AI-ДАЙДЖЕСТ

Математик: оцінюйте кожну статтю так, ніби її писав AI

Red Hat виправив ядро Linux, Ubuntu ще ні, Intel мінус 29%, Binance відкрилась, агенти в Minecraft

понеділок, 2 листопада 2026

У ЦЬОМУ ВИПУСКУ

1. Калегарі в блозі Тао: оцінюйте кожну статтю так, ніби її писав AI
2. CVE-2026-98432: Red Hat виправив ядра, Ubuntu досі ні, і вимкнений MPTCP не рятує
3. Ринок засумнівався в AI-витратах: Intel мінус 29% за день, neocloud дорожчає
4. Binance відкрилась після зламу: за день клієнти вивели $3,64 мільярда
5. Скільки коштує агенту JavaScript-фреймворк: Нолан Лоусон зібрав той самий застосунок 60 разів
6. Claude Code змонтував влог з 58 хвилин відео і сам вибрав інструменти
7. Моллік: режими GPT-6 плутаються, а межу продуктивності варто ставити на січень 2026
8. 50 агентів у Minecraft отримали задачу збудувати цивілізацію і збудували бюрократію

ТЕМА 1

Калегарі в блозі Тао: оцінюйте кожну статтю так, ніби її писав AI

ДЖЕРЕЛА блог Теренса Тао, гостьовий пост Франка Калегарі, 01.11 Wordpress · HN, 01.11 Hacker News

6 жовтня OpenAI опублікувала понад 700 математичних статей. Тут про це писали 07.10. Тепер математик Франк Калегарі пояснює колегам, як з цим жити. Його текст вийшов гостьовим постом у блозі Теренса Тао. Тао додав примітку, що текст перевели в інший формат за допомогою AI.

Калегарі визнає, що статті OpenAI «жахливо написані», порушують норми атрибуції, а деякі з них хибні. Але він каже, що математики мають більше влади над наймом, журналами і навчанням, ніж над поведінкою компаній на трильйон доларів. Він цитує Юго Дюміль-Копена: жодна з великих відкритих задач, які той згадував за кар'єру, не лишилась без заявленого доведення.

Калегарі дає шість пропозицій. Оцінювати кожну роботу так, ніби її зробили з AI. Наймати після особистої розмови, також постдоків і аспірантів. Вимагати більше від журналів і кидати ті, що не змінюються. Вчити аспірантів ширше, але зберігати технічні навички. Робити кращі семінари. Брати відповідальність за результати AI. Найрадикальніша думка: результат, який може видати машина, більше не має приносити кредит, навіть якщо автор зробив його руками.

На HN тред набрав 244 бали і 273 коментарі.

Чому це важливо: інші професії ще не мають такої розмови, а математика вже має. Механізм простий: якщо результат дешевий, цінність переходить до вибору задачі і пояснення, чому вона цікава. Такий самий тиск відчують усі, кого оцінюють за кількістю публікацій, звітів чи комітів.

ТЕМА 2

CVE-2026-98432: Red Hat виправив ядра, Ubuntu досі ні, і вимкнений MPTCP не рятує

ДЖЕРЕЛА Atlas, оновлено 01.11 Atlasum · трекер Ubuntu Ubuntu · @levelsio, 01.11 @levelsio

Учора тут писали, що RHEL і Ubuntu не мають виправлення. 1 листопада Red Hat випустив виправлені ядра для RHEL 8, 9 і 10.

Трекер Ubuntu станом на ранок 02.11 показує «Vulnerable» для всіх релізів. Для 26.10, 26.04, 24.04 і 22.04 там стоїть «work in progress». AlmaLinux тримає виправлені ядра в тестовому репозиторії.

Atlas додала важливе уточнення. Anthropic каже, що Claude написав робочий експлойт, який дає root на сервері зі слухачем MPTCP. Але сама помилка живе у звичайному IPv4 TCP. Команда безпеки Go пише, що системи без слухачів MPTCP теж можуть бути вразливі до схожих атак. Тому вимкнений MPTCP прибирає лише відомий шлях атаки. Помилку він не прибирає.

Станом на вечір 01.11 Atlas нарахувала 41 репозиторій GitHub, які згадують цей CVE. Anthropic свій експлойт не опублікувала. @levelsio радить закрити на VPS усі порти, пускати SSH лише через Tailscale, а вебтрафік через Cloudflare Tunnel.

Чому це важливо: вразливий код працює до того, як застосунок бачить з'єднання. Тому захищає тільки нове ядро і перезавантаження. На Ubuntu поки лишаються правило nftables проти TCP-пакетів з опціями IPv4 і мінімум відкритих портів.

ТЕМА 3

Ринок засумнівався в AI-витратах: Intel мінус 29% за день, neocloud дорожчає

ДЖЕРЕЛА Semafor, 01.11 Semafor · BBC, 01.11 BBC · The Wall Street Journal, 01.11 WSJ

Учора тут писали про кредитний стиск у neocloud. Тепер його видно і на біржі. Semafor пише, що в п'ятницю Nasdaq увійшов у корекцію. Акції Intel впали на 29%, це найбільше падіння за день з 1970-х. Звіти Amazon і Google розчарували інвесторів. S&P Global змінила прогноз для Meta на «негативний» через великі капітальні витрати.

BBC пояснює, де слабке місце. Neocloud-компанії, як CoreWeave і Nebius, позичають гроші під довгі контракти з великими клієнтами і під самі чипи. Борг CoreWeave

становить $35,1 мільярда. Її акції за місяць втратили чверть вартості, у Nebius, IREN і Applied Digital падіння таке саме або більше. Gartner прогнозує, що до 2030 року 80% neocloud-компаній припинять незалежну роботу.

Коли Microsoft і Google дали прогноз AI-витрат нижчий за очікування аналітиків, акції neocloud впали. WSJ виніс тему в заголовок розсилки «AI Spenders Get Spooked». Текст за пейволом.

Чому це важливо: уся будова AI-інфраструктури тримається на одному припущенні, що великі клієнти й далі збільшать витрати. Перший прогноз нижче за очікування б'є по найбільш закредитованих ланках. Для тих, хто купує обчислення в малих провайдерів, це ризик постачальника, і його варто врахувати в договорі.

ТЕМА 4

Binance відкрилась після зламу: за день клієнти вивели $3,64 мільярда

ДЖЕРЕЛА BBC, 02.11 BBC · Financial Times, 01.11 FT · Semafor, 01.11 Semafor

Учора тут писали, що ФБР підтвердило слід Північної Кореї. У неділю Binance відновила операції. За словами біржі, з 06:00 до 15:30 за Гринвічем клієнти вивели $4,649 мільярда і внесли $1,01 мільярда. Чистий відтік склав $3,64 мільярда, це трохи більше за 2% від $171 мільярда активів під управлінням.

Binance каже, що вже покрила близько 95% викраденого. Решта може потребувати більше часу. За ранніми перевірками біржі, атака почалась зі зламаного ноутбука одного інженера. ФБР опублікувала список гаманців групи TraderTraitor і просить галузь блокувати транзакції з ними.

Чому це важливо: точка входу в найбільший криптозлам історії, за даними самої біржі, звичайний робочий ноутбук.

Відтік 2% за день показує, що паніки нема, але довіра тепер коштує біржі мільярди резервів.

ТЕМА 5

Скільки коштує агенту JavaScript-фреймворк: Нолан Лоусон зібрав той самий застосунок 60 разів

ДЖЕРЕЛА Нолан Лоусон, 28.10 Nolanlawson · HN, 01.11 Hacker News

[одне джерело] Розробник Нолан Лоусон перевірив твердження, що якийсь фреймворк «кращий для агентів». Він дав Opus 5.5 ту саму специфікацію застосунку про покемонів і попросив зібрати його на 12 фреймворках. На кожному фреймворку агент зібрав застосунок 5 разів, Лоусон брав медіану.

Найдешевше вийшло на Hono+htmx: $2,67 за збірку за цінами API. Найдорожче на Angular: $4,97, і два запуски на Angular взагалі не дали робочого застосунку. SvelteKit коштував $4,28, бо агент щоразу читав гайд міграції на v3. Лоусон пояснює це тим, що нова версія ще не потрапила в навчальні дані моделі.

Оцінки Lighthouse майже не відрізнялись: продуктивність 97-100 і доступність 100 у всіх. Офіційні MCP і скіли агенти часто ігнорували. Скіл TanStack Start агент знайшов лише у 2 з 5 запусків, MCP від Nuxt не використав жодного разу.

Чому це важливо: на питання «який стек кращий для агентів» тепер можна відповісти замірами, і замір коштує кілька десятків доларів. Перший висновок: фреймворк, якого модель не знає, обходиться дорожче, бо агент вчиться на ходу.

ТЕМА 6

Claude Code змонтував влог з 58 хвилин відео і сам вибрав інструменти

ДЖЕРЕЛА @levelsio, 01.11 @levelsio · @levelsio, 01.11 @levelsio

[одне джерело] Пітер Левелс скопіював кліпи з камери DJI в папку і попросив Claude Code змонтувати 10-хвилинний влог.

На вході було 58 хвилин відео з 14 кліпів. Про інструменти він дізнався лише тоді, коли його спитали, як він монтував.

Агент транскрибував мову через mlx-whisper на GPU макбука. Він робив сітки кадрів кожні кілька секунд, щоб бачити зміст кліпів. Голос Левелса він відділив від інших моделлю SpeechBrain ECAPA.

Сам монтаж став JSON-списком нарізок: кліп, початок, кінець. Фрагменти агент вибрав за транскриптами і сітками кадрів. Левелс каже, що без AI він би не вів влог, бо монтаж забирав би забагато часу.

Чому це важливо: агент розклав незнайому задачу на звичайні локальні інструменти і нікого не питав про кожен крок.

Для рутинного медіа-монтажу бар'єр тепер у формулюванні запиту.

ТЕМА 7

Моллік: режими GPT-6 плутаються, а межу продуктивності варто ставити на січень 2026

ДЖЕРЕЛА @emollick, 01.11 @emollick · @emollick, 01.11 @emollick · @emollick, 01.11 @emollick

[одне джерело] Ітан Моллік хвалить GPT-6 Pro за складні одноразові задачі з розрахунками і посиланнями. За його словами, модель працює повільно, але дає відчуття «спитати оракула».

Pro доступний лише в інтерфейсі чату. У Codex і ChatGPT Work найвищий режим зветься Ultra, і він робить інше: запускає багато агентів. Є ще Max Thinking, який теж слабший за Pro.

Окремо Моллік пише про продуктивність. GPT-4 мав 50% шанс виконати 4 хвилини самостійної роботи, а сучасні моделі виконують роботу на кілька тижнів. Тому він пропонує вважати січень 2026 початком агентної роботи. Великий ефект до цієї дати, за його словами, був переважно в коді.

Чому це важливо: дослідження, які не бачать ефекту AI в економіці, часто міряють період чат-ботів. Межа Молліка дає просту перевірку для будь-якого такого звіту: які дані він бере після січня 2026.

ТЕМА 8

50 агентів у Minecraft отримали задачу збудувати цивілізацію і збудували бюрократію

ДЖЕРЕЛА YC Labs, 29.10 Ycombinator · Tom's Hardware, 01.11 Tomshardware · HN, 01.11 Hacker News

YC Labs разом з Olam Labs запустили 50 агентів GPT-6.1 Sol у світ Minecraft на 3 години з метою «збудувати процвітаючу цивілізацію». Агенти мали каталог учасників, спільну пісочницю і особисті повідомлення. Вони надіслали близько 5 900 повідомлень.

Перша ніч убила багатьох: 22 з 34 смертей за весь запуск. Смерть нічим не карала, крім втрати речей, але агенти все одно стали обережними. Вони сиділи в укриттях, ділили їжу за журналом, писали правила і дозволи. Tom's Hardware цитує випадок, коли четверо агентів 11 хвилин призначали «єдиного оператора добрива» для одного блоку пшениці.

У грі Mindustry агенти GPT-6.1 Sol виграли в агентів Claude Opus 5.5 з рахунком 6:1 у 7 іграх. Середовища і обв'язку для Minecraft автори відкрили.

Чому це важливо: автори кажуть, що поведінка нагадала їм роботу з агентами для коду. Великий рій без ціни помилки стає обережним і витрачає ресурси на координацію. Це корисний орієнтир для тих, хто масштабує агентів числом.

---

misc

- **HackerBooks:** після HackerTube Карпаті, про який писали вчора, автор зробив те саме для книжок. Сайт зібрав 15 362 книжки з 270 334 згадок на HN, тред набрав 1 044 бали.

  Hackerbooks · Hacker News
- **Flock:** місто Плімут скасувало контракт з Flock 22.09, але компанія не забрала камери. Начальник поліції наказав висмикнути шнури живлення.

  Thedrive · Hacker News

- **Бразилія:** суд оштрафував двох адвокатів приблизно на $16 000 за прихований білим шрифтом промпт для судового AI. Рішення від липня, на HN воно спливло зараз.
  Jetstream · Hacker News
- **Proton:** розробник Раед пише, що історія 404 Media про Proton стосується керівництва, AI тут ні до чого. CEO назвав прохання про кілька днів пентесту «loser thinking».
  Raed · Hacker News
- **Монорепо:** @tobi згадав, як Shopify переходила на монорепо. Інженер Shopify Берк Ліббі пише, що для агентів це великий плюс, і назад він не повернувся б.
  @tobi
- **Jepsen:** Саймон Віллісон процитував Кайла Кінгсбері: LLM підривають довіру до документації і софту, бо ознаки зрілої системи тепер легко підробити.
  Simon Willison
- **Британія:** Openreach вимикає стару телефонну мережу PSTN 31.01.2027 без відстрочок. Під удар потрапляють сигналізації, термінали і тривожні кнопки для літніх людей.
  Theregister · Hacker News
- **Тіссайд:** National Grid купує 29,5 гектара під найбільшу підстанцію Британії поруч із запланованим AI-датацентром.
  Guardian
- **Підписки:** @amasad попереджає власників дотованих AI-підписок про різке підвищення цін. Привід: Ілон Маск пояснив, чому користувачі Grok Bot швидше вичерпують ліміт.
  @amasad
