

# Система виявлення аномалій на основі нейронних мереж

---

Виконала Томенко Наталя

Керівник к.т.н., доц. Савченко Т.В.

---

КН 2025 | НаУКМА

1

Недостатня ефективність традиційних методів

2

Потреба в ефективних підходах постійно зростає

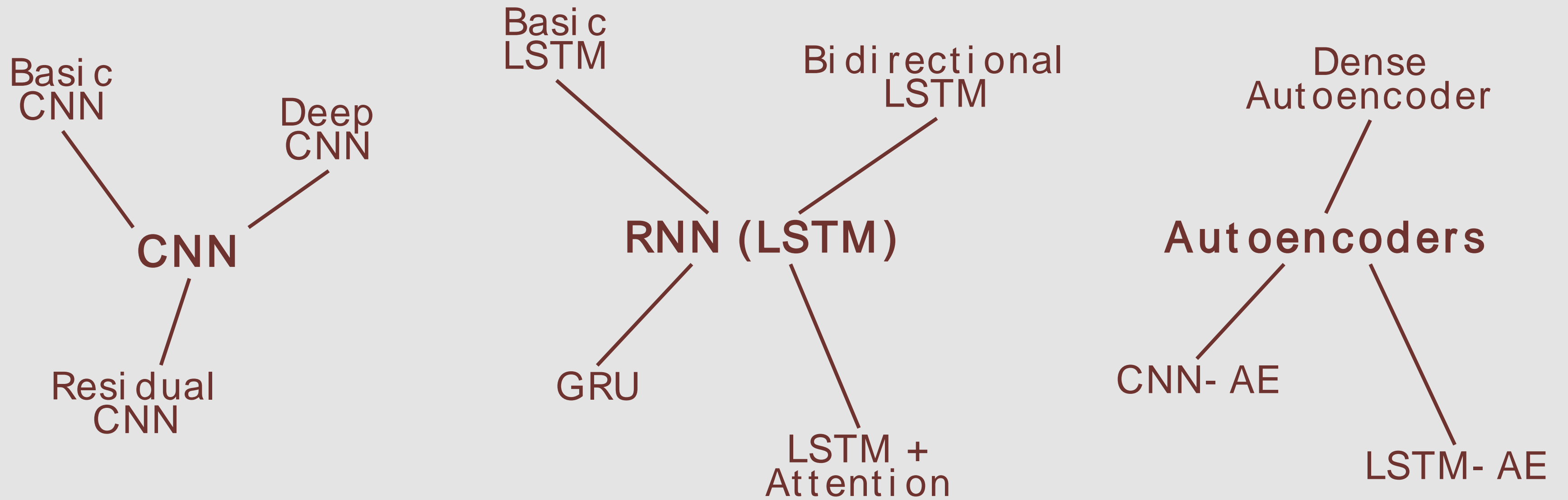
3

Використання нейронних мереж показує високі результати

**Домен:** мережеві аномалії

- 0 1 Брак комплексних досліджень
- 0 2 Проблема узагальнення моделей
- 0 3 Адаптація до змін мережевого середовища
- 0 4 Інтерпретованість результатів
- 0 5 Виявлення нульового дня та невідомих атак
- 0 6 Баланс між точністю та обчислювальною ефективністю

**Мета дослідження:** вирішення відкритих питань та формування комплексних знань про ефективність різних архітектур нейронних мереж для виявлення аномалій.



**Мета експерименту:** Встановити базову ефективність різних архітектур нейронних мереж для виявлення мережових аномалій.

