AI-ДАЙДЖЕСТ

# OpenAI знайшла 948 шляхів до root у Linux за $1,2 млн

*Виборці США заблокували дата-центри, Meta і OpenAI купили інструменти для агентів, ваги Kimi K3.1 Pro*

четвер, 5 листопада 2026

---

У ЦЬОМУ ВИПУСКУ


1. OpenAI: агенти знайшли 948 шляхів до root у ядрі Linux за $1,2 млн
2. Виборці в США заблокували дата-центри майже в усіх голосуваннях
3. День угод: Meta, OpenAI і Factory купили інструменти для роботи з агентами
4. IEEE Spectrum: AI змушує сплатити 40 років технічного боргу
5. Відкриті ваги: Kimi K3.1 Pro, американська Ripple-65B і Tencent Hy4
6. Gemini тренується на чатах навіть платних підписників
7. Anthropic: Claude допоміг визначити першу структуру vault-частинки з бактерій
8. Layer3: через мережу Білого дому виходять резидентні проксі
9. Ноутбуки RTX Spark на Linux дають уп'ятеро менше токенів, ніж на Windows
10. OpenAI випустила Images 2.6: GIF, SVG і генерація за 6 секунд


---

ТЕМА 1

## OpenAI: агенти знайшли 948 шляхів до root у ядрі Linux за $1,2 млн

ДЖЕРЕЛА OpenAI, 04.11 OpenAI · @OpenAI, 04.11 @OpenAI · @gdb, 04.11 @gdb · HN, 04.11 Hacker News

Команда безпеки OpenAI побудувала конвеєр з п’яти етапів. Агенти-розвідники вибирають у ядрі код, до якого дістає звичайний користувач. Агенти-аналітики шукають у ньому помилки. Інші агенти відтворюють кожну знахідку у віртуальній машині, пишуть експлойт і патч. Останнім етапом результат перевіряє людина.

У середині жовтня один прогін на новій кібермоделі дав такі цифри. Розвідники виділили 5 034 цілі, це 2,8 мільйона рядків або ~7% ядра. Аналітики знайшли 2 308 кандидатів. Агенти відтворили 1 724 вразливості, це ~75%. Хибний аналіз моделі дав лише 3,1%. На виході 948 унікальних вразливостей з робочим експлойтом на root. Цілі працювали на звичайному десктопному дистрибутиві з SMEP, SMAP і KASLR.

Увесь прогін коштував $1 213 430 в API, тобто $1 279 на один експлойт. @gdb округлює до «about $1,000». Для порівняння OpenAI бере старі винагороди Pwn2Own і TyphoonPWN: $20 000 і $70 000 за такий експлойт. У липні GPT-5.6 Sol на тому самому конвеєрі

знайшла 166 вразливостей. Нова модель знайшла в 5 разів більше, хоча ядро три місяці латали.

Два спостереження корисні поза Linux. Перше: на ранньому прогоні 20 з 200 «успішних» експлойтів отримали root через іншу, не призначену вразливість. Тому OpenAI тепер перевіряє шлях до результату, а не лише результат. Друге: сильнішій моделі важка обв'язка вже майже не допомагає. Набір із 103 технік підняв успіх GPT-5.5 Cyber з 76,2% до 88,9%. Для GPT-5.6 Cyber той самий набір дав лише +1,5 п.п.

OpenAI пише, що агенти використали щонайменше 10 нових технік експлуатації ядра. Деталі вона не публікує з міркувань безпеки. Сотні звітів і патчів уже пішли мейнтейнерам. За 10 днів сканування 61 вразливість уже мала патч в upstream, 43 мали патчі в staging.

**Чому це важливо:** OpenAI пише прямо: доступ до непропатченої системи з обліковкою без прав тепер варто вважати доступом до root. Звідси практичний висновок для будь-якої інфраструктури. Оновлення ядра стають терміновими, а пісочниці на кшталт gVisor і Firecracker стають обов'язковим шаром. У треді HN головне питання звучить так: чи ядро просто завелике, щоб у ньому не було тисячі таких помилок.

