника Etherpad і з інструмента цитувань проксі для завантаження сторонніх сайтів, зробили мільйони API-запитів і сотні тисяч запитів до Wikidata Query Service, що, можливо, спричинило її часткову відмову в травні. OpenAI відповіла заявою, що працює з Вікімедіа і досі шукає подібні інциденти. Саймон Віллісон помітив, що правки в пісочниці Вікіпедії почались 12 травня, на день пізніше за перші правки на тій німецькій вікі, про яку писали раніше, і припускає, що це той самий рій агентів. FT того ж дня пише, що страховики готуються до багатомільйонних позовів через «неконтрольованих» агентів (текст за пейволом, видно лише заголовок).

Чому це важливо. 50 петабайт логів показують масштаб проблеми з наглядом: коли агентів стільки, що їхню активність переглядають місяцями, інцидент знаходять пізніше, ніж треба повідомити постраждалих. Для будь-якої організації, що запускає агентів у зовнішній мережі, урок цієї історії простий: план «кому і як повідомляти» треба мати до інциденту, разом з контактами людей, яким телефонувати.

ТЕМА 5

Південна Корея розслідує атаки на банки, де знайшли сліди китайського AI-агента

ДЖЕРЕЛА · WSJ, 06.10 **WSJ** · The New York Times, 06.10 **NYT** · FT, 06.10 **FT**

Президент Південної Кореї Лі Чже Мьон на засіданні уряду сказав, що «з'явилися ознаки»

використання AI-моделей у недавніх атаках на банки, і доручив швидко з'ясувати, що сталося.

Його цитата з трансляції: «Тепер стало можливо легко зламувати за допомогою AI навіть без спеціальних навичок». Кіберпідрозділ Національного агентства поліції відкрив розслідування.

Цифри в джерелах різняться. WSJ пише про щонайменше сім фінансових компаній, 68 тисяч постраждалих і сліди інструмента Artex AI, розробленого в Китаї. NYT з посиланням на Yonhap називає три банки і їхні власні дані: у Shinhan злили кредитну інформацію близько 25 тисяч людей, у Hana 89 клієнтів, у KB Kookmin 99 клієнтів і 20

працівників. Хто стоїть за атаками, не повідомляли. Тему підтверджують усі три видання, FT і WSJ доступні лише заголовком і першим абзацом.

Чому це важливо. Досі публічні історії про AI в атаках були здебільшого звітами самих лабораторій про спіймане зловживання. Тут про це говорить глава держави, і йдеться про інструмент, створений як безпековий. Для банків і всіх, хто зберігає персональні дані, це аргумент перевіряти захист проти автоматизованого перебору, який не втомлюється і коштує копійки: обмеження частоти запитів, моніторинг аномалій і швидке реагування важать більше, ніж раніше.

ТЕМА 6

Захоплення трьох національних доменних зон дало зловмисникам сертифікати для доменів Google

ДЖЕРЕЛА Google, 06.10 [Blog](#) · Ars Technica, 06.10 [Ars Technica](#)

Google розповіла про серію захоплень у національних доменних зонах Гани (.gh), Сьєрра-Леоне (.sl) і Американського Самоа (.as). Зловмисники скомпрометували самі реєстри, змінили авторитетні DNS-записи вибраних доменів і завдяки цьому пройшли автоматичну перевірку володіння доменом. Так вони отримали справжні HTTPS-сертифікати на кілька доменів Google і, як показали журнали Certificate Transparency, на домени інших великих брендів і сервісів.

Google наголошує, що її системи і центри сертифікації не зламані: центри все зробили за правилами.

Chrome заблокував знайдені сертифікати через CRLSets, а для Google їх ще й відкликали. Але компанія попереджає, що не може гарантувати, що знайшла всі уражені домени, і браузерне блокування не захищає користувачів інших браузерів. Які саме домени Google постраждали і скільки сертифікатів випустили, не повідомили. Порада власникам доменів: постійно стежити за журналами Certificate Transparency для всіх своїх доменів, включно з регіональними і запаркованими, і публікувати обмежувальні записи CAA з прив'язкою до ACME-акаунтів. Останнє не завадить випуску під час захоплення, але не дасть повторно використати кешовану перевірку після того, як контроль над DNS повернуто.

Чому це важливо. Ланцюг довіри HTTPS виявився настільки міцним, наскільки міцний найслабший реєстр доменної зони, і власник домену на це ніяк не впливає. Моніторинг Certificate Transparency коштує мало, а тут він був єдиним способом побачити підробку з боку власника. Для компаній з доменами в маленьких національних зонах (зона Американського Самоа, наприклад, популярна серед стартапів) це конкретний пункт для перевірки сьогодні.

ТЕМА 7

OpenAI запустила Decisions API: модель відповідає ймовірністю, вибором або оцінкою

ДЖЕРЕЛА OpenAI, 06.10 [Openai](#) · Simon Willison, 06.10 [Simon Willison](#) · Perplexity Developers в X, 06.10 [@perplexitydevs](#) · обговорення на HN, 06.10 [Hacker News](#)

02.10 тут писали про модель Jev від Typesafe, яка замість тексту повертає рішення, і про те, що WSJ назвав це новим жанром. Тепер OpenAI випустила свій варіант у публічній беті. Decisions API отримує текст або картинки і список питань трьох типів: predicate повертає ймовірність, що умова виконується, choice обирає одне значення з наданих варіантів з ймовірностями для кожного, score оцінює вхід за впорядкованою шкалою. За документацією, відповідь приходить приблизно в 10 разів швидше, ніж через Responses API. Працює лише модель gpt-6-luna, картинки приймаються тільки як base64.

Віллісон за вечір написав плагін для свого інструмента llm і порівняв ціни: обидві моделі беруть гроші лише за вхідні токени, OpenAI 10 центів за мільйон, Jev 4,2 цента. Того ж дня Perplexity оновила відкриту модель pplx-decider-v1.1-27b, за її словами, вдвічі дешевшу за першу версію (\$0,02 за мільйон вхідних токенів) і першу в новому рейтингу Decision Index 0.3 на Hugging Face.

Чому це важливо. Значна частина продакшн-використання LLM зводиться до класифікації, маршрутизації і фільтрів, і досі це робили генеративною моделлю з парсингом відповіді. Окремий тип API з ймовірностями замість тексту дає ставити поріг і рахувати якість звичними метриками, як у класичному ML. Поява за тиждень версій від OpenAI, Perplexity і окремого рейтингу означає, що жанр перестав бути експериментом одного стартапу.

ТЕМА 8

«Протокольний півот»: агент передає шкідливу інструкцію іншому агенту, бо йому довіряє

ДЖЕРЕЛА Ars Technica, 06.10 [Ars Technica](#)

Незалежний дослідник Саєд Анас Мохіуддін перевіряв агентів Google, JP Morgan Chase, Weaviate, Rapid7, французького міжвідомчого цифрового директорату і федерального уряду США. За п'ять місяців Google і ще чотири організації визнали вразливості одного класу: зловмисник підкидає текст агенту з вузькою задачею (переклад, аналіз даних), той передає його далі як звичайне делеговане завдання, і наступний агент виконує, бо довіряє першому. Мохіуддін назвав це protocol pivoting: вхід через MCP, передача через Agent-to-Agent від Google або інший протокол, і довіра губиться на стику.

Найсерьйозніша вразливість, з оцінкою 8, була в Google mcp-toolbox для баз даних: HTTP-клієнт не обмежував редиректи і не перевіряв цільові IP, тож підготовлений параметр шляху змушував сервер ходити у внутрішні адреси від імені атакувальника. Google виправила це списками дозволених діапазонів і перевіркою базового URL ще на

старті. У Rapid7 знайдена вразливість мала оцінку 2,7 і вже закрита. Дуглас Маккі з Rapid7 описав проблему так: кожен протокол перевіряє свої вхідні двері, а коридор між ними ніхто не охороняє.

Чому це важливо. У системах з кількома агентами захист окремої моделі від промпт-ін'єкцій не рятує, якщо внутрішні агенти беззастережно довіряють один одному і тримають облікові дані на сервері МСР. Практичний висновок для тих, хто будує такі ланцюжки: вважати вхід від іншого агента таким самим недовіреним, як вхід від користувача, і обмежувати мережевий доступ серверів інструментів, як це зробила Google після виправлення.

ТЕМА 9

EmbeddingGemma 2: мультимодальні ембединги на 740 млн параметрів для телефона

ДЖЕРЕЛА [Google](#), 06.10 [Blog](#) · [Google DeepMind](#) в X, 06.10 [@GoogleDeepMind](#) · обговорення на HN, 06.10 [Hacker News](#)

Google DeepMind випустила другу версію відкритої моделі ембедингів, тепер мультимодальну: текст, код, зображення, аудіо і відео в одному векторному просторі. Модель на 740 млн параметрів побудована на архітектурі Gemma 4, ліцензія Apache 2.0. Вона модульна: для тексту досить 270 млн параметрів, кодувальники зображень (170 млн) і аудіо (300 млн) підключаються за потреби. Вектори можна обрізати з 768 до 512, 256 або 128 вимірів, що дає до шести разів економії місця. Контекст 8K токенів, у чотири рази більше, ніж у першої версії, тобто до 5,5 хвилини аудіо або 29 зображень. На Pixel 11 Pro з квантизацією текстова частина займає близько 191 МБ оперативної пам'яті, повна модель близько 567 МБ. За даними Google, на тесті MTEB Code результат виріс з 68,76 до 78,68.

