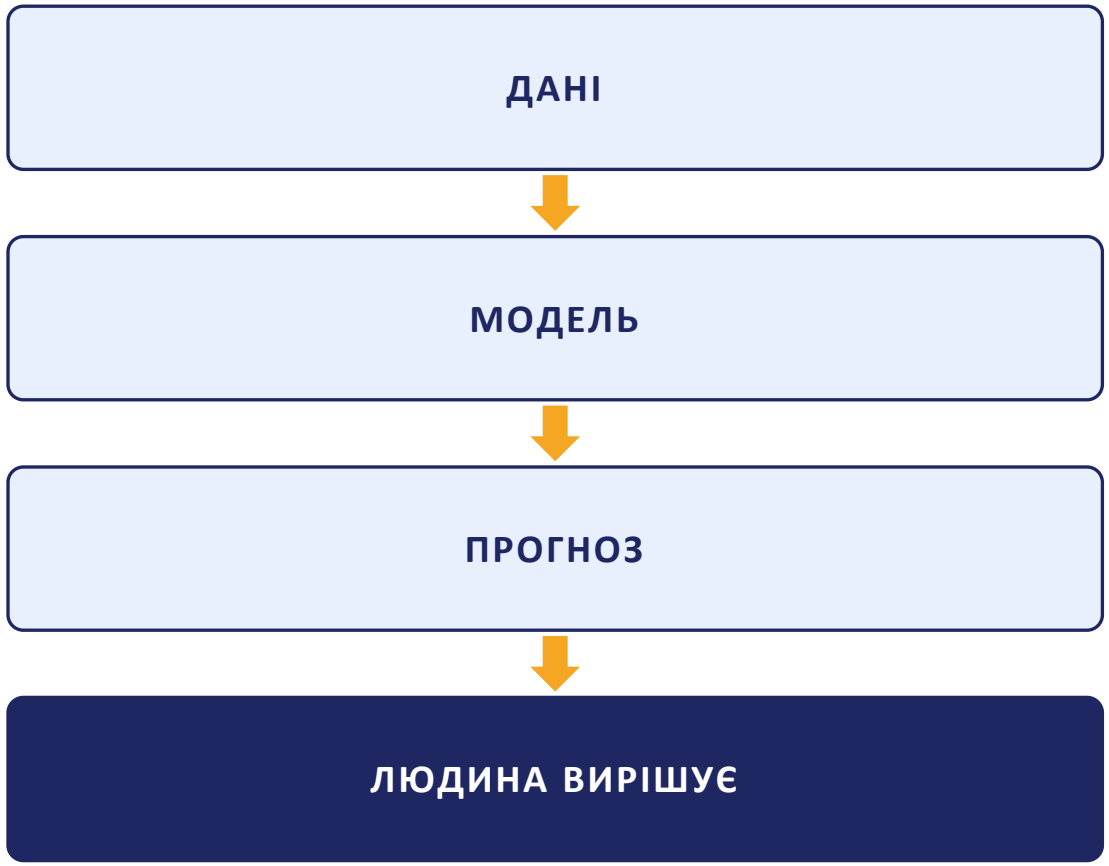
Георгій Вишня,
CTO/co-founder, aistra.biz

Від прогнозування до агентного ШІ

Підготовлено в липні 2026

Звідки ми починали: прогнозний ШІ

1. Навчання з учителем (supervised learning): регресія та класифікація
2. Прогнозування часових рядів для попиту, ризиків, обслуговування або класифікація спостережень/кейсів
3. Результат — число, ймовірність або належність до дискретного класу, але не рішення
4. Цикл завжди замикає людина



Ключовий зсув: робочі процеси проти агентів

W Робочий процес

- LLM та інструменти оркеструються за заздалегідь визначеними шляхами коду
- Передбачуване, послідовне виконання
- Найкраще для чітко визначених, повторюваних завдань

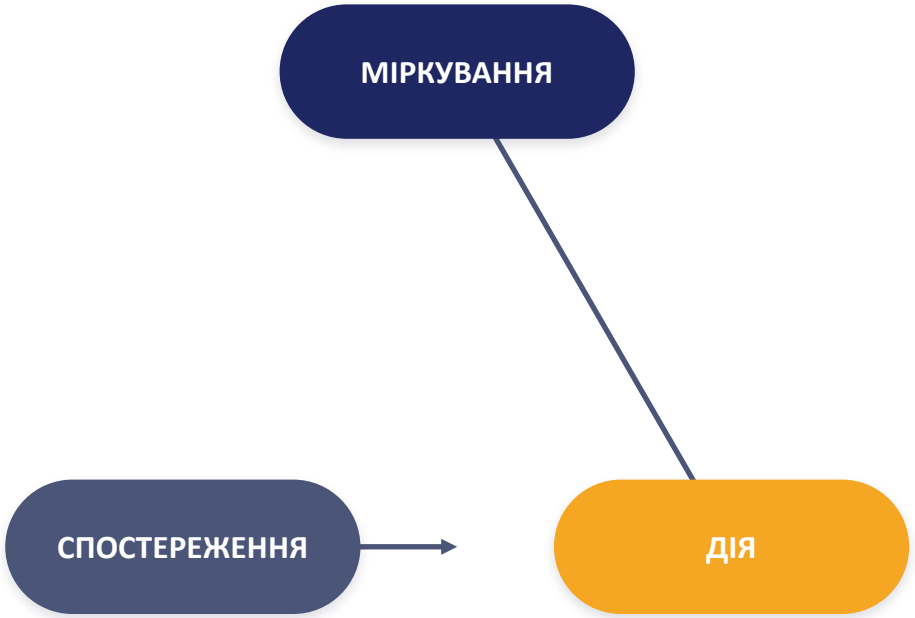
A Агент

- LLM динамічно керує власним процесом і використанням інструментів
- Зберігає контроль над тим, як виконати завдання
- Є Найкращим для гнучкості та відкритих задач

«Агенти — це системи, у яких LLM динамічно керують власними процесами та використанням інструментів, зберігаючи контроль над тим, як вони виконують завдання».

— Anthropic, «Building Effective Agents»

Міркування → Дія → Спостереження



1. ReAct (Yao та ін., 2023) поєднує ланцюжки міркувань із конкретними діями

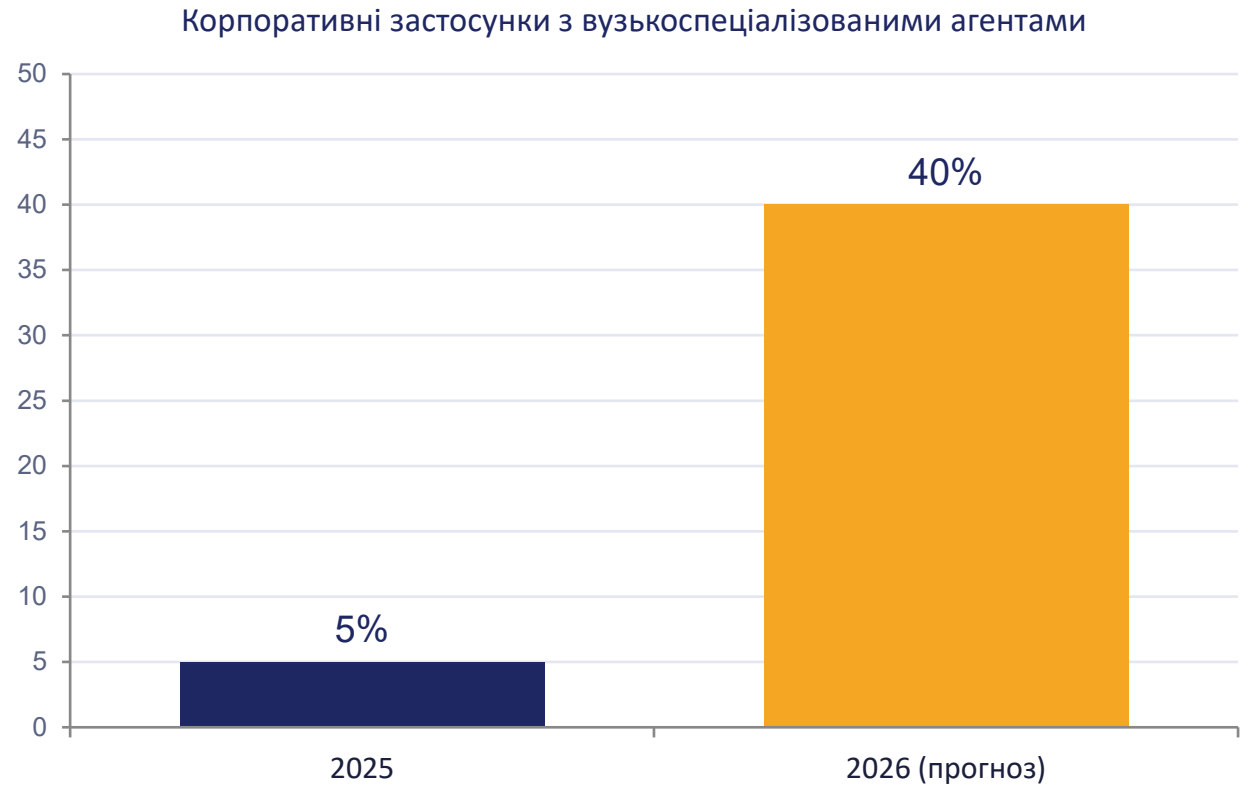
2. Дії дозволяють моделі звертатися до зовнішніх джерел, а не покладатися лише на внутрішні — і часто хибні — знання

3. Цей цикл є механічним ядром практично кожного сучасного агента, що використовує інструменти

Що стоїть за агентом

Контекстна інженерія	Підбір оптимального набору токенів, які модель бачить на кожному кроці
Пам'ять	Збереження релевантного стану між кроками та сесіями
Model Context Protocol (MCP)	Стандарт того, як агенти виявляють і викликають зовнішні інструменти
Використання інструментів / виклик функцій	Механізм, що дозволяє LLM виконувати реальні дії у світі
Базова модель	Двигун міркувань, на якому тримається все інше

Впровадження — це реальність



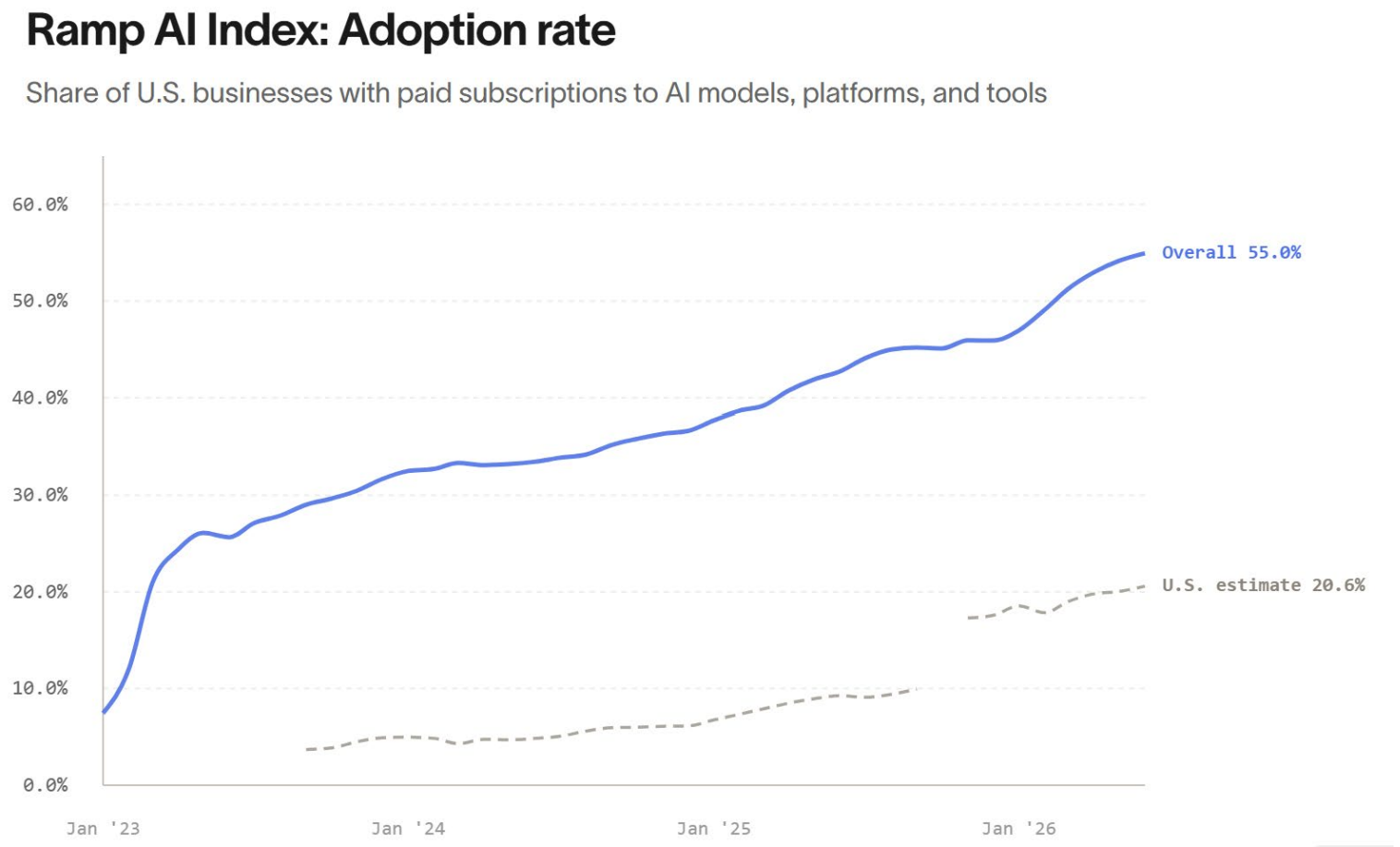
Джерело: Gartner, серпень 2025

74%

компаній планують помірне або масштабніше впровадження агентного ШІ протягом двох років

порівняно з 23% раніше (Deloitte, опитування щодо корпоративного ШІ, 2025)

Впровадження — це реальність



Джерело: https://ramp.com/data/ai-index, липень 2026

Прогнозування не зникає — воно вбудовується

Прогнозний ШІ

прогнозує результати,
симулює сценарії

Агент

планує, діє,
оркеструє

1	2	3	4	5
Інформувати	Прогнозувати	Виконувати	Рекомендувати	Оркеструвати

Перевірка реальністю

40%+

проєктів агентного ШІ, за прогнозами, зазнають невдачі до 2027 року

Gartner

27%

глобальна довіра до повністю автономного ШІ у 2026 році — порівняно з 43% у 2025 р.

галузеве опитування, 2025

“—”

«Agent-washing»: перейменування простих асистентів на «агентів»

Gartner

Потенційні бар`єри впровадження

Складність

Новини 2026 року свідчать, що значна кількість клієнтів не може перетворити передову модель ШІ на результат самостійно.

OepAI, Anthropic, Microsoft

Бюджети

В США лише 18% компаній мають статті бюджету на використання ШІ, за даними US Census Buerau

RAMP AI Index, 2026

Ризики

Системи ШІ підпадають під дію «новітніх» ризиків, які не були притаманні іншим IT-системам

Gartner

Складність: реалії 2026 р.

1. **2 липня 2026 р.** Microsoft оголошує підрозділ впровадження ШІ: $2.5 млрд і 6 000 співробітників.

2. **11 травня 2026 р.** OpenAI створює структуру з промовистою назвою — The Deployment Company. Компанія з розгортання.

3. **15 липня 2026 р.** Anthropic разом із Blackstone, Hellman & Friedman, Goldman Sachs, General Atlantic, Apollo, GIC і Sequoia запускає **Ode** — окрему фірму, яка входить у корпорацію і впроваджує Claude руками власних інженерів.

4. Дослідження NBER на ~6 000 керівників: 69% компаній з-поміж опитаних використовують ШІ, і при цьому **дев'ять із десяти не бачать жодного впливу на зайнятість чи продуктивність** (нездатність розкрити потенціал новітніх моделей ШІ самостійно).

5. **Про що це говорить:** Існує розрив між моделлю ШІ і бізнес-процесом.

Джерело: новини індустрії, травень-липень 2026

RAMP AI Index: бюджетні тренди «під капотом»

1. Медіанна компанія в США витрачає на ШІ… $11.38 на співробітника на місяць. Менше, ніж на каву

2. Топ-10% компаній — $611 на місяць.

3. Топ-1% — $7 449 на людину, і саме вони нарощують витрати на +14% щомісяця, навіть переходячи на дешевші моделі.

4. Клієнти Ramp — молоді, технологічні, здебільшого венчурні компанії США, тож «54% бізнесів платять за ШІ» — це про авангард. По всій економіці США, за даними Census Bureau, ШІ використовує лише ~18% фірм.

Джерело: https://ramp.com/data/ai-index, липень 2026

Нові ризики потребують нового управління

OWASP Top 10 для агентних застосунків (2026)

- Викрадення цілі
- Зловживання інструментами
- Зловживання ідентифікацією та привілеями
- Отруєння пам'яті
- Каскадні збої

Регуляторний часовий графік

черв. 2026 — Закон штату Колорадо про ШІ набуває чинності

серп. 2026 — Зобов'язання ЄС щодо систем ШІ високого ризику набувають повної чинності

Кейс 1: аналітична система Due Dilligence

1. **Замовник**: міжнародна бухгалтерська й аудиторська компанія, що діє в ЄС

2. **Мета**: автоматизація підготовки аналітичних дос’є з метою проведення Due Dilligence компаній-контрагентів

3. **Результат**: побудова автоматизованих конвеєрів даних із застосуванням агентів Ші за допомогою платформи N8N

4. **Lessons Learned:** low code/no code-платформи можуть бути ефективними й у царині агентського ШІ

Кейс 2: Realtime Competitor Intelligence

1. **Замовник**: Американська консалтингова компанія середніх розмірів

2. **Мета**: створення аналітичної системи, що відстежує найм персоналу конкурентами (LinkedIn), новини про залучення фінансування, запуск нових продуктів, відгуки клієнтів, вакансії та участь у конференціях. Формує щотижневі «бойові картки» (battlecards) для команди продажів, які показують, чим займаються конкуренти, які кроки вони роблять та як змінюється їхня ринкова активність.

3. **Результат**: успішне впровадження системи, розробленої на Python

4. **Lessons Learned:** персоналізація агентів та надання їм певних «психотипів» може покращити рівень задоволення від використання систем агентського ШІ

Кейс 3: платформа мульти-агентської взаємодії

1. **Замовник**: американська компанія з розробки програмного забезпечення (startup)

2. **Мета**: незалежне тестування й вдосконалення бізнес-орієнтованої платформи ШІ, яка використовує технологію мультиагентної взаємодії типу «glass-box» («прозора архітектура») для одночасної оркестрації роботи кількох моделей ШІ. Замість того щоб покладатися на єдиний ШІ-чатбот, її робочий простір використовує екосистему агентів ШІ, що ведуть між собою дискусію, взаємно перевіряють результати та доповнюють один одного, забезпечуючи високий рівень достовірності й результати корпоративного класу.

3. **Результат**: тестування і апробація системи, підготовка до запуску платформи в продуктив

4. **Lessons Learned:** складність адаптації технологій та моделей ШІ є реальністю на західних ринках

ПІДСУМОК

Практичні висновки

1. Починайте з найпростішого рішення — додавайте агентну складність лише тоді, коли вона виправдана
2. Враховуйте бюджетні обмеження й компроміси (доступ до LLM через API в рази дорожчий)
3. Надійність важливіша за автономність для продуктивного використання

«Ефективні агенти нудні. Вони працюють. Вони надійні. Вони завершують завдання».

ДОДАТОК

Джерела

Фундаментальні технічні джерела

Yao та ін., «ReAct: Synergizing Reasoning and Acting in Language Models», ICLR 2023 — arxiv.org/abs/2210.03629

Anthropic, «Building Effective AI Agents» — anthropic.com/research/building-effective-agents

Anthropic, «Effective Context Engineering for AI Agents» — anthropic.com/engineering

Anthropic, «Writing Effective Tools for AI Agents» — anthropic.com/engineering

Ринок та впровадження

Gartner, «40% of Enterprise Apps Will Feature Task-Specific AI Agents by 2026», серпень 2025 — gartner.com

Deloitte Insights, «Agentic AI Strategy», 2026 Tech Trends — deloitte.com

World Economic Forum, «Agentic AI Will Revolutionize Business in the Cognitive Era» — weforum.org

Futurum, «Was 2025 the Year of Agentic AI, or Just More Agentic Hype?» — futurumgroup.com

Управління та ризики

OWASP, «Top 10 for Agentic Applications 2026» (через Microsoft Open Source Blog) — opensource.microsoft.com

Cloud Security Alliance, «Agentic AI Governance: NIST Standards for Autonomous Systems», березень 2026

TechTarget, «How Agentic AI Governance Tackles Data, Security Challenges» — techtarget.com

arXiv 2510.15739, «AURA: An Agent Autonomy Risk Assessment Framework»