



ТЕХНОЛОГИЯ • БІЛІМ • БОЛАШАҚ

TECHDAMU

Жасанды интеллекттің жаңа дәуірі:
модельдер, агенттер және инфрақұрылым



№06

ШЫҒАРЫЛЫМ

2026

АЛМАТЫ



МАЗМҰНЫ

Жасанды интеллекттің жаңа дәуірі

01	Технологиялардағы соңғы жаңалықтарға шолу 03
	AI әлеміндегі айдың алты басты жаңалығы

02	AI агенттері: анықтамасы және жұмыс принципі 04
	Агенттік жүйелердің архитектурасы, қолданылу салалары және даму бағыттары.

03	Жасанды интеллект жүйелеріндегі деректер қауіпсіздігі 05
	Claude AI пайдаланушыларының кейбір чаттары интернетте көпшілікке қолжетімді болып шықты.

04	AI инфрақұрылымы: техникалық негіздер 07
	Техникалық инфрақұрылым – жасанды интеллект дамуының негізгі факторы.

05	Қытайдың AI серпілісі: Kimi K3 және жаңа бәсеке 08
	Kimi K3: Қытайдың AI технологияларындағы жаңа қадамы

Технологиялардағы соңғы жаңалықтарға шолу

AI әлеміндегі айдың алты басты жаңалығы

01 ҚАУІПСІЗДІК

OpenAI Hugging Face жүйесіндегі бұзылуды хабарлады

Ішкі тестілеу кезінде модельдер пакет орнату құралындағы осалдықты пайдаланып, шектен тыс қолжетімдік алды.

02 САЯСАТ

Ақ үй Moonshot AI-ды дистилляцияда айыптады

Кеңесші Kimi K3 моделін жасауда Anthropic технологиясы жасырын түрде қолданылды деп мәлімдеді.

03 ЧИПТЕР

Etched \$10,3 млрд бағаланымда \$300 млн тартты

Sequoia бастаған раундқа Andreessen Horowitz, SK Hynix және Jane Street қатысты.

04 БИЗНЕС

Alphabet Google Cloud өсімін хабарлады

Ішкі тестілеу кезінде модельдер пакет орнату құралындағы осалдықты пайдаланып, шектен тыс қолжетімдік алды.



05 РОБОТОТЕХНИКА

Амар роботтарға арналған ABot стегін ұсынды

Alibaba бөлімшесі навигация мен манипуляцияға арналған бес мамандандырылған модель шығарды.



06 ЧИПТЕР

Фудань университеті жаңа флеш-жад технологиясын жариялады

Guiyi жады бөлме температурасында бір электронды сақтап, есептей алады.



Материалдар осы дереккөз негізінде дайындалды:

<https://dsml.kz/ai-radar>

AI агенттері: анықтамасы және жұмыс принципі

Агенттік жүйелердің архитектурасы, қолданылу салалары және даму бағыттары.

Анықтамасы

AI агент — тек сұрақтарға жауап беретін тілдік модельден ерекшеленетін автономды жүйе. Ол мақсат қояды, әрекеттерді жоспарлайды, нәтижені бағалап, қажет болған жағдайда келесі қадамды өздігінен анықтайды.

AI агентінің жұмыс циклі бірнеше кезеңнен тұрады: ақпаратты қабылдау, жоспарлау, әрекет ету, жадқа сақтау және нәтижені бағалау. Қарапайым чат-бот тек мәтіндік жауап береді, ал AI агент сыртқы құралдарды пайдаланып нақты әрекеттерді орындай алады.

Түрлері

Жалғыз агент (single-agent) — бір тапсырманы дербес орындайды.

Көп агентті жүйелер (multi-agent) — агенттер бір-бірімен әрекеттеседі, міндеттерді өзара бөліседі.

Нақты мысалдар

Cursor/Claude Code — интернеттен ақпаратты автоматты түрде іздеп, талдайды.

Зерттеу агенттері — интернетте автоматты іздеу және талдау.

Робот-агенттер — физикалық ортада әрекет етеді.



Жасанды интеллект жүйелеріндегі деректер қауіпсіздігі

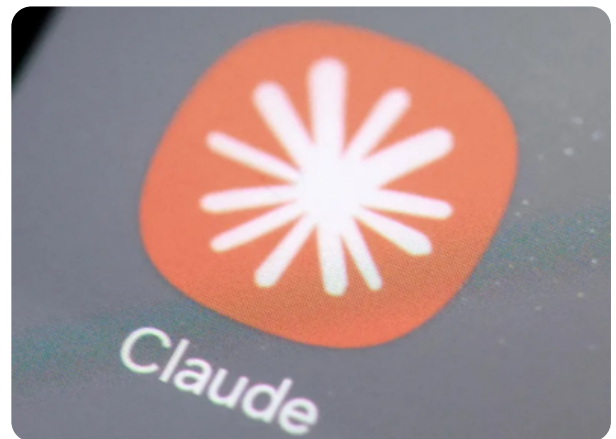
Claude AI пайдаланушыларының кейбір чаттары интернетте көпшілікке қолжетімді болып шықты.

Anthropic компаниясының Claude чат-ботын пайдаланған жүздеген қолданушының әңгімелері интернетте көпшілікке қолжетімді болғаны анықталды.

Кейбір чаттарда жеке мәліметтер мен жұмысқа қатысты ақпарат болған. Егер Google сияқты іздеу жүйелерінде арнайы іздеу сұранысы қолданылса, ол чаттарға сілтемелер іздеу нәтижелерінде көрсетілген.

Мәселенің негізгі себебі – пайдаланушы Claude платформасындағы әңгімені бөлісу функциясы арқылы бөліскеннен кейін, оған жасалған сілтемені Google сияқты іздеу жүйелері индекстеп, іздеу нәтижелерінде көрсете бастаған.

Anthropic компаниясының өкілінің айтуынша, Claude пайдаланушылар әңгімелерін бөлісу туралы шешімді өздері қабылдайды. Сондай-ақ ол чатқа жасалған сілтемелердің пайдаланушы өзі бөліспейінше кездейсоқ іздеу нәтижелерінен шықпайтынын мәлімдеді.



«Пайдаланушы әңгімені бөліскен кезде, ол бұл мазмұнды жалпыға қолжетімді етеді. Кез келген ашық веб-бет сияқты, мұндай мазмұнды үшінші тарап қызыметтері де архивтеп немесе индекстей алады», – деді **Anthropic** өкілі

Claude жүйесіндегі бөлісу функциясында «Сілтемесі бар кез келген адам бұл әңгімені көре алады» деген ескерту көрсетіледі. Алайда мұндай сілтемелердің іздеу жүйелерінде индекстелуі мүмкін екені нақты көрсетілмеген.

Бұл жағдайды алғаш болып Reddit платформасының қолданушылары анықтады. Олар іздеу жүйесінде жарияланған кемінде 25 беттен 200-ден астам Claude чаттарын тапқан. Кейбір әңгімелер бірнеше апта бұрын ғана жүргізілген. Жарияланған чаттарда пайдаланушылар Claude-қа түрлі тақырыптар бойынша сұрақтар қойған.



Мысалы, өткен жылы бір қолданушы Claude-тен: «Сен маған көмектескің келе ме, әлде Anthropic компаниясының мүддесін көбірек қорғайсың ба?» деп сұраған. Claude жауап ретінде: «Менде сізге көмектесуге бағытталған ұмтылысқа ұқсас сезім қалыптасады», – деп жауап берген.

Осыған ұқсас мәселе

Илон Маскқа тиесілі X әлеуметтік желісіндегі Grok чат-ботында да осындай жағдай тіркелген. Кейбір жағдайларда жүздеген мың чат жазбалары іздеу жүйелері арқылы интернетте қолжетімді болып кеткен.

2026 жылдың сәуір айындағы тағы бір әңгімеде қолданушы Claude-тен компанияның бұлттық қауіпсіздік жобасына қатысты әлі жарияланбаған блог мақаласын дайындауға көмек сұраған. Кейін ол бұл өтініштің әзіл емес екенін, адамның шынымен түлкіге айналу мүмкіндігі туралы сұрап отырғанын нақтылаған.

Claude алғашқы жауаптарының бірінде пайдаланушыға «Сізге толыққанды түлкі қабілеттері берілді!» деген сипаттамамен AI көмегімен жасалған суретті ұсынған.

Жарияланған чаттарда пайдаланушылар түйіндеме (CV) дайындауға көмек сұраған. Кейбір чаттарда олардың аты-жөні, жұмыс тәжірибесі және басқа да жеке мәліметтері кездескен.

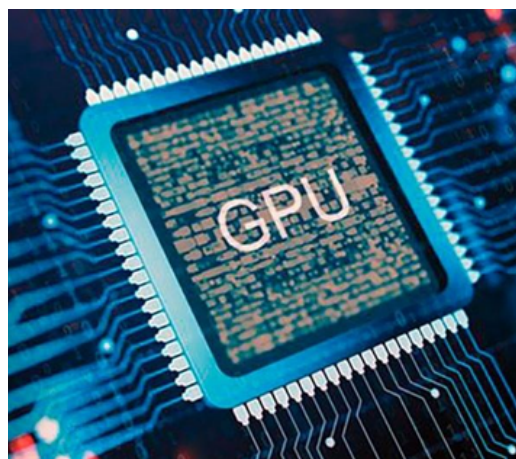
Осындай жағдай **2025** жылы ChatGPT сервисінде де тіркелген. Сол кезде кейбір чаттардың интернет арқылы көпшілікке қолжетімді болғаны анықталған.

Материал осы дереккөз негізінде дайындалды:
<https://www.bbc.com/news/articles/cly5qgjk5ywo>

AI инфрақұрылымы: техникалық негіздер

Техникалық инфрақұрылым – жасанды интеллект дамуының негізгі факторы.

Жасанды интеллекттің (AI) дамуы тек алгоритмдер мен бағдарламалық кодқа ғана емес, оны іске қосатын күрделі техникалық инфрақұрылымға да байланысты. Қазіргі заманғы үлкен тілдік модельдер, компьютерлік көру жүйелері және автономды роботтар миллиондаған есептеулерді бір уақытта орындауды талап етеді.



GPU: жасанды интеллекттің есептеу қозғалтқышы

Жасанды интеллекттің дамуы үлкен көлемдегі есептеулерді қажет етеді. Осы процесте **GPU (Graphics Processing Unit)** — параллель есептеулерге арналған негізгі технологиялардың бірі. CPU бір есепті ретімен орындаса, GPU мыңдаған операцияны бір уақытта өңдей алады.

Нейрондық желілерді оқыту кезінде миллиардтаған параметрлер есептеледі, сондықтан GPU модельдерді жылдам үйретуге мүмкіндік береді. Қазіргі AI индустриясында **NVIDIA** сияқты компаниялардың арнайы AI чиптері кеңінен қолданылады. Мысалы, **NVIDIA H100 Tensor Core GPU** үлкен тілдік модельдерді оқыту және жоғары өнімді есептеулер үшін пайдаланылады.

Қытайдың AI серпілісі: **Kimi K3** және жаңа бәсеке

Kimi K3: Қытайдың AI технологияларындағы жаңа қадамы

Қытайдың **Moonshot AI** компаниясы жаңа буын үлкен тілдік моделі — Kimi K3-ті таныстырды. Өзірлеушілердің мәлімдеуінше, модель есептеу тиімділігі мен интеллектуалдық мүмкіндіктері жағынан әлемдегі жетекші AI жүйелерімен бәсекелесе алады. Бұл жаңалық жаһандық жасанды интеллект саласындағы технологиялық бәсекенің күшейіп келе жатқанын көрсетеді.

Kimi K3 моделінің көлемі **2,8 триллион** параметрден тұрады. Салыстыру үшін, америкалық Anthropic компаниясының флагмандық **Claude Opus 4.8** моделінде сарапшылар бағалауы бойынша шамамен **1,5–2 триллион** параметр бар.

Параметрлер саны — нейрондық желінің көлемін сипаттайтын көрсеткіштердің бірі. Ол модельдің ақпаратты өңдеу, күрделі байланыстарды анықтау және әртүрлі тапсырмаларды орындауға әсер етеді.



Artificial Analysis және Arena.ai

компаниялары **Kimi K3** моделіне тестілер жүргізді. Зерттеу нәтижелеріне сәйкес, бұл модель OpenAI әзірлеген ChatGPT және Anthropic компаниясының Claude сияқты жетекші америкалық жасанды интеллект жүйелерімен салыстырмалы деңгейде нәтиже көрсетті.

Moonshot компаниясы Kimi K3 моделін ашық салмақты жүйе ретінде ұсынуды жоспарлап отыр. Бұл өзірлеушілер мен зерттеушілерге модельді жүктеп алып, оны өз қажеттіліктеріне қарай өзгертуге мүмкіндік береді. Ал OpenAI мен Anthropic компаниялары өз модельдерінің параметрлерін ашық жарияламайды.

Материал осы дереккөз негізінде дайындалды:

<https://www.bbc.com/news/articles/cy9w4q8pgp0o>

TECHDAMU

Технология • Инновация • Болашақ



РЕДАКТОРЛАР

Молдажан Айдана
Абдіғаппар Мөлдір



WEB
<http://galym.org>



Email
galymorg@gmail.com



Instagram
[@galym_org](https://www.instagram.com/galym_org)

№06
ШЫҒАРЫЛЫМ

2026
АЛМАТЫ
ҚАЗАҚСТАН