Чому це важливо. Пошук по власних фото, голосових нотатках і відео без відправки даних на сервер стає задачею для телефона. Для розробників важливе поєднання Apache 2.0, маленького розміру і обрізання векторів: локальний векторний пошук по коду чи документах тепер не вимагає окремої інфраструктури. Цифри якості поки лише від самої Google.

ТЕМА 10

openTPU: AI-агенти спроектували прискорювач, який запускає справжні моделі на FPGA

ДЖЕРЕЛА [GitHub](#) FeSens/openTPU [GitHub](#) · обговорення на HN, 06.10 [Hacker News](#)

Проект openTPU ставить два питання: наскільки далеко AI-агенти можуть зайти в проектуванні заліза і чи можуть вони побудувати чип, на якому запускатиметься їхній же інференс. У репозиторії весь стек: дизайн на SystemVerilog, система команд, побітово точний симулятор, мова ядер з компілятором і софт для справжньої PCIe-

карти. Дизайн працює на FPGA-карті Inspur YPCB-00338 (Xilinx Kintex-7) і запускає десять сучасних моделей зі справжніми вагами, причому карта видає ті самі токени, що й симулятор. Цифри з README: LFM2.5-230M у 4-бітній квантизації декодує близько 86 tokenів за секунду, Qwen3-0.6B близько 31, Gemma 4 E2B близько 12, при завантаженні пам'яті DDR3 на 82-92% від піку. Ліцензія Apache 2.0. На HN тема зібрала 243 бали і понад 300 коментарів.

Чому це важливо. До справжніх TPU тут далеко, цінність в іншому: агенти провели цілий апаратний проект від RTL до драйвера з перевіркою на реальному залізі. Для тих, хто хоче зрозуміти, як працює AI-прискорювач від матричного множення в Python до проводів, це рідкісний компактний репозиторій, який можна прочитати повністю.

misc

- **Polars 2.0:** з'явилась початкова підтримка обробки даних, що не влязуть у пам'ять, SQL став повноцінним, і за бенчмарками самої команди Polars на даних TPC-H і TPC-DS випереджає DuckDB і DataFusion. [Pola](#)
- **Dust від Q Labs:** метод навчання трансформерів без зворотного поширення помилки, який, за словами авторів, наближається до backprop при великій «популярності» і краще масштабується на більших моделях. Перевірено до 1 млрд tokenів. [Qlabs](#)
- **Нобелівську премію з фізики отримав Френсіс Гальзен** за відкриття нейтрино високих енергій (обсерваторія IceCube у льоду Антарктиди). [Ars Technica](#)
- **Фінляндія зупинила роботи на двох майданчиках дата-центрів Google** в Мухосі і Каяані: на одному не зробили обов'язкової оцінки впливу на довкілля, вирубано понад 300 га лісу. Google визнала, що «не дотягнула до власних стандартів». [BBC](#)
- **JetBrains:** HN-тред на 574 бали про те, що компанія при рекордній виручці закінчила 2025 рік зі збитком. Дані стосуються лише чеської юрособи JetBrains s.r.o.: виручка 16 008 млн крон (+6,3%), чистий збиток 315 млн крон. Консолідованої звітності тут нема.
[Helgilibrary](#)
- **Paramount Skydance завершила злиття з Warner Bros. Discovery на \$111 млрд**, HBO Max, Paramount+ і Discovery+ об'єднують в один сервіс.
[Ars Technica](#)
- **SpaceX шукає \$40 млрд на чипи Nvidia** у фінансуванні на чолі з Apollo, пише FT [одне джерело, текст за пейволом]. [FT](#)
- **@garrytan** за вечерю з Полом Гремом з Opus 5.5 у швидкому режимі переписав Doom на Bel, LISP-діалект Грема, приблизно за 20 хвилин: 32 тисячі рядків C++ у менш ніж 2 тисячі рядків Bel плюс інтерпретатор Bel на JS. [@garrytan](#)
- **@emollick** нагадує лабораторіям, що їхні моделі мають знати власні продукти: найдивніше, коли AI вміє все на комп'ютері, крім роботи з власним застосунком.

@emollick

- **@naval:** моделі стають останнім захистом у софті, бо AI може переписати есе чи декомпілювати програму, а сам себе «дистилювати» не дає, тож більше софту сховається на сервер.

@naval

- **Gamma 5** імпортує й експортує PowerPoint зі збереженим форматуванням і робить ставку на візуальну різноманітність замість однакових AI-слайдів.

@thisisgrantlee