

АІ-РИЗИКИ У БАНКІВСЬКІЙ ДІЯЛЬНОСТІ ТА ПІДХОДИ ДО ЇХ ОЦІНЮВАННЯ

ХОДАКЕВИЧ Сергій¹, ГЛАДИШЕНКО Микола², ХОДАКЕВИЧ Богдан³

¹ Київський національний економічний університет імені Вадима Гетьмана

<https://orcid.org/0000-0002-8951-2605>

e-mail: khs@kneu.edu.ua

² Київський національний економічний університет імені Вадима Гетьмана

<https://orcid.org/0009-0001-6917-045X>

e-mail: kg757600@gmail.com

³ Київський національний економічний університет імені Вадима Гетьмана

<https://orcid.org/0009-0003-4081-0542>

e-mail: bogdankhodakevych@gmail.com

У статті систематизовано ризики, що виникають у процесі впровадження технологій штучного інтелекту (АІ) у банківську діяльність, та обґрунтовано методичні підходи до їх оцінювання. Уточнено зміст поняття «АІ-ризик у банківській діяльності», запропоновано класифікацію АІ-ризиків (модельні, даних, кібербезпекові, операційні, етичні та регуляторні) й окреслено їх місце в загальній системі ризиків банку. На основі узагальнення міжнародних стандартів і наукових праць розроблено інтегровану методичку оцінювання АІ-ризиків, що поєднує кількісні (матриці «ймовірність-вплив»), ключові індикатори ризику, стрес-тестування та якісні (алгоритмічний аудит, оцінка упередженості, зрозумілий АІ, управління модельним ризиком) інструменти. Показано, що ефективне управління АІ-ризиками потребує інституціоналізації управління модельним ризиком, розвитку політик управління даними та адаптації регуляторних вимог до специфіки АІ у банківському секторі.

Ключові слова: штучний інтелект, банківська діяльність, АІ-ризик, модельний ризик, ризик даних, кіберризик, алгоритмічна упередженість, управління ризиками.

<https://doi.org/10.31891/mdes/2025-18-8>

Стаття надійшла до редакції / Received 20.09.2025

Прийнята до друку / Accepted 26.10.2025

ПОСТАНОВКА ПРОБЛЕМИ У ЗАГАЛЬНОМУ ВИГЛЯДІ ТА ЇЇ ЗВ'ЯЗОК ІЗ ВАЖЛИВИМИ НАУКОВИМИ ЧИ ПРАКТИЧНИМИ ЗАВДАННЯМИ

Цифрова трансформація фінансової системи супроводжується інтенсивним впровадженням технологій штучного інтелекту у ключові бізнес-процеси банків: кредитний скоринг, комплаєнс, управління ризиками, протидію шахрайству, персоналізацію продуктів та автоматизацію обслуговування клієнтів [13]. За оцінками міжнародних консалтингових компаній, інвестиції у ШІ-рішення забезпечують суттєве підвищення операційної ефективності та доходності банків, зокрема за рахунок зниження частки проблемної заборгованості, скорочення часу обробки заявок і підвищення точності виявлення шахрайства [13; 17; 18].

Разом із тим широке використання АІ породжує комплекс нових ризиків, пов'язаних із складністю моделей, залежністю від якості даних, кіберзагрозами, недостатньою прозорістю алгоритмів та можливістю алгоритмічної дискримінації [10; 15]. Реалізація таких ризиків здатна призвести не лише до фінансових втрат, а й до порушення прав клієнтів, регуляторних санкцій та суттєвого зниження довіри до банківських установ [4; 5; 6].

На практичному рівні перед банками постає завдання інтеграції АІ-ризиків у загальну систему ризик-менеджменту, розроблення спеціальних політик управління модельним ризиком і ризиками даних, а також забезпечення відповідності національному та наднаціональному регулюванню, включно з вимогами щодо захисту персональних даних і використання високоризикових АІ-систем [1–3; 5; 6]. Наукова проблема полягає у теоретичному обґрунтуванні змісту АІ-ризиків у банківській діяльності, їх систематизації та розробленні комплексних методичних підходів до їх оцінювання.

АНАЛІЗ ОСТАННІХ ДОСЛІДЖЕНЬ І ПУБЛІКАЦІЙ; ВИДІЛЕННЯ НЕВИРІШЕНИХ ЧАСТИН ЗАГАЛЬНОЇ ПРОБЛЕМИ

Питання цифрової трансформації банківського сектору, розвитку фінансових технологій та фінтех-екосистеми відображені у роботах вітчизняних і зарубіжних дослідників, які аналізують вплив FinTech на структуру фінансового ринку, моделі взаємодії банків із клієнтами та регуляторні виклики [16; 20; 21]. Дослідження зосереджуються на еволюції фінансових технологій, класифікації FinTech-рішень, а також на зміні бізнес-моделей банків під впливом цифрових інновацій [16; 21].

Окрема група праць присвячена застосуванню штучного інтелекту у фінансах: розглядаються питання використання машинного навчання для кредитного скорингу, управління ризиками, виявлення шахрайства, а також оцінюється вплив AI на продуктивність і фінансову інклюзивність [11; 12; 13; 17]. У роботах аналізується зростання точності моделей, можливості використання альтернативних джерел даних, розвиток поведінкових і біометричних підходів [36; 39; 41; 45].

Міжнародні організації (Базельський комітет, Рада з фінансової стабільності, ОЕСР, Європейська банківська влада) сформували низку принципів і рекомендацій щодо управління операційними, кібер- та модельними ризиками, що охоплюють також використання AI-технологій у фінансовому секторі [4; 9]. На рівні ЄС ухвалено регуляторні акти, які встановлюють правила обробки персональних даних (GDPR) та гармонізовані вимоги до високоризикових AI-систем, включно з фінансовими послугами [4; 5].

При цьому, на наш погляд, в науковій літературі та практичних документах переважає фрагментарний розгляд окремих компонентів AI-ризиків: модельного ризику, ризику даних, кіберризiku або алгоритмічної упередженості [7; 10; 15; 19]. Недостатньо розробленими залишаються:

- узгоджене визначення та системна класифікація AI-ризиків у банківській діяльності;
- інтегрований підхід до їх оцінювання, який поєднував би класичні інструменти ризик-менеджменту з специфікою AI-систем [6; 7];
- адаптація міжнародних стандартів до умов банківських систем країн із ринками, що розвиваються, з урахуванням ресурсних обмежень та стану інституційного середовища.

Зазначені прогалини зумовлюють необхідність подальшої розробки теоретичних та методичних підходів до систематизації та оцінювання AI-ризиків у банківській діяльності.

ФОРМУЛЮВАННЯ ЦІЛЕЙ СТАТТІ

Метою статті є систематизація AI-ризиків у банківській діяльності та обґрунтування інтегрованих методичних підходів до їх оцінювання з урахуванням сучасних міжнародних стандартів і практики застосування AI у банківському секторі.

Для досягнення поставленої мети необхідно розв'язати наступні завдання:

1. Уточнити зміст поняття «AI-ризик у банківській діяльності» та визначити їх місце в системі ризиків банку.
2. Узагальнити підходи до управління AI-ризиками, відображені в наукових дослідженнях і регуляторних документах.
3. Запропонувати класифікацію AI-ризиків, релевантну для банківських установ.
4. Розробити інтегровану методику оцінювання AI-ризиків, що поєднує кількісні та якісні інструменти аналізу.
5. Окреслити напрями удосконалення системи управління AI-ризиками у банківських установах.

ВИКЛАД ОСНОВНОГО МАТЕРІАЛУ

1. Теоретичні засади AI-ризиків у банківській діяльності. У банківському секторі штучний інтелект розглядається як сукупність алгоритмів і моделей, здатних виконувати завдання класифікації, прогнозування, оптимізації, обробки природної мови та розпізнавання образів, що традиційно вимагали людського інтелекту [13; 16]. На практиці це реалізується через моделі машинного навчання, глибокого навчання, методи NLP, комп'ютерного зору, генеративні моделі та системи рекомендацій [14].

Сьогодні в банках AI-системи інтегруються в процеси кредитного скорингу, виявлення шахрайства, моніторингу транзакцій, управління ліквідністю та маркетингових комунікацій [17]. Відтак помилки моделей, спотворення даних чи технічні збої можуть мати істотний вплив на кредитний портфель, рівень операційних витрат, дотримання регуляторних вимог та репутацію банківської установи [10].

У цьому контексті доцільно трактувати AI-ризик у банківській діяльності як сукупність ризиків, що пов'язані з розробкою, впровадженням та функціонуванням AI-систем у банку і реалізація яких може спричинити фінансові, операційні, регуляторні та репутаційні втрати, а також порушення прав та інтересів клієнтів [6; 7].

2. Класифікація AI-ризиків у банківській діяльності. На основі узагальнення наукових підходів та рекомендацій регуляторів [4; 6; 9; 10] AI-ризиків, на наш погляд, доцільно класифікувати на такі основні групи:

1. Модельні ризики. Пов'язані з помилками у специфікації, тренуванні та валідації моделей, їх деградацією у часі, некоректним використанням. Для AI-моделей характерними є ризики перенавчання, зміна даних (коли якість передбачення моделі змінюється під впливом статистичних властивостей вхідних даних), зміна концепту (зміна у відносинах між вхідними даними та тим, що намагаємося передбачити), нестійкості до змін середовища та залежності від обмежених або нерепрезентативних вибірок [10; 14; 15].

2. Ризики даних. Охоплюють низьку якість, неповноту, несвоєчасність, неузгодженість даних, а також їх історичну та інші упередженості. Вказані проблеми можуть призводити до хибних рішень моделей, алгоритмічної дискримінації та порушення вимог до обробки персональних даних [5; 14; 15].

3. Кібербезпекові ризики AI-систем. Стосуються можливості спеціалізованих атак, компрометації моделей і несанкціонованого доступу до тренувальних даних, що створює загрозу як для фінансової стійкості, так і для інформаційної безпеки [5; 10].

4. Операційні ризики. Виникають у процесі інтеграції AI-рішень у бізнес-процеси: технічні збої, несумісність IT-інфраструктури, залежність від зовнішніх постачальників, дефіцит кваліфікованого персоналу, помилки в експлуатації систем.

5. Етичні ризики та алгоритмічна упередженість. Пов'язані з непрозорістю рішень, можливістю дискримінації певних груп клієнтів, порушенням принципів справедливості, недискримінації та поваги до приватності [4; 11; 17; 19].

6. Регуляторні та комплаєнс-ризики. Зумовлені невідповідністю AI-рішень чинному банківському регулюванню, вимогам до захисту персональних даних та новим нормам щодо високоризикових AI-систем (у т.ч. AI Act ЄС) [1-5; 9].

Запропонована класифікація дозволяє узгодити AI-ризиків із традиційними категоріями ризиків банку (кредитний, операційний, комплаєнс-ризик, репутаційний ризик, ризик фінансової стійкості) та створює основу для побудови єдиного профілю ризику, що включає інтелектуальні системи.

3. Методичні підходи до оцінювання AI-ризиків. Методологічні основи оцінювання AI-ризиків передбачають адаптацію класичного ризик-орієнтованого підходу до специфіки інтелектуальних систем [6; 7]. Виходячи з рекомендацій Базельського комітету та практики банківських установ, доцільно виділити блоки кількісних і якісних інструментів.

3.1. Кількісні інструменти оцінювання:

1. Матриця «ймовірність–вплив». Для кожного виду AI-ризиків визначаються ймовірність реалізації та очікуваний вплив на ключові показники (капітал, прибуток, рівень дефолтів, безперервність операцій, репутацію). На основі матриці формується карта ризиків, що дозволяє ранжувати їх за критичністю [6].

2. Ключові індикатори ризику (KRI). Для модельних ризиків такими індикаторами можуть бути частка моделей із простроченим оновленням, відхилення фактичних втрат від прогнозованих, частка ручних відмін-рішень; для ризиків даних – частота інцидентів неякісних або неповних даних; для кіберризиків – кількість інцидентів безпеки AI-систем, спроб несанкціонованого доступу [6; 7; 10].

3. Сценарний аналіз і стрес-тестування. Оцінювання наслідків реалізації сценаріїв відмови ключових AI-систем (скоринг, AML-моніторинг), масової деградації моделей або порушення цілісності даних дозволяє оцінити вплив AI-ризиків на капітал, ліквідність та дотримання нормативів [6; 10; 17].

4. Метрики якості моделей. Використання ML-метрик (AUC (Area Under the ROC Curve), коефіцієнт Джині, точність, чутливість), показників стабільності (дані, зміна концепту) забезпечує кількісне представлення модельного ризику та дає змогу контролювати деградацію моделей у часі [4; 17].

3.2. Якісні інструменти оцінювання:

1. Алгоритмічний аудит. Передбачає незалежну оцінку AI-систем щодо відповідності внутрішнім політикам банку, регуляторним вимогам, етичним принципам та стандартам управління модельним ризиком [4; 6; 7].

2. Оцінка алгоритмічної упередженості. Здійснюється шляхом аналізу результатів моделей для різних груп клієнтів, виявлення систематичних відмінностей у рішеннях за відсутності економічного обґрунтування таких розбіжностей [11; 15; 19].

3. Зрозумілий AI. Використання підходів, що забезпечують пояснюваність рішень моделей (важливість ознак, локальні та контрфактичні пояснення, інтерактивні інструменти) сприяє зниженню етичних та регуляторних ризиків і полегшує зовнішній та внутрішній нагляд [4; 14; 15].

4. Управління модельним ризиком. Формування окремого фреймворку управління модельним ризиком, що включає реєстр моделей, їх класифікацію за критичністю, формалізовані процедури розробки, валідації, моніторингу й виведення з експлуатації, є ключовою передумовою контролю AI-ризиків [6;7].

4. Інтегрована методика оцінювання AI-ризиків у банку. На основі узагальнення викладених інструментів можна обґрунтувати інтегровану методику оцінювання AI-ризиків, яка включає послідовні етапи [4; 6; 7; 10; 18]:

1. Ідентифікація AI-систем. Формування повного переліку AI-рішень банку, опис їх функцій, каналів впливу на показники діяльності та клієнтів.

2. Класифікація ризиків. Віднесення ризиків кожної AI-системи до виділених груп (модельні, даних, кібербезпекові, операційні, етичні, регуляторні).

3. Якісна оцінка. Експертне ранжування ризиків за критеріями «ймовірність–вплив» із побудовою карти ризиків, визначенням критичних зон і пріоритетів реагування.

4. Кількісна оцінка. Визначення та моніторинг KRI, застосування метрик якості моделей, аналіз історії інцидентів, проведення сценарного аналізу й стрес-тестування для найбільш критичних AI-застосувань.

5. Планування заходів мітингації. Розроблення технічних і організаційних заходів (регулярний retraining моделей, резервні процеси прийняття рішень, dual control для високоризикових рішень, підсилення заходів кібербезпеки тощо).

6. Моніторинг та перегляд. Регулярний перегляд оцінок ризиків, оновлення карти ризиків, періодичні алгоритмічні аудити, коригування політик і процедур управління AI-ризиками з урахуванням змін регуляторного середовища та технологічного розвитку.

Таким чином, вважаємо, що зазначена методика узгоджується з принципами управління операційними та модельними ризиками Базельського комітету та може бути інтегрована у загальну систему ризик-менеджменту банку [6; 9].

ВИСНОВКИ З ДАНОГО ДОСЛІДЖЕННЯ І ПЕРСПЕКТИВИ ПОДАЛЬШИХ РОЗВІДК У ДАНОМУ НАПРЯМІ

У статті уточнено зміст категорії «AI-ризик у банківській діяльності» та запропоновано їх розуміння як сукупності ризиків, пов'язаних із життєвим циклом AI-систем у банку, реалізація яких може суттєво впливати на фінансову стійкість, регуляторну відповідність і репутацію банківської установи [6; 7].

На основі аналізу наукових джерел і регуляторних документів узагальнено підходи до управління AI-ризиками та виділено шість основних груп AI-ризиків (модельні, даних, кібербезпекові, операційні, етичні та регуляторні), що забезпечує цілісний підхід до формування профілю ризику AI-рішень [4; 10].

Таким чином сформовано інтегровану методику оцінювання AI-ризиків, яка поєднує кількісні (матриці «ймовірність–вплив», ключові індикатори ризику, стрес-тестування, ML-метрики) та якісні (алгоритмічний аудит, зрозумілий AI, управління модельним ризиком) інструменти. Запропонований підхід дозволяє системно ідентифікувати та ранжувати ризики, визначати пріоритетні заходи їх зменшення та інтегрувати AI-ризик в загальну систему ризик-менеджменту банку.

Вважаємо, що перспективними напрямками подальших наукових розвідок є:

- розроблення кількісних моделей оцінки впливу реалізації AI-ризиків на капітал і ліквідність банків з використанням сценарного та імітаційного моделювання;
- емпіричний аналіз фактичних інцидентів, пов'язаних із AI у фінансовому секторі, та оцінка їх довгострокового впливу на ринкову позицію банків;
- адаптація міжнародних стандартів управління AI-ризиками до умов національних фінансових систем, зокрема щодо регуляторних вимог, організаційних структур управління та ресурсних обмежень.

ЛІТЕРАТУРА:

1. Про банки і банківську діяльність : Закон України від 07.12.2000 № 2121-III. URL: <https://zakon.rada.gov.ua/laws/show/2121-14> (дата звернення: 15.03.2025).
2. Про захист персональних даних : Закон України від 01.06.2010 № 2297-VI. URL: <https://zakon.rada.gov.ua/laws/show/2297-17> (дата звернення: 15.03.2025).
3. Про платіжні послуги : Закон України від 30.06.2021 № 1591-IX. URL: <https://zakon.rada.gov.ua/laws/show/1591-20> (дата звернення: 18.03.2025).
4. Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act). Official Journal of the European Union. 2024. L, 2024/1689. URL: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32024R1689> (дата звернення: 10.04.2025).
5. Regulation (EU) 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data (General Data Protection Regulation). Official Journal of the European Union. 2016. URL: <https://eur-lex.europa.eu/eli/reg/2016/679/oj> (дата звернення: 10.04.2025).
6. Basel Committee on Banking Supervision. Principles for the sound management of operational risk. Bank for International Settlements. 2011. URL: <https://www.bis.org/publ/bcbs195.pdf> (дата звернення: 15.04.2025).
7. Basel Committee on Banking Supervision. Principles for operational resilience. Bank for International Settlements. 2021. URL: <https://www.bis.org/bcbs/publ/d516.pdf> (дата звернення: 15.04.2025).
8. Financial Stability Board. Artificial intelligence and machine learning in financial services. 2017. URL: <https://www.fsb.org/2017/11/artificial-intelligence-and-machine-learning-in-financial-services/> (дата звернення: 18.04.2025).
9. OECD. Artificial Intelligence in Society. Paris : OECD Publishing, 2019. 150 p. DOI: <https://doi.org/10.1787/eedfee77-en>
10. https://www.oecd.org/content/dam/oecd/en/publications/reports/2019/06/artificial-intelligence-in-society_c0054fa1/eedfee77-en.pdf
11. Baryannis G., Validi S., Dani S., Antoniou G. Supply chain risk management and artificial intelligence: state of the art and future research directions. International Journal of Production Research. 2019. Vol. 57. № 7. P. 2179-2202. DOI: <https://doi.org/10.1080/00207543.2018.1530476>
12. Buchanan B. G. Artificial intelligence in finance. The Alan Turing Institute, 2019. 40 p. URL: https://www.turing.ac.uk/sites/default/files/2019-04/artificial_intelligence_in_finance_ati.pdf (дата звернення: 22.04.2025).
13. Carbó-Valverde S., Cuadros-Solas P. J., Rodríguez-Fernández F. A machine learning approach to the digitalization of bank customers: Evidence from random and causal forests. PLoS ONE. 2020. Vol. 15. № 10. DOI: <https://doi.org/10.1371/journal.pone.0240362>
14. Davenport T. H., Ronanki R. Artificial intelligence for the real world. Harvard Business Review. 2018. Vol. 96. № 1. P. 108-116. <https://hbr.org/webinar/2018/02/artificial-intelligence-for-the-real-world>
15. Duan Y., Edwards J. S., Dwivedi Y. K. Artificial intelligence for decision making in the era of Big Data: evolution, challenges and research agenda. International Journal of Information Management. 2019. Vol. 48. P. 63-71. DOI: <https://doi.org/10.1016/j.ijinfomgt.2019.01.021>
16. Feuerriegel S., Dolata M., Schwabe G. Fair AI: Challenges and opportunities. Business & Information Systems Engineering. 2020. Vol. 62. P. 379-384. DOI: 10.1007/s12599-020-00650-3. <https://link.springer.com/article/10.1007/s12599-020-00650-3>
17. Gai K., Qiu M., Sun X. A survey on FinTech. Journal of Network and Computer Applications. 2018. Vol. 103. P. 262-273. DOI: <https://doi.org/10.1016/j.jnca.2017.10.011>
18. Leo M., Sharma S., Maddulety K. Machine Learning in Banking Risk Management: A Literature Review. Risks. 2019. Vol. 7. № 1. Article 29. DOI: <https://doi.org/10.3390/risks7010029>
19. McKinsey & Company. The State of AI in 2024: Generative AI's breakout year. 2024. URL: <https://www.mckinsey.com/capabilities/quantumblack/our-insights/the-state-of-ai> (дата звернення: 02.05.2025).
20. Petropoulos G. The impact of artificial intelligence on employment. Praise for Artificial Intelligence, Automation, Economy and Society. 2018. P. 119-132.
21. World Economic Forum. The Future of Financial Services: How disruptive innovations are reshaping the way financial services are structured, provisioned and consumed. Geneva, 2015.

URL: https://www3.weforum.org/docs/WEF_The_future_of_financial_services.pdf (дата звернення: 08.05.2025).

22. Zetzsche D. A., Buckley R. P., Arner D. W., Barberis J. N. From FinTech to TechFin: The Regulatory Challenges of Data-Driven Finance. European Banking Institute Working Paper Series. 2017. № 6. 45 p. DOI: <https://doi.org/10.2139/ssrn.2959925>

REFERENCES:

1. On Banks and Banking Activities: Law of Ukraine dated 07.12.2000 No. 2121-III. URL: <https://zakon.rada.gov.ua/laws/show/2121-14> (accessed: 15.03.2025).
2. On Personal Data Protection: Law of Ukraine dated 01.06.2010 No. 2297-VI. URL: <https://zakon.rada.gov.ua/laws/show/2297-17> (accessed: 15.03.2025).
3. On Payment Services: Law of Ukraine dated 30.06.2021 No. 1591-IX. URL: <https://zakon.rada.gov.ua/laws/show/1591-20> (accessed: 18.03.2025).
4. Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act). *Official Journal of the European Union*. 2024. L, 2024/1689. URL: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32024R1689> (accessed: 10.04.2025).
5. Regulation (EU) 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data (General Data Protection Regulation). *Official Journal of the European Union*. 2016. URL: <https://eur-lex.europa.eu/eli/reg/2016/679/oj> (accessed: 10.04.2025).
6. Basel Committee on Banking Supervision. Principles for the Sound Management of Operational Risk. Bank for International Settlements. 2011. URL: <https://www.bis.org/publ/bcbis195.pdf> (accessed: 15.04.2025).
7. Basel Committee on Banking Supervision. Principles for Operational Resilience. Bank for International Settlements. 2021. URL: <https://www.bis.org/bcbis/publ/d516.pdf> (accessed: 15.04.2025).
8. Financial Stability Board. Artificial Intelligence and Machine Learning in Financial Services. 2017. URL: <https://www.fsb.org/2017/11/artificial-intelligence-and-machine-learning-in-financial-services/> (accessed: 18.04.2025).
9. OECD. Artificial Intelligence in Society. Paris: OECD Publishing, 2019. 150 p. DOI: <https://doi.org/10.1787/eedfee77-en>
10. https://www.oecd.org/content/dam/oecd/en/publications/reports/2019/06/artificial-intelligence-in-society_c0054fal/eedfee77-en.pdf
11. Baryannis G., Validi S., Dani S., Antoniou G. Supply Chain Risk Management and Artