JEL Classification: G21; D81

Примостка Людмила Олександрівна
д.е.н., професор, завідувачка кафедри банківської справи та страхування
Київського національного економічного університету
імені Вадима Гетьмана
м. Київ, Україна
Лавренюк Владислав Володимирович
к.е.н., доцент, доцент кафедри банківської справи та страхування
Київського національного економічного університету
імені Вадима Гетьмана
м. Київ, Україна

РИЗИКИ ВИКОРИСТАННЯ ТЕХНОЛОГІЙ ШТУЧНОГО ІНТЕЛЕКТУ У БАНКІВСЬКІЙ ДІЯЛЬНОСТІ

Технології штучного інтелекту мають значний потенціал для трансформації суспільства та життя людей - від торгівлі та охорони здоров'я до транспорту, кібербезпеки та навколишнього середовища. Акцентовано, що штучний інтелект сприяє інклюзивному економічному зростанню та сталому розвитку. Виявлено, що технології штучного інтелекту також створюють ризики, які можуть негативно вплинути на суспільство, навколишнє середовище та фінансову систему, в тому числі й на банківський сектор.

Ключові слова: *банк, банківські ризики, фінтех, штучний інтелект.*

Штучний інтелект (англ. *Artificial intelligence*) швидко трансформує банківську діяльність, перебираючи на себе частину функцій щодо оптимізації витрат і операційної ефективності. Штучний інтелект (ШІ) допомагає як ризик-менеджерам, так і фінансовим органам приймати базові управлінські рішення в частині своїх компетенцій. Відповідно до міжнародної практики використання технологій ШІ у банківській діяльності зустрічається на двох основних рівнях: 1) мікроекономічний (використання ШІ на рівні окремого банку чи банківської групи); 2) макроекономічний або регуляторний (використання ШІ центральними банками, наприклад Банком Англії) [1; 2]. Зокрема, до найбільш поширених напрямів використання технологій штучного інтелекту у банківській діяльності віднесемо: використання чат-ботів на основі ШІ (наприклад ChatGPT), виявлення та протидія шахрайству (виявлення аномальних операцій, ідентифікація моделей шахрайства), менеджмент відносин з клієнтами (персоналізація послуг банків 24/7, аналіз патернів поведінки), прогностична аналітика (машинне навчання, прогнозування показників діяльності), управління кредитними ризиками (оцінка ймовірності дефолту позичальника, оптимізація резервів).

Водночас, ШІ може дестабілізувати банківську діяльність на будь-якому рівні (макро та/чи мікро), створюючи нові додаткові ризики та посилюючи вже існуючі. Науковці наголошують на потенційній шкоді від використання ШІ, адже це в свою чергу породжує конкретні види ризиків для діяльності банків та

інших фінансових установ: 1) для фінансових установ, включаючи банки: ризики бізнес-процесів (кредитні, ліквідності, ринкові), ризики кібербезпеки, операційні ризики (в т.ч. модельний ризик), репутаційні ризики; 2) для фінансової екосистеми: системні ризики.

Ризики, пов'язані із використанням технологій ШІ на рівні окремого банку, у більшості випадків є менш катастрофічними та краще керованими. Варто наголосити, що йдеться про банки, які не мають статусу системно важливих, тобто для їхньої діяльності характерні екзогенні ризики. Екзогенний ризик можна оцінити статистичними методами, будь то традиційні моделі ризику чи машинне навчання. Для таких цілей технології ШІ є дуже ефективними, а ризик збоїв у алгоритмах досить низький, однак все ж потребує відповідного контролю. Складніша ситуація з використанням технологій ШІ банками зі статусом системно важливих. Для таких банків характерний ендогенний ризик, тобто «кожен, хто взаємодіє з системою, змінює її» [2]. За таких умов, ризик збоїв у алгоритмах ШІ при прийнятті управлінських рішень може призвести не тільки до порушень функціонування системно важливого банку, а й до порушення фінансової стабільності банківської системи.

Приймаючи рішення, наприклад, щодо оцінки кредитоспроможності позичальника, виявлення шахрайських операцій чи консультування клієнтів щодо продуктів/послуг банку ШІ може припускатися помилок. Систематичні помилки призводять до алгоритмічної упередженості, тобто ШІ перенавчаючись, може зміщувати результат у гірший бік. Постає питання відповідальності за такі помилки для персоналу, що використовує відповідні алгоритми та/чи розробників ШІ. У будь-якому випадку це викликає реалізацію низки банківських ризиків (кредитного, ліквідності, репутаційного, ринкового), що негативно відображується на фінансовій та репутаційній стійкості банку. Такі проблеми часто пов'язують із недостатньою валідністю даних, на яких навчається алгоритм, та можливими «вродженими» помилками у процесі навчання (ШІ невірно розуміє цілі).