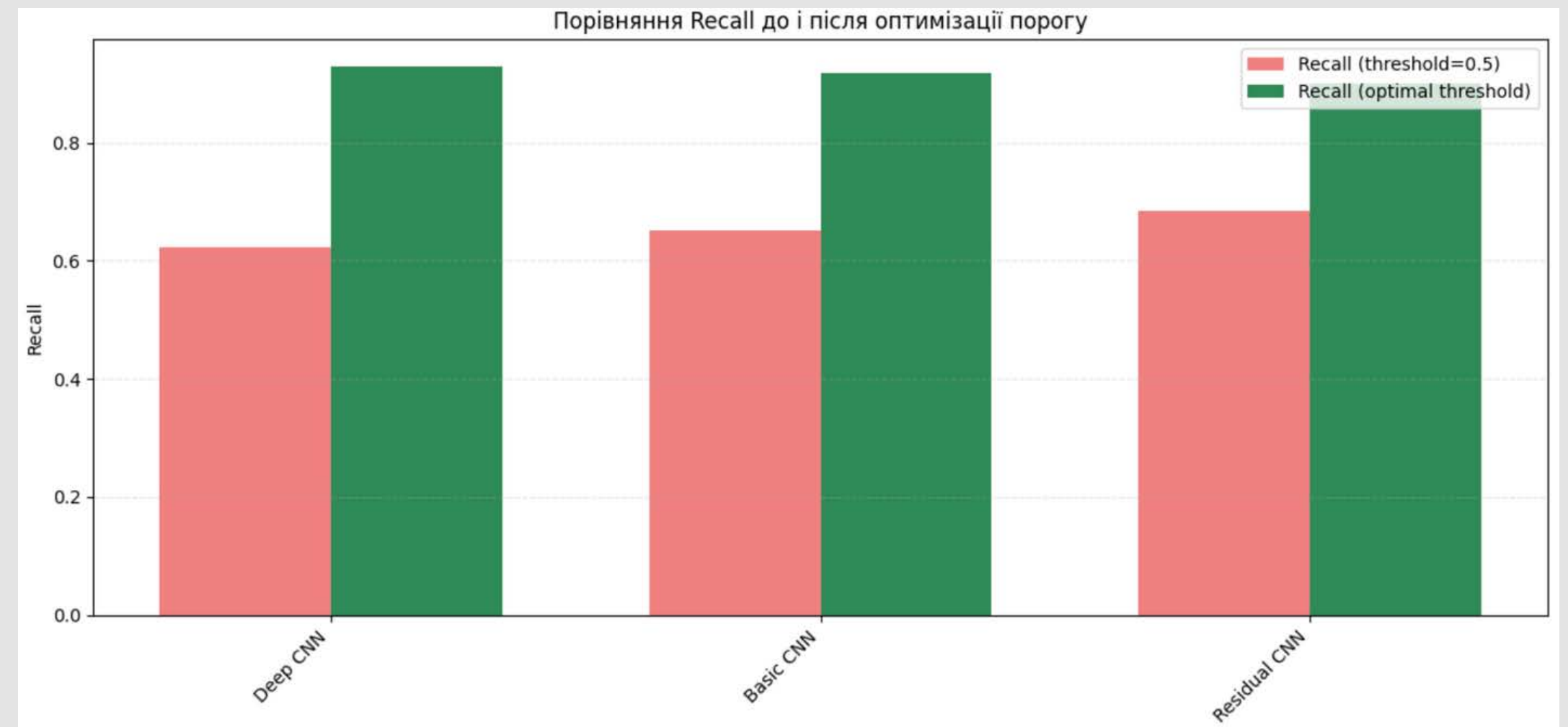
**Набір даних NSL-KDD:** еталонний датасет для виявлення мережових аномалій.

**Виявлена проблема:**

Стандартний поріг класифікації 0.5 дає погані результати → Розроблено метод оптимізації порогу за F1 оцінкою

**Наслідки оптимізації порогу:**

Покращення Recall на майже 40%. (з 62-68% до 90-92%)



**Результати з оптимальними порогами:**

	precision	recall	F1	ROC AUC
Базова CNN	88.70%	91.90%	90.20%	93.00%
Deep CNN	89.10%	92.90%	90.90%	93.10%
Residual CNN	89.20%	90.00%	89.60%	92.40%
Basic LSTM	87.90%	87.40%	87.70%	89.60%
Bidirectional LSTM	87.40%	89.50%	88.40%	92.40%
GRU	85.10%	91.70%	88.30%	91.40%
LSTM with Attention	86.30%	87.80%	87.00%	89.40%
Dense Autoencoder	88.50%	95.30%	91.80%	93.40%
CNN Autoencoder	85.90%	97.00%	91.10%	95.30%
GRU Autoencoder	97.30%	99.80%	98.50%	99.10%

**Найкращі результати - GRU Autoencoder**

**Інші моделі:**

- Dense Autoencoder: F1=91,8%
- CNN Autoencoder: F1=91,1%
- Deep CNN: F1=90,9%
- Bidirectional LSTM: F1=88,4%

Тестування здатності моделей, навчених на NSL- KDD, адаптуватися до нового домену UNSW- NB15, імітуючи концептуальний дрейф мережевого середовища чи перенос системи між середовищами.

