ТЕХНОЛОГІЇ ШТУЧНОГО ІНТЕЛЕКТУ ТА БЕЗПЕКА ДАНИХ

Лекція 1

Що таке штучний інтелект: від алгоритмів до генеративних моделей

Освітня програма «Економіка і аналітика» · 1 курс · 4 кредити ECTS

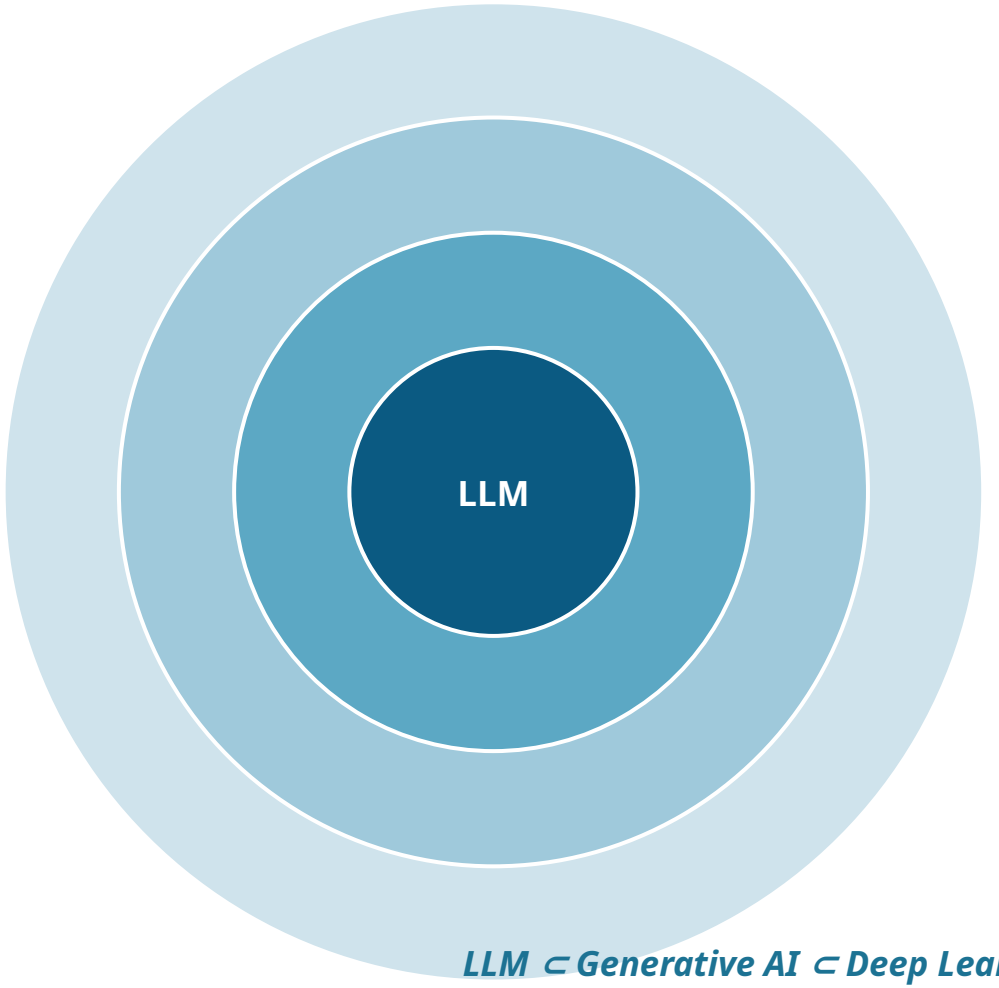
Чому саме зараз такий інтерес до ШІ?

- Термін «штучний інтелект» існує в науці понад 70 років, але масовим став лише нещодавно
- **Головна хибна теза, яку варто розвінчати:**
  - «ШІ» і «LLM» (великі мовні моделі, напр. ChatGPT) — не синоніми
  - LLM — лише один із сучасних різновидів ШІ
- Мета лекції — розвести терміни й побачити ШІ ширше, ніж чат-боти

Різкий стрибок — реліз ChatGPT (кінець 2022)

ТЕРМІНОЛОГІЯ

ШІ, машинне навчання, глибоке навчання, генеративний ШІ



Штучний інтелект (AI)
Будь-яка спроба відтворити машиною процес прийняття рішень

Машинне навчання (ML)
Система вчиться на даних, а не на жорстких правилах

Глибоке навчання (DL)
Багатошарові штучні нейронні мережі

Генеративний ШІ / LLM
Генерує новий текст, зображення, код

LLM ⊂ Generative AI ⊂ Deep Learning ⊂ Machine Learning ⊂ AI

ВИЗНАЧЕННЯ 1 / 3

Що таке штучний інтелект?

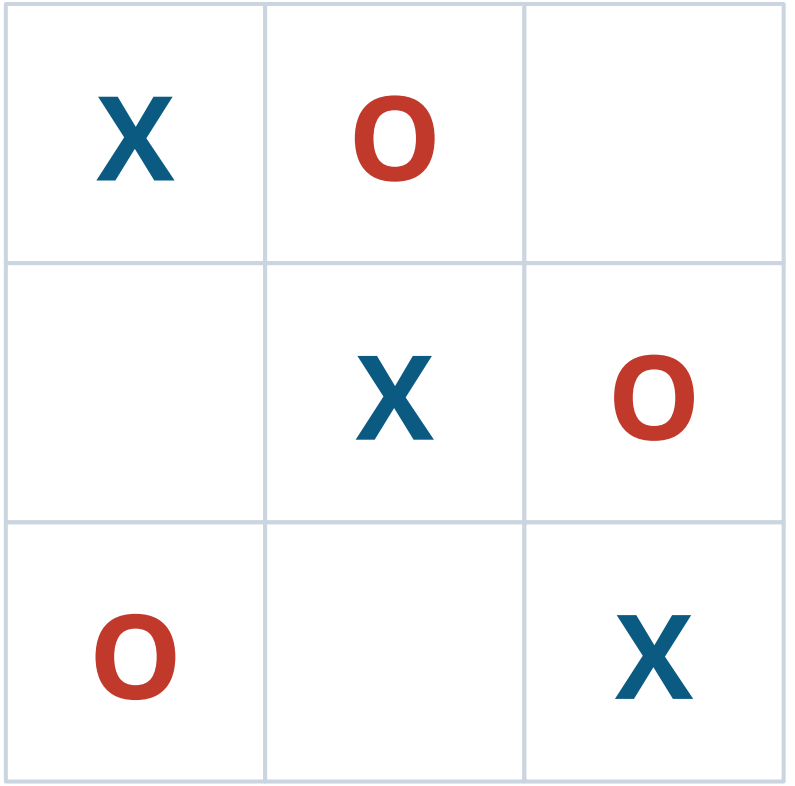
Спроба за допомогою математичних формул та алгоритмів відтворити логіку людського міркування та прийняття рішень.

Важливо: ШІ не обов'язково означає «навчання» чи «розум» — досить, щоб система імітувала прийняття рішень.

ПРИКЛАД

Приклад елементарного ШІ: хрестики-нулики

- **Правило 1 (Перемога)**
  - два свої знаки в ряд → поставити третій
- **Правило 2 (Блок)**
  - два знаки суперника в ряд → заблокувати
- **Правило 3 (Центр)**
  - центр вільний → зайняти (більше варіантів)
- **Правило 4 (Рандом)**
  - жодне правило не спрацювало → випадкова клітинка



Процес прийняття рішень визначений людською логікою — тому це вже підпадає під визначення «штучного інтелекту», хоч і без жодного навчання чи статистики.

ВИЗНАЧЕННЯ 2 / 3

Що таке машинне навчання (ML)?

Різновид ШІ, що має подобу «пам'яті» і використовує її для покращення результатів. По суті — поєднання статистики та алгоритмів.

Класичний ШІ (п. 3)

Людина сама пише правила («якщо..., то...»)

Машинне навчання

Система сама виводить закономірності з великої кількості прикладів (даних)

МАШИННЕ НАВЧАННЯ

Навчання з учителем: приклад — розпізнавання цифр

1 Тренування → **2 Валідація** → **3 Тестування**

Приклад + правильна відповідь

Аналогічний приклад — перевірка результату

Незнайомий приклад — фінальна перевірка

Аналогія: підручник з розв'язаними прикладами → домашнє завдання з ключем → контрольна робота без підказок

- Датасет: тисячі зображень рукописних цифр (0–9), кожне 28×28 пікселів
- Кожне зображення має відому правильну мітку — яка це цифра
- Модель поступово вчиться асоціювати «малюнок» із правильною цифрою

ЛІРИЧНИЙ ВІДСТУП

Типи помилок моделі — і їхня ціна

Помилка I роду

(false positive — «хибне спрацювання»)

Модель каже «так», хоча насправді «ні».
Приклад: чоловіку кажуть «ви вагітні».

Помилка II роду

(false negative — «хибний пропуск»)

Модель каже «ні», хоча насправді «так».
Приклад: вагітній жінці кажуть «ви не вагітні».

Для економіста це важливо:

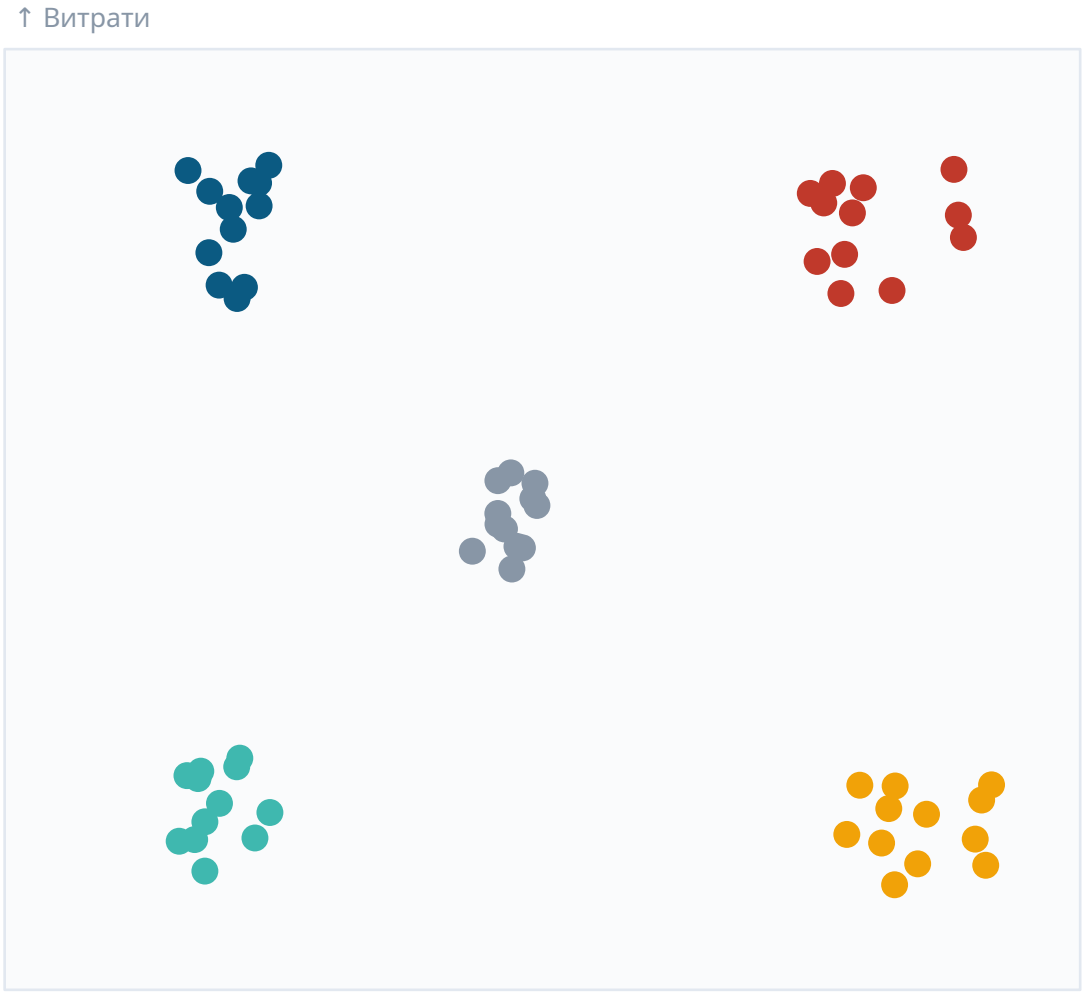
• Кредитний скоринг: відмовити надійному клієнту (I рід) = втрачений прибуток; видати кредит ненадійному (II рід) = прямі збитки.

• Антифрод: пропустити шахрайство (II рід) зазвичай дорожче за хибне блокування (I рід).

Навчання без учителя: кластеризація клієнтів магазину

Комп'ютеру не дають «правильну відповідь» — лише характеристики і завдання: «згрупуй схожі точки в групи».

- Ознаки: річний дохід і рівень витрат клієнта
- Модель сама виділяє групи (кластери) без підказок
- **Низький дохід + великі витрати**
  - → схильні до імпульсивних покупок, кандидати на розстрочку
- **Високий дохід + великі витрати**
  - → преміум-клієнти, варто утримувати лояльність



ЛІРИЧНИЙ ВІДСТУП

Чому ШІ переважає людину в багатовимірних задачах?

- Людина візуально аналізує залежності максимум у 2–3 вимірах (лінія, площина, 3D-об'єкт)
- Реальні бізнес-задачі мають десятки й сотні змінних одночасно (дохід, вік, регіон, історія покупок, сезонність…)
- Людина фізично не може «побачити» чи уявити таку залежність
- Алгоритму не потрібно «уявляти» простір геометрично — він оперює рівняннями в N-вимірному просторі так само «легко», як і в двовимірному

ШІ не «розумніший» за людину — він просто не обмежений біологією зорового сприйняття.

ВИЗНАЧЕННЯ 3 / 3

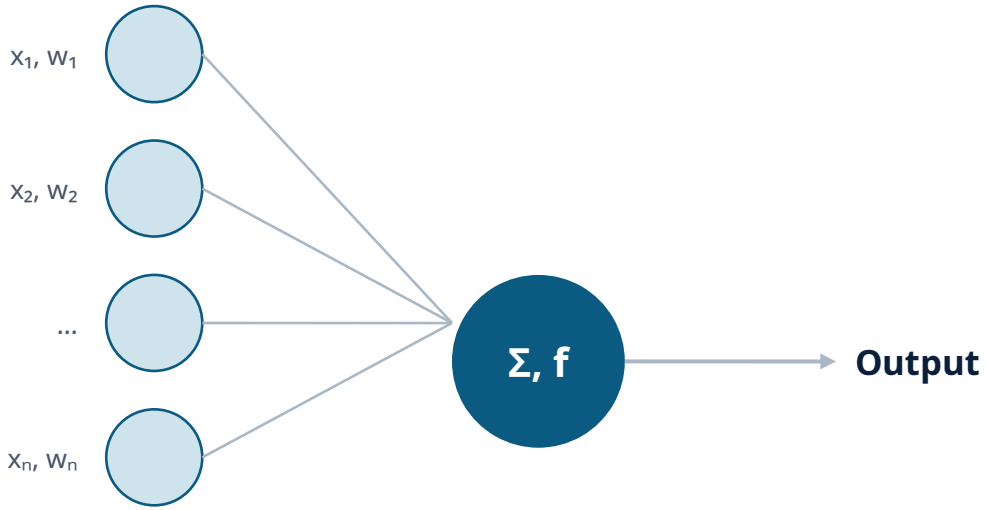
Що таке глибоке навчання (DL)?

Використання штучних нейронних мереж, де навчальними прикладами є «представлення» даних.

- **Класичний ML:**
  - людина сама обирає ознаки (дохід, вік, кредитна історія)
- **Глибоке навчання:**
  - мережа сама виявляє потрібні ознаки із «сирих» даних — пікселів, тексту, звуку

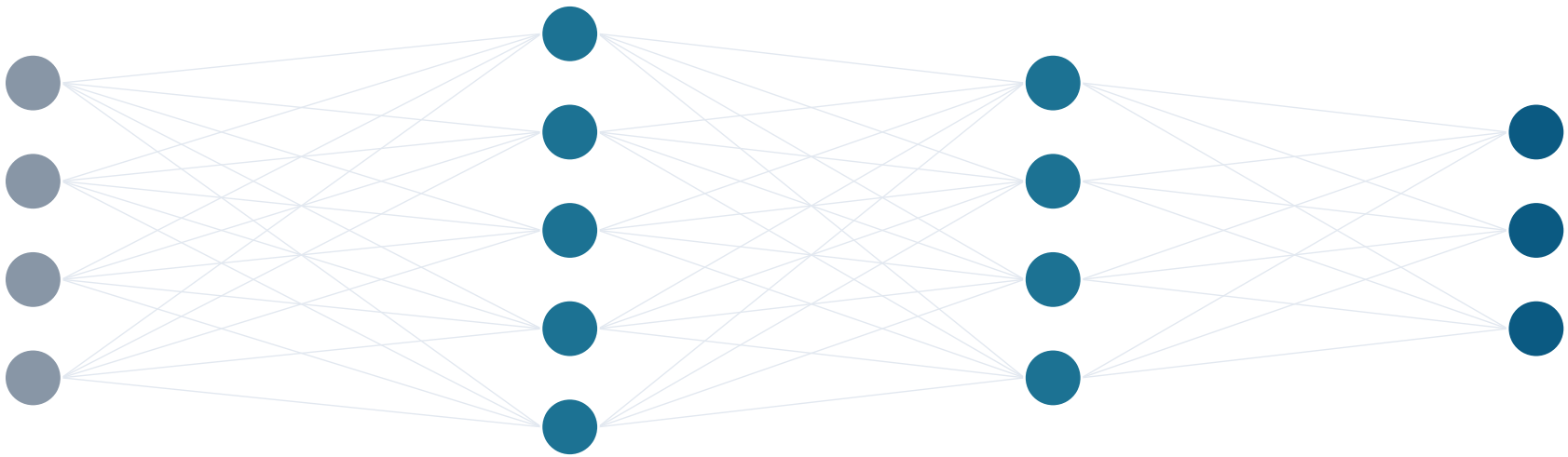
Лінійний перцептрон — «цеглинка» нейромережі

- Найпростіша штучна нейронна «клітина» — груба аналогія з біологічним нейроном
- Отримує кілька входів ($x_1…x_n$) з вагами ($w_1…w_n$)
- Рахує зважену суму → застосовує функцію активації → видає результат
- **«Навчання» мережі**
  - = поступовий підбір ваг (w), щоб вихід збігався з правильною відповіддю



ПРИКЛАД

Розпізнавання цифр нейронною мережею



Вхідний шар

784 пікселі (28×28)

Прихований шар

128 нейронів

Прихований шар

64 нейрони

Вихідний шар

10 цифр (0–9)

Мережа сама виявляє ознаки (лінії, вигини, форми) з тисяч прикладів — без ручного програмування правил.

ВИЗНАЧЕННЯ 4 / 4

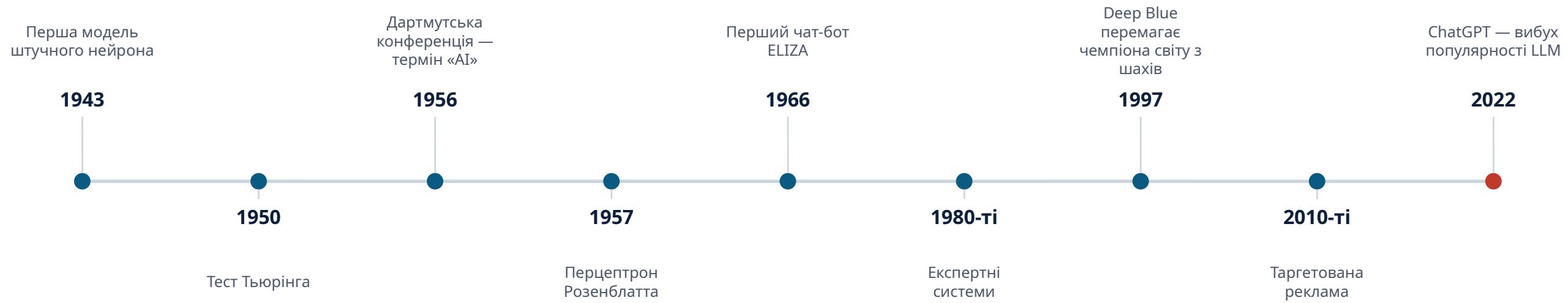
Що таке генеративний ШІ?

Штучний інтелект, здатний генерувати новий контент (текст, зображення, код) через «породжуючі» моделі.

- Опрацювавши величезні обсяги даних, модель продукує власні дані, схожі на ті, що вона опрацювала
- Це ті самі нейромережі (п. 9–11), тільки значно більшого масштабу
- Мережа отримує запит, «декомпонує» його і через ряд перетворень видає відповідь, максимально подібну на людську
- **Великі мовні моделі (LLM)**
  - — генеративний ШІ, спеціалізований на тексті (ChatGPT, Claude, Gemini…)

ІСТОРІЯ

Коротка історія штучного інтелекту



Від першої ідеї (1943) до масового продукту (2022) — майже 80 років.

ЧОМУ «РАПТОМ»?

Три стримуючі фактори розвитку ШІ

1

Технічні можливості

Достатня обчислювальна потужність (GPU, дата-центри) для тренування великих моделей

2

Інтерес великого бізнесу

Готовність компаній інвестувати значні кошти в розробку й впровадження

3

Дані для навчання

Наявність достатньої кількості якісних, оцифрованих даних

Технологія «вистрелює», лише коли всі три фактори збігаються одночасно — саме через цю призму розберемо наступні три сплески популярності ШІ.

ПЕРШИЙ СПЛЕСК ПОПУЛЯРНОСТІ

Експертні системи 80-х у банківській сфері

Технічні можливості

Комп'ютери вже здатні зберігати порівняно великі обсяги даних

Дані

Банки накопичили дані про кредитні історії клієнтів у цифровому вигляді

Інтерес бізнесу

Банки хочуть приймати рішення про кредити на основі даних, а не лише думки експерта

Результат: «Експертні системи» — база знань + механізм логічного виведення + інтерфейс користувача. Системи підтримки прийняття рішень на основі формалізованих правил.

ДРУГИЙ СПЛЕСК ПОПУЛЯРНОСТІ

Таргетована реклама (2000-ні – 2010-ті)

Технічні можливості

Великі сервери зберігають дані про поведінку користувачів у браузері під час покупок

Дані

Історичні дані онлайн-магазинів вже накопичені

Інтерес бізнесу

Магазини хочуть підвищувати конверсію через персоналізовану рекламу

Результат: Рекомендаційні системи («покупці, які придбали цей товар, також купували...») та таргетована реклама — основа бізнес-моделі більшості онлайн-платформ і донині.

Поява великих мовних моделей

Технічні можливості

Сучасні GPU дозволяють тренувати величезні моделі в рази швидше

Дані

Дані не потрібно спеціально шукати — існує весь інтернет

Інтерес бізнесу

Бізнес-інтерес прийшов після того, як люди відчули в LLM не інструмент, а «співрозмовника»

Результат: Уперше всі три фактори зійшлися одночасно й у величезному масштабі — звідси вибухова хвиля інвестицій, досліджень і продуктів 2022–2026 років.

ПІДСУМОВУЄМО

Що варто запам'ятати з цієї лекції

- ШІ ≠ LLM: LLM — лише вершина великої піраміди ШІ → ML → DL → GenAI
- ШІ — це імітація прийняття рішень; ML — це навчання на даних, а не жорсткі правила
- Три фактори визначають, коли технологія стає масовою: обчислення, дані, інтерес бізнесу
- LLM — перший випадок, коли всі три фактори зійшлися одночасно й глобально
- Наступні лекції: як безпечно працювати з даними у світі LLM — організаційно та юридично

Дякую за увагу!