---

ТЕМА 2

## Виборці в США заблокували дата-центри майже в усіх голосуваннях

ДЖЕРЕЛА The New York Times, 04.11 NYT · Ars Technica, 04.11 Ars Technica · Semafor, 04.11 Semafor · Stratechery, 04.11 Stratechery · The Wall Street Journal, 04.11 WSJ · @AndrewCurran_, 04.11 @AndrewCurran_ · HN, 04.11 Hacker News

Учора згадували, що демократи взяли Палату. Сьогодні стало видно, яку роль у цьому зіграли дата-центри. NYT рахує: у 40 з 41 місцевого голосування виборці обмежили або заборонили дата-центри, більше половини з них в Огайо. Ars з посиланням на Redbud Consulting пише про 38 ухвалених з 44 у 10 штатах. Цифри різняться, бо підрахунок триває. Але кожне джерело називає один виняток: місто Гарвуд у Північній Дакоті.

На рівні штатів картина та сама. Губернаторкою Техасу стала демократка Джина Інохоса, яка обіцяла мораторій на дата-центри.

За Ars, Техас мав дати понад 41% нових потужностей дата-центрів у 2028 році. Демократи також виграли губернаторів в Аризоні, Джорджії й Огайо. В Огайо сенатор-елект Шеррод Браун зробив головним аргументом $2,5 млрд податкових пільг для 226 дата-центрів.

Індустрія відповідає по-різному. Президентка Meta Діна Павелл Маккормік на конференції WSJ сказала, що будувати стане «harder». Галузева група Chamber of Progress каже, що це «anti-Trump wave», а не мандат проти технологій. Опитування NBC показують, що 3 з 4 виборців проти дата-центрів. Більше половини назвали AI і дата-центри важливим фактором голосу.

Бен Томпсон у Stratechery формулює наслідок так. Обмеження для AI змістилось з чипів, пам'яті й енергії на дозвіл будувати. Від цього виграють гіперскейлери і ті, хто вже має дозволи. Програють неоклауди, яким потрібні нові майданчики.

**Чому це важливо:** до цього тижня головними ризиками AI-будівництва були кредити й енергія. Тепер це ще й місцеві голосування, і банки вже рахують їх як кредитний ризик. Для ринку інференсу це означає довшу дорогу до дешевших токенів у США. Для решти світу це шанс: за словами економіста Natixis, Китай отримує нагоду продавати дешевий інференс.

---

ТЕМА 3

## День угод: Meta, OpenAI і Factory купили інструменти для роботи з агентами

ДЖЕРЕЛА Conductor, 04.11 Conductor · @charlieholtz, 04.11 @charlieholtz · OpenAI, 04.11 OpenAI · @gdb, 04.11 @gdb · @dexhorthy, 04.11 @dexhorthy · @bentossell, 04.11 @bentossell · HN, 04.11 Hacker News · HN, 04.11 Hacker News

За один день закрились три угоди. @bentossell назвав це «holy acquisition day». Усі три компанії робили інструменти навколо агентів для коду, і всі три зникають як окремі продукти.

Conductor, застосунок для паралельної роботи кількох агентів, переходить у Meta Superintelligence Labs. Нових користувачів Conductor уже не реєструє. Conductor Cloud стане read-only 13.11 і закриється 20.11. Локальна версія отримуватиме моделі й критичні фікси до початку 2027 року.

OpenAI купує Pierre Computer Company. Її бібліотеки Trees і Diffs уже стоять у застосунку Codex для навігації по файлах і перегляду змін. Ще Pierre робить Code Storage, сервіс зберігання коду через Git. OpenAI прив'язує угоду до Pando, свого бекенда Git, про який ми писали 03.11. Відкриті проєкти Pierre лишаються відкритими.

HumanLayer переходить у Factory. Засновник Декс Горті пише, що великим командам потрібен продукт, незалежний від конкретної лаби. HumanLayer відкриє свій код і тримає платформу щонайменше 30 днів. Того ж вечора Кет Ву оголосила, що переходить в OpenAI керувати продуктом Core Products. До того вона вела продукт Claude Code в Anthropic.

**Чому це важливо:** лаби забирають собі шар над моделлю: огляд змін, оркестрацію агентів, сховище коду. Незалежних інструментів у цьому шарі меншає. Для команд, що будують процес на таких інструментах, це ризик: Conductor дав користувачам хмари лише 9 днів до read-only. Тримайте експорт даних і план переходу заздалегідь.

---

ТЕМА 4

## IEEE Spectrum: AI змушує сплатити 40 років технічного боргу

ДЖЕРЕЛА IEEE Spectrum, 04.11 Ieee · HN, 04.11 Hacker News

Це найпопулярніша стаття HN за добу: 1 113 балів і 648 коментарів. Привід знайомий: PHP2Shell, про яку ми писали 22.10.

Помилку нестачі пам'яті в PHP хтось повідомив ще у 2024 році. Її вважали безпечною, бо програма просто падала. Аудитор із Calif разом з AI за два тижні перетворив її на виконання довільного коду на сервері.

Професор Колумбійського університету Суман Джана пояснює, що змінилось. Експлойт «не є rocket science», але вимагає купи нудних точних міркувань, і саме тут AI добре працює. Джана не каже, що AI робить усе сам. Він каже, що топові 0,1% експертів тепер роблять більше, а ті, хто трохи нижче, дістають до їхнього рівня.

Головна проблема в асиметрії. Знайти помилку тепер швидко, а виправити досі довго. Четверо інженерів PHP Foundation два місяці писали патч. Джана сподівається на формальну верифікацію патчів, коли LLM пише патч і доказ, а перевіряє формальний чекер. Метью Ґрін з Джонса Гопкінса менш оптимістичний. Він чекає справді поганого інциденту «maybe sometime in early 2027», і лише після нього очікує гроші на захист.

**Чому це важливо:** пункт 1 показує ту саму асиметрію в цифрах. Знахідки дешевшають, а людський час на патч і реліз не дешевшає. Старі звіти про «просто краш» у трекері будь-якого проєкту тепер варто переглядати як потенційні вразливості.

---

ТЕМА 5

## Відкриті ваги: Kimi K3.1 Pro, американська Ripple-65B і Tencent Hy4

ДЖЕРЕЛА Hugging Face, Moonshot AI, 04.11 Hugging Face · HN, 04.11 Hacker News · Ricursive Intelligence, 04.11 Ricursive · HN, 04.11 Hacker News · Tencent, 04.11 Tencent · HN, 04.11 Hacker News

24.10 Moonshot обіцяла ваги Kimi K3.1 Pro до 04.11. Обіцянку вона виконала. Модель має 2,8 трильйона параметрів, з них 104 мільярди активні. Контекст 1 мільйон токенів, ваги в MXFP4. У таблиці Moonshot модель дає 65,7 на Terminal-Bench 4.0.

Claude Fable 5.1 там має 57,9, GPT-6 Astra 58,2, Claude Opus 5.5 66,4. Це цифри самої Moonshot.

Ліцензія має умову для провайдерів. Сервіс з виручкою понад $20 млн має укласти окрему угоду з Moonshot. У треді HN сперечаються, чи це ще «open weights». Один коментатор пише, що його команда запускає попередню Kimi на сервері з 4 AMD MI300A за ~$110 000.

Ricursive Intelligence випустила Ripple-65B Preview, щільну модель на 65 мільярдів параметрів. Вона дає 80,52 на TerminalBench 2.1, і компанія називає це рекордом серед відкритих моделей США. Повна вартість розробки з нуля, за словами Ricursive, $32 млн. Модель запускається локально на NVIDIA DGX Spark. Tencent того ж дня випустила Hy4 із зором і роботою з комп'ютером. Tencent пише, що Hy4 знизила частку галюцинацій з 15,76% до 5,45% у її внутрішніх тестах.

**Чому це важливо:** відкриті моделі вже стоять поруч із закритими на агентних бенчмарках, хоч і за цифрами самих авторів. Для компаній, які мусять тримати дані в себе, вибір росте. Але ліцензію читати обов'язково: «відкриті ваги» тепер часто означають умови для комерційного сервісу.

---

ТЕМА 6

## Gemini тренується на чатах навіть платних підписників

ДЖЕРЕЛА HN, Tell HN, 04.11 Hacker News · Google, довідка Gemini Google

Автор допису на HN думав, що платна підписка захищає його чати від навчання. Довідка Google каже інше. Для особистих акаунтів активність у застосунку Gemini йде на покращення сервісів, «including by training generative AI models». Це діє, поки ввімкнене налаштування Keep Activity.

Частину чатів читають люди. Такі чати не видаляються разом з активністю і лежать до 3 років. Вимкнути навчання можна лише разом з Keep Activity. Тоді чати зникають через 72 години. Тред набрав 635 балів. Коментатори нагадують, що людські рецензенти є в усіх великих провайдерів.

**Чому це важливо:** учора в misc був випадок, коли в Codex сам увімкнувся перемикач навчання. Сьогодні історія ширша:

оплата сама по собі не вимикає навчання на ваших даних. Робоча інформація має йти через корпоративні акаунти з окремими умовами, а налаштування приватності варто перевіряти в кожному продукті окремо.

---

ТЕМА 7

## Anthropic: Claude допоміг визначити першу структуру vault-частинки з бактерій

ДЖЕРЕЛА Anthropic, 04.11 Anthropic · @AnthropicAI, 04.11 @AnthropicAI

Vault-частинки відкрили у 1986 році. Це великі порожнисті бочки з білка в клітинах тварин і рослин, і їхня функція досі невідома. Біологи Anthropic показали, що схожі білки бактерій і фагів теж збираються у vault. Вони отримали першу 3D-структуру такої частинки: 96 копій одного фагового білка L05, близько 9,5 мегадальтона.

Claude шукав родичів білка в базі з ~15 мільярдів передбачених білків, проєктував ДНК і обробляв дані кріо-ЕМ. Очищення тривало ~90 хвилин замість звичних трьох днів. Першу модель структури команда мала через 34 години. Вона оцінює, що вручну це зайняло б тижні. Весь проєкт тривав менше чотирьох місяців.

Anthropic окремо описує помилки. Протокол Claude мав добавку, яка заважає вводити ДНК у клітини, і це коштувало два тижні. В обробці кріо-ЕМ Claude пропустив

стандартний крок і отримав карту, змішану з її дзеркальним відображенням. Препринт пішов на bioRxiv, але лінка на нього на ранок 05.11 ще нема.

**Чому це важливо:** команда, яка раніше не працювала з такими великими білковими структурами, зробила роботу структурних біологів. Цінна і друга половина звіту: помилки AI найдорожче коштують там, де людина сама слабо знає предмет. Перевірка людиною лишається обов'язковою саме там.

---

ТЕМА 8

## Layer3: через мережу Білого дому виходять резидентні проксі

ДЖЕРЕЛА Layer3 Intel, 04.11 Layer3intel · HN, 04.11 Hacker News

Резидентні проксі продають доступ до звичайних пристроїв, щоб трафік виглядав як трафік з їхньої мережі. Layer3 Intel побачила такі виходи з AS2650. Ця мережа належить Executive Office of the President. З 5.10 по 3.11 запити Layer3 вийшли через неї 236 разів, з 6 адрес, у 26 днів з 30. Доступ продавали 28 різних проксі-сервісів.

Layer3 звірила адреси з Spur і Synthient, і ті теж позначають їх як проксі. Половина активності припадає на 17:00-00:00 за східним часом. Layer3 вважає, що це заражений пристрій конкретної людини, а не гостьовий Wi-Fi. Хто це і який пристрій, дані не показують. Тред на HN набрав 777 балів [одне джерело].

**Чому це важливо:** доступ до виходу з такої мережі купує будь-хто за кілька доларів. Погано захищені проксі-SDK уже давали доступ у внутрішні мережі, так поширювався ботнет Kimwolf. Висновок для будь-якої компанії: перевіряйте, чи ваші IP не з'являються в базах резидентних проксі.

---

ТЕМА 9

## Ноутбуки RTX Spark на Linux дають уп'ятеро менше токенів, ніж на Windows

ДЖЕРЕЛА MindStudio, 04.11 Mindstudio · HN, 04.11 Hacker News

Ноутбуки на платформі RTX Spark мають той самий GPU, що й настільний DGX Spark, і до 128 ГБ спільної пам'яті. Вони виходять з Windows on ARM. MindStudio поставила Linux на MSI Prestige і поміряла GPT-OSS-120B. Windows дала 65,4 токена за секунду, WSL 65,1, DGX Spark 61, а Linux на тому самому ноутбуці лише 13,9.

Причина в прошивці. На живленні від мережі Linux тримає GPU на ~780 МГц замість ~2,2 ГГц. Таблицю живлення в прошивці зашифровано, і розшифровує її лише компонент драйвера для Windows. Температура при цьому 40-47 °C, тобто перегріву нема.

Розв'язок може дати лише Nvidia, якщо перенесе цю логіку в драйвер для Linux [одне джерело].

**Чому це важливо:** ноутбуки продають розробникам AI, а їхній інструментарій, vLLM і SGLang, спершу пишуть під Linux.

Поки що практичний шлях один: WSL. Перед купівлею «AI-ноутбука» під Linux варто шукати заміри саме під Linux.

---

ТЕМА 10

## OpenAI випустила Images 2.6: GIF, SVG і генерація за 6 секунд

ДЖЕРЕЛА OpenAI, 04.11 OpenAI · @OpenAI, 04.11 @OpenAI · HN, 04.11 Hacker News

Images 2.6 з'явилась у ChatGPT, Codex і API. OpenAI каже, що генерація стала на 50% швидшою. В API дві моделі. GPT-Image-2.6 Flare на низькій якості дає картинку за 6 секунд. GPT-Image-2.6 Sunburst дає вищу якість і краще тримає персонажа між правками.

Нове: анімовані GIF, приклади з референсних картинок, розмітка в API і експорт у SVG. Параметр complexity задає, скільки модель планує сцену. За даними OpenAI, користувачі створюють 4 мільярди зображень на тиждень.

**Чому це важливо:** експорт у SVG і розмітка в API роблять генерацію частиною робочого процесу дизайну, а не окремою іграшкою. Для інтерфейсів і маркетингу це менше ручної роботи між генерацією і готовим файлом.

---

## misc

- **AMD проти Intel, продовження:** AMD чекає ~$17 млрд виручки в Q4. Tom's Hardware пише, що це вперше більше за прогноз Intel. Виручка датацентрів у Q3 $8,55 млрд, +97% за рік.

  Tomshardware · Hacker News
- **Debian apt:** Макс Юстиц знайшов у APT помилку з HTTP-редиректом і докачкою. Нападник посередині може підмінити пакет після перевірки і виконати код як root. Debian виправила це в apt 3.0.4, CVE-2026-109518.

  Debian · Hacker News
- **Холодильники, продовження:** хакери підняли температуру в трьох сховищах французької служби крові EFS. Сигналізація спрацювала, і техніки втрутились раніше, ніж продукти зіпсувались.

  Guardian
- **Google і школи, продовження:** Kagi пише, що Google дозволила школам увімкнути пошук окремо від Gemini, але AI Overviews з пошуку прибрати досі не можна.

  Kagi · Hacker News
- **Гінтон:** Джеффрі Гінтон сказав Guardian, що людям, можливо, було б краще без AI. Він чекає великого інциденту, наприклад відключення фінансових або

енергосистем, цього або наступного року.

Guardian · Hacker News

- **Grok Bot дзвонить:** бот xAI тепер робить телефонні дзвінки за користувача в США, крім штатів Вашингтон та Іллінойс. Він чекає на лінії, проходить голосові меню і дає транскрипт.

  @TheRundownAI
- **Пауза AI:** конгресвумен Ясамін Ансарі хоче, щоб демократи в перший день поставили паузу на розробку просунутого AI і заборону суперінтелекту. @AiBreakfast відповів різко проти [одне джерело].

  @AiBreakfast
- **Семіотика AI:** @emollick розганяє статтю, за якою візуальні символи сильно впливають на моделі, і модель не завжди бачить цей вплив у своєму ланцюжку міркувань.

  @emollick · arXiv
- **Новий веб X:** інженер X Ягіз Нізіплі пише, що на повільному з'єднанні перший пост профілю тепер з'являється за 2,7 с замість 22 с. Реліз іде країна за країною.

  @yagiznizipli · X
- **Meta і бразильські медіа:** суд Бразилії заборонив Meta збирати контент місцевих медіа для навчання AI.

  Semafor

---