**NSL- KDD**



**UNSW - NB15**

### Методологія експерименту:

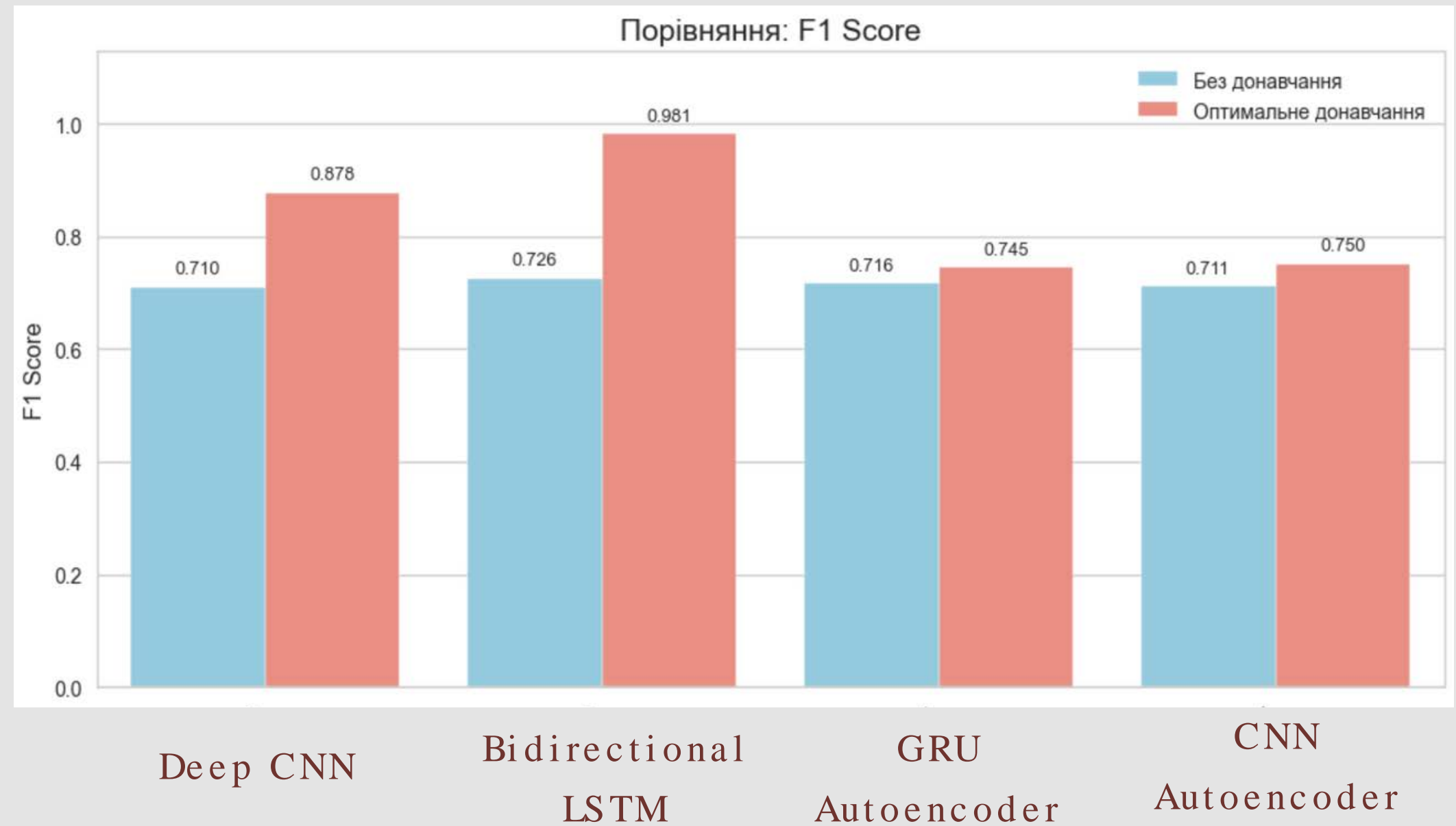
1. Вибір найкращих моделей
2. Створення відповідного адаптаційного шару для роботи з даними UNSW- NB15.
3. Застосування адаптованої моделі до тестових даних
  - а. без будь-якого донавчання
  - б. з донавчанням на 1% до 50 % UNSW- NB15

## Прямий трансфер:

F1  $\approx$  71% (падіння з 88-98%)

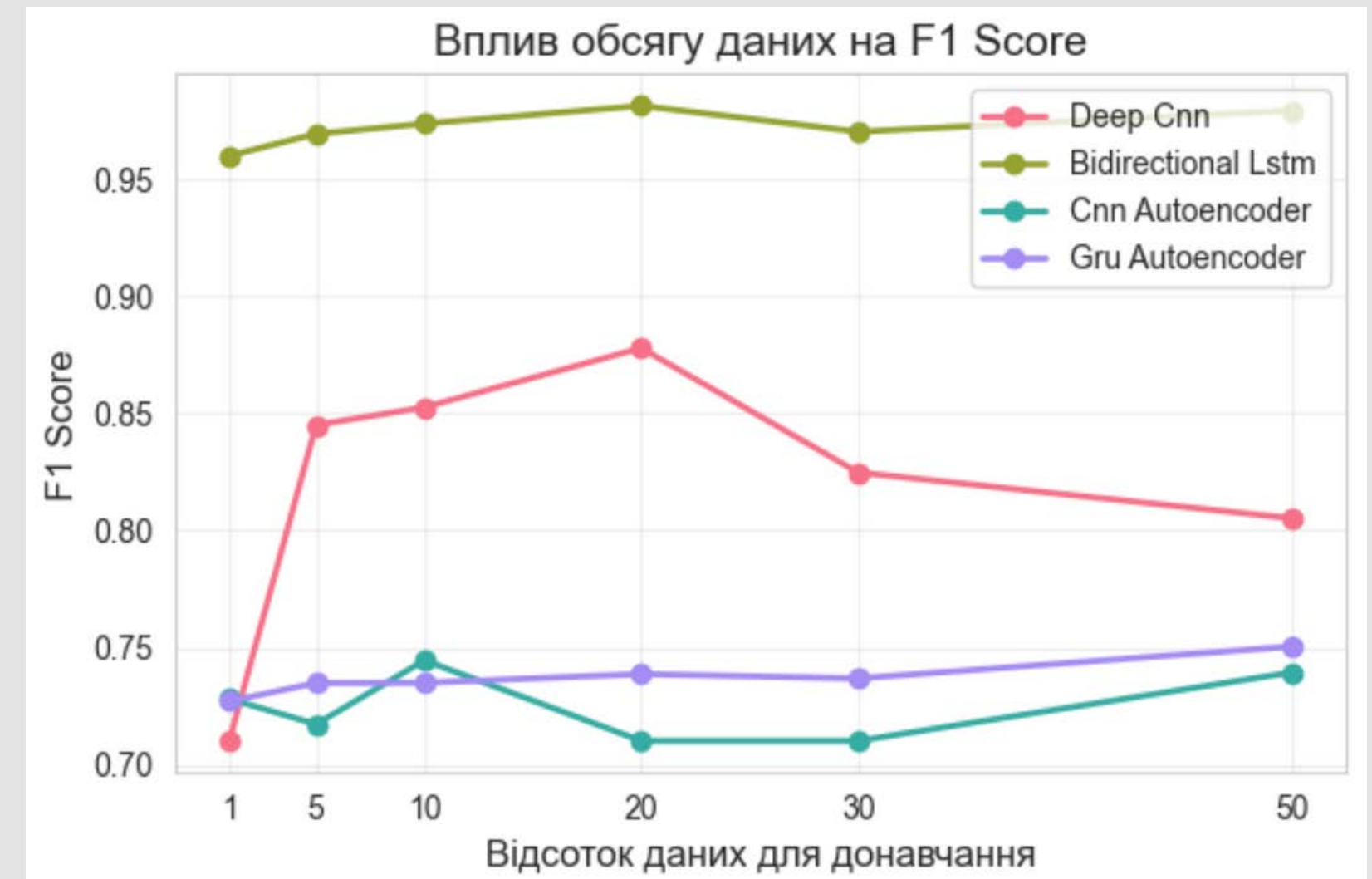
## Трансфер із донавчанням:

Покращення від 4% до 35% порівняно з прямим трансфером



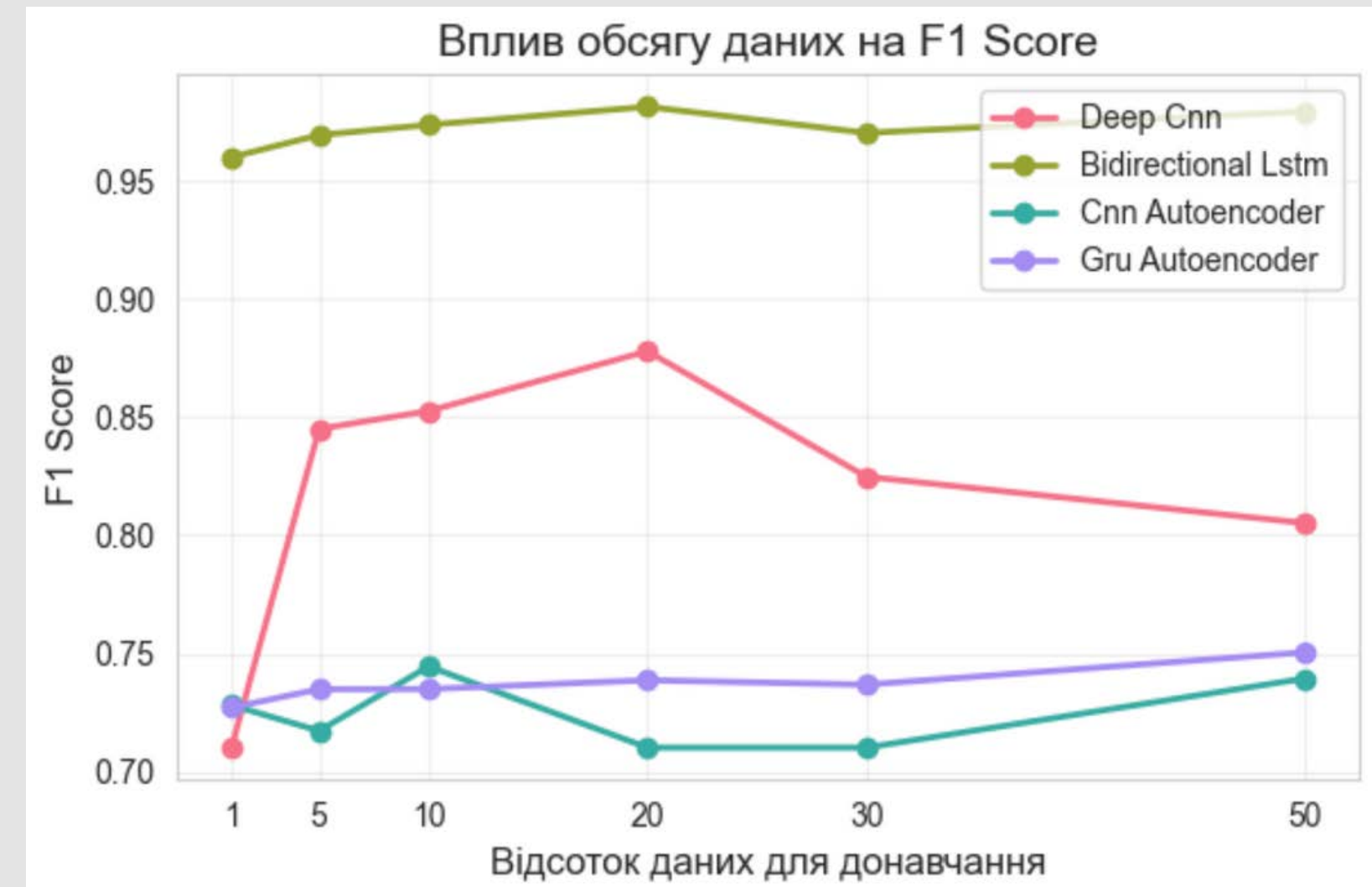
## Bidirectional LSTM

- Найкраща трансферність:
  - $F1 = 0.9599$  уже при 1% даних.
  - Максимум:  $0.9812$  (20%).
- Стабільність при будь-якому обсязі даних



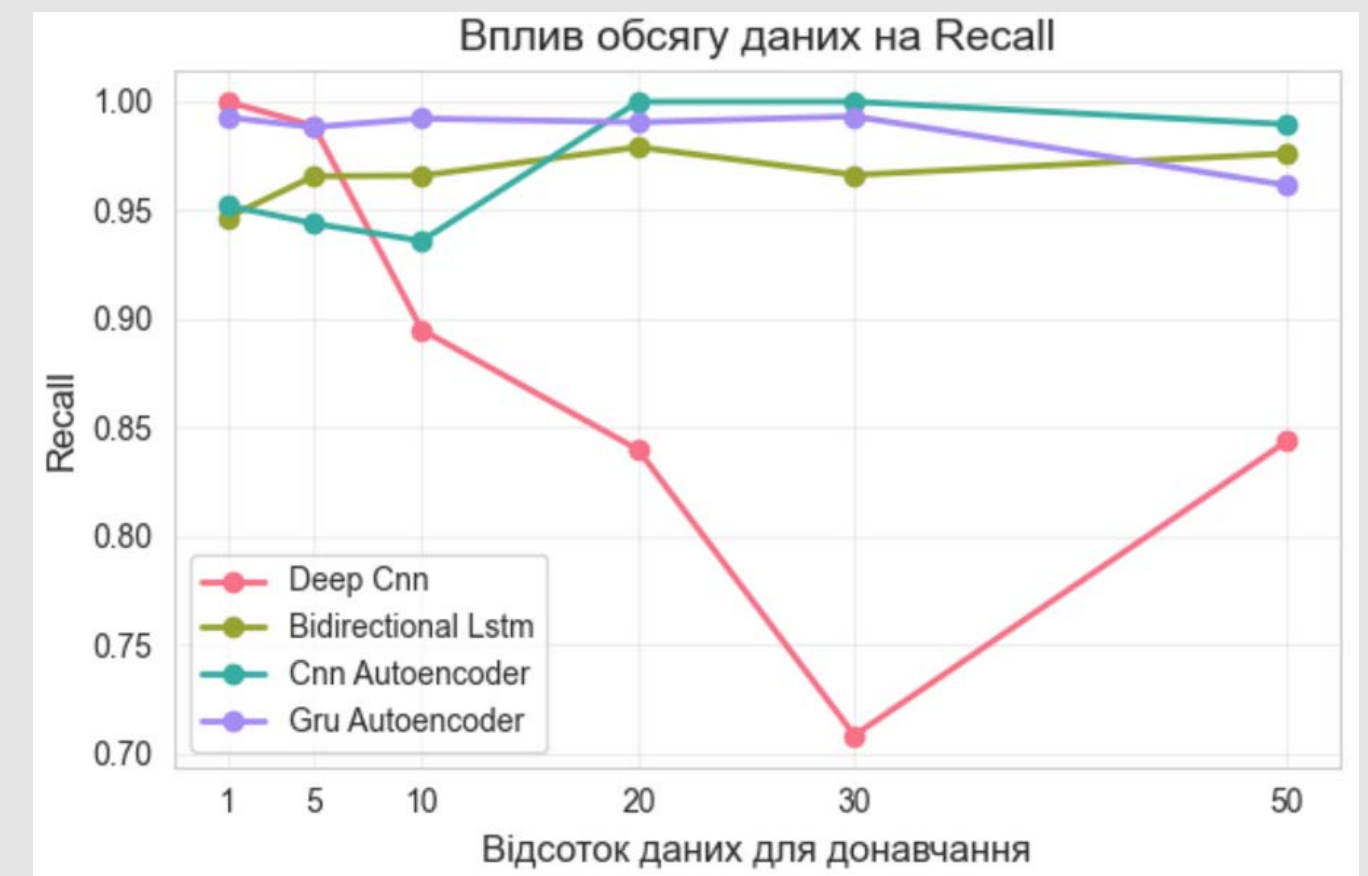
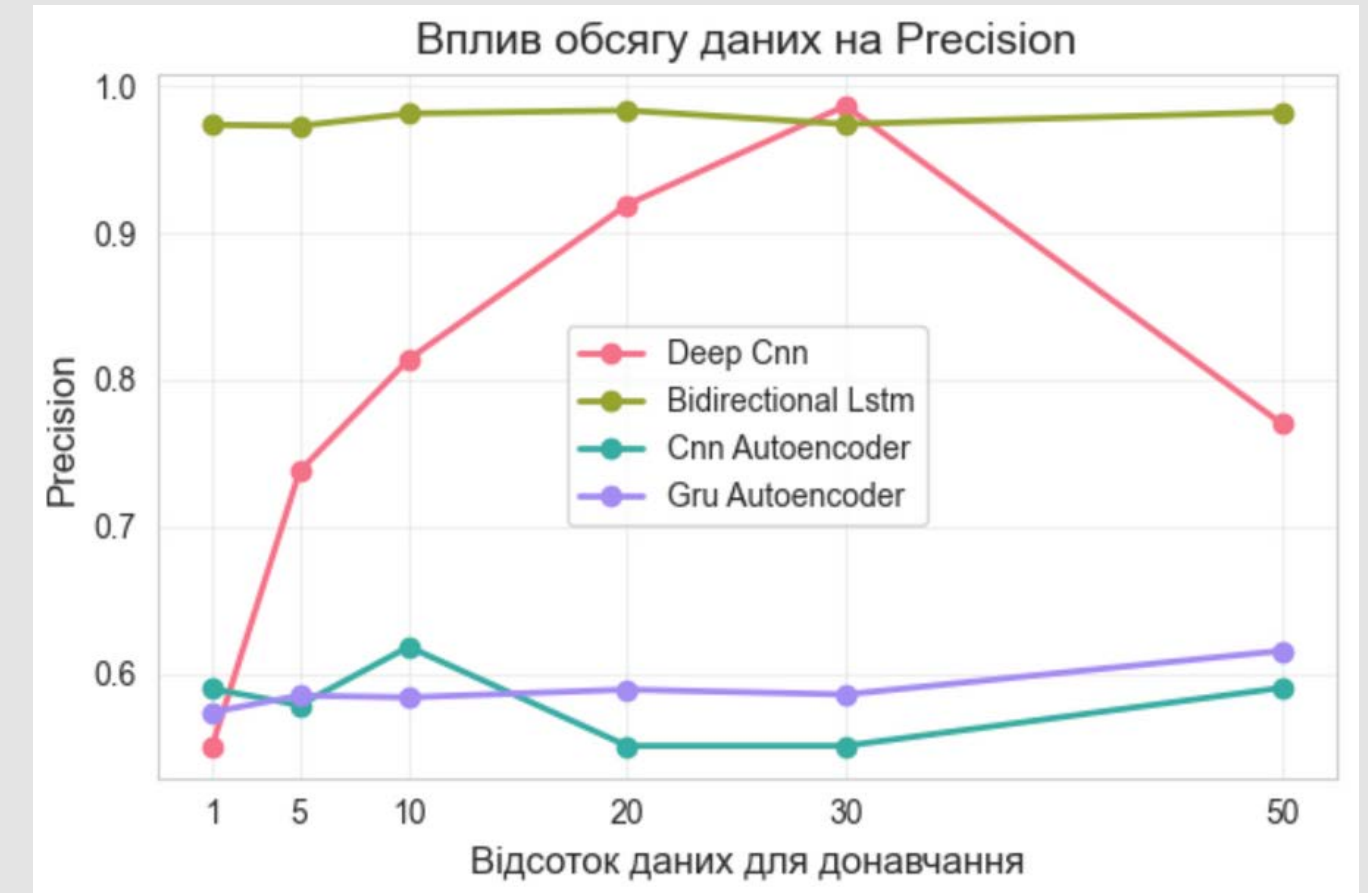
## Deep CNN

- Сильна залежність від обсягу даних:
  - Різкий приріст F1 з 0.7102 (1%) до 0.8449 (5%).
  - Погіршення після 20% — ймовірно перенавчання.



## Autoencoders

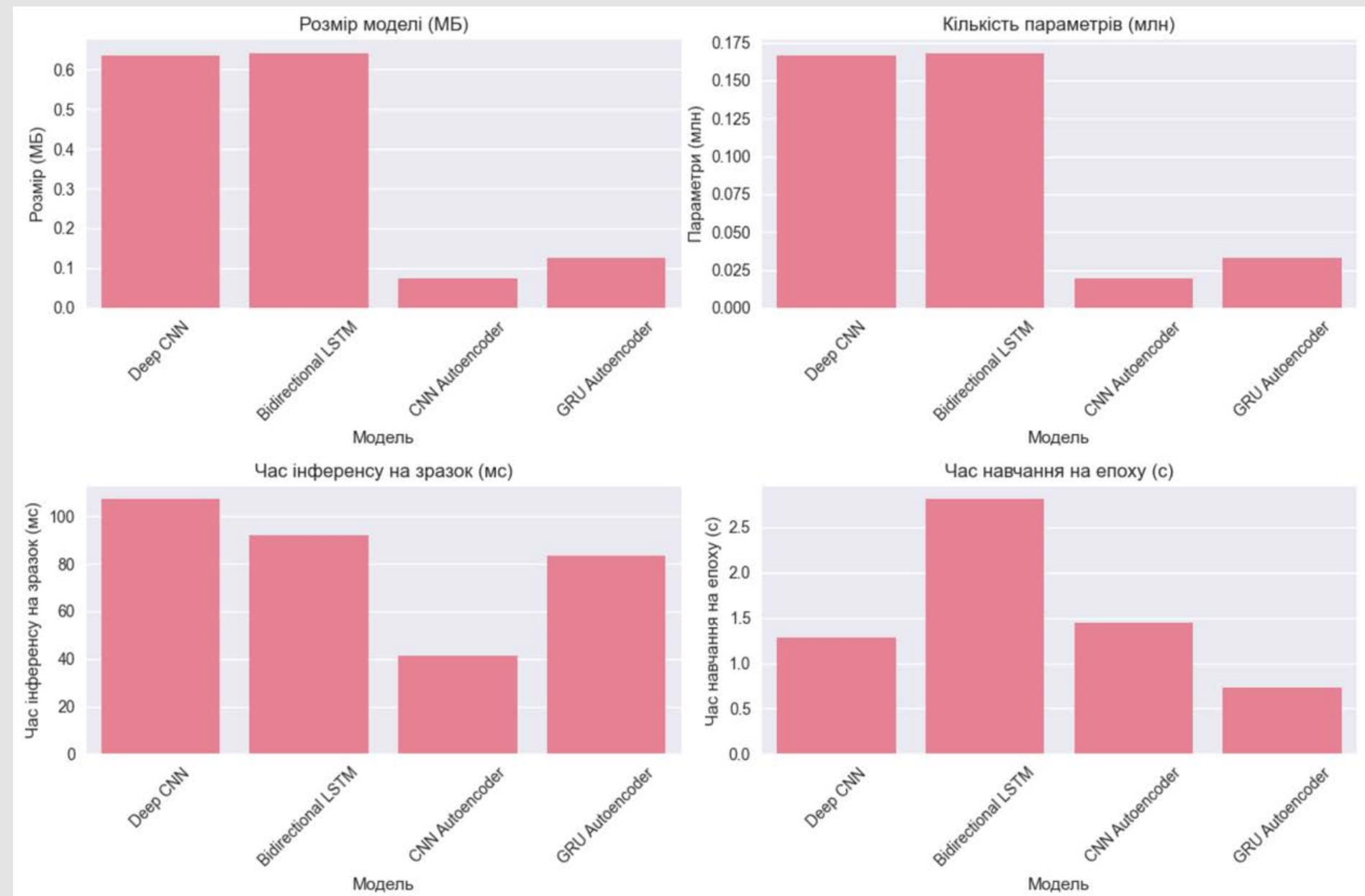
- Обмежене покращення при донавчанні:
  - GRU AE: F1 від 0.7271 до 0.7504.
  - CNN AE: F1 від 0.7281 до 0.7445.
- Високий recall ( $>0.93$ ), але низька precision ( $\sim 0.55-0.62$ ).



Баланс між точністю виявлення та обчислювальними вимогами визначає придатність архітектури для реальних систем.

## Метрики:

- розмір моделі
- швидкість обробки
- швидкість навчання
- баланс точність/ефективність





### Найшвидша: Autoencoder

- Мінімальний розмір, найшвидше навчання та інференс
- Але – посередня точність при зміні середовища



### Найбільш надійна: Bidirectional LSTM

- Висока точність, помірний розмір
- Повільна пакетна обробка та довге навчання



### Оптимальна для реального часу: Deep CNN

- Найшвидша обробка пакетів, стабільна адаптація

## Характер аномалій

**Точкові:** Автоенкодери

**Контекстуальні:** LSTM

**Колективні:** CNN + LSTM

## Доступність міток

**Є розмічені дані:** Класифікаційні моделі

**Немає міток:** Автоенкодери

## Стабільність середовища

- **Стабільні:** Autoencoder (GRU AE - F1=98.5%)
- **Динамічні:** LSTM (адаптація при 1% донавчання — F1=95.99%)

## Критичність хибних спрацювань

**Пріоритет мінімізувати пропуски:** Autoencoder

**Критично мінімізувати хибні спрацювання:** CNN

## CNN

- Глибші архітектури → краще виявлення
- Залишкові зв'язки не дають покращення на мережевих даних

## RNN

- Bidirectional LSTM – найкращі результати серед RNN
- GRU - виявляє найбільше аномалій, але більше false positives
- Механізм уваги неефективний

## Autoencoder

- GRU AE → найвища точність
- CNN AE → менше точність, але краща швидкодія

## Попередня обробка 0 1

Модулі збору даних, фільтрації шуму, екстракції ознак та нормалізації.

---

## Адаптація 0 2

**Класифікаційні моделі:** донавчання на невеликих обсягах даних

**Автоенкодери:** не піддаються адаптації

## Виявлення 03

Застосування даних мережі на попередньо навченій моделі або ансамблі моделей.



## Реагування 04

Модулі агрегації та кореляції виявлених аномалій, пріоритизації, генерації сповіщень та звітів.

- Проведено **комплексне дослідження** систем виявлення аномалій на основі нейронних мереж, із фокусом на мережевий трафік.
- Поєднано **теоретичний аналіз** із **практичним експериментом**, у якому порівнювалися різні типи моделей.
- Досліджено **можливості трансферного навчання**, що дозволило оцінити адаптивність моделей до нових мережевих середовищ, а також їхню обчислювальну ефективність.

Розробка гібридних  
моделей

Методи покращення  
адаптації моделей

Підвищення  
інтерпретованості

Тестування у  
реальних умовах

Д Д Я К У Ю  
З А У В А Г У