З іншого боку, надання банківської інформації для навчання алгоритмів ШІ супроводжується ризиками витоку чи неправомірного використання інформації (наприклад інформація про позичальників). Так, найбільші фінансові установи світу (Bank of America, Citigroup, Deutsche Bank, Goldman Sachs Group, Wells Fargo, JPMorgan Chase) заборонили своїм співробітникам використовувати нейромережу ChatGPT від OpenAI для будь-яких пов'язаних з роботою завдань через те, що подібні системи часто видають неактуальну або помилкову інформацію. У контексті українського законодавства такі збої у роботі ШІ банків класифікуються як операційний ризик, однак, зважаючи на широку специфіку таких ризиків, вважаємо це не зовсім вірним підходом. Також, технології ШІ несуть ризик і для ринку праці банківських працівників, оскільки ШІ вже зараз може замінити низку рутинних процесів, які донедавна виконували співробітники банків.

Коли йдеться про регуляторний рівень використання ШІ, більшість дослідників вважають, що найбільш ймовірним негативним сценарієм є генерація системного ризику. Вважається, що ШІ при вирішенні макроцілей

регулятора може стикнутися із проблемою доступності необхідних даних, що може викликати негативні системні наслідки. Проблема полягає у тому, що наявні регуляторні дані дещо обмежені, оскільки генеруються в межах регуляторної політики у певний момент часу. Оскільки банки і регулятор, як правило, приймають рішення на основі ретроспективних подій, то трансформують цим власну екосистему, і як наслідок, знову ж адаптуються до змін, що є прямим наслідком застосування «критики Лукаса» [3]. Варто зазначити, що не всі банки є добросовісними у власній діяльності, що може викликати спотворення результатів роботи ШІ. Тобто, ґрунтуючись на історичних даних, використовуючи традиційні методи машинного навчання і не маючи розуміння причинно-наслідкових взаємозв'язків та політик регулятора, ШІ може запропонувати невірні рішення, які призведуть до нарощування системного ризику. Перед будь-яким штучним інтелектом мають бути поставлені чіткі цілі, що важко зробити, якщо вирішення макропроблеми проводиться без чіткого формулювання мети та стратегії її досягнення. З іншого боку, будь-яка фіксована мета за своєю суттю є вразливою до сценарію «невідоме невідомих» (англ. *unknown-unknowns*). Штучний інтелект з фіксованими цілями, який функціонує у складному середовищі, матиме неочікувану поведінку [4]. Такі концептуальні проблеми породжують багато практичних викликів, з якими стикаються ті, хто хоче використовувати ШІ у регулюванні банківської діяльності.

Проведений аналіз дозволив виокремити три концептуальні проблеми ШІ у банківській діяльності, які є потенційними тригерами для різноманітних ризиків, в тому числі системного: 1) реакція банків на запропоновані заходи ШІ; 2) необхідні для навчання алгоритмів ШІ дані; 3) виявлення «невідомого невідомих» при роботі алгоритмів ШІ. Наразі вирішити цю проблему можливо за допомогою: 1) модульних організаційних структур з формальними та неформальними каналами комунікації; 2) проведенням стратегічних ігор з прийняття рішень (симуляції реальних подій) для навчання ШІ; 3) відбором персоналу на основі освіти, досвіду та результатів роботи. На даний час не вирішеним залишається завдання, як відтворити такі децентралізовані механізми прийняття рішень при розробці ШІ для банківської системи, однак це є перспективою подальших наукових досліджень.

Список використаних джерел:

1. Tabassi E. AI Risk Management Framework. Gaithersburg, MD: National Institute of Standards and Technology, 2023. DOI: 10.6028/nist.ai.100-1
2. Daníelsson J., Macrae R., Uthemann A. Artificial intelligence and systemic risk. *Journal of Banking & Finance*. 2021. P. 106290. URL: DOI: 10.1016/j.jbankfin.2021.106290
3. Lucas R. E. Econometric policy evaluation: A critique. *Carnegie-Rochester Conference Series on Public Policy*. 1976. Vol. 1. P. 19-46. DOI: 10.1016/s0167-2231(76)80003-6
4. Russell S. J. Human Compatible: Artificial Intelligence and the Problem of Control. Penguin Books, 2020. 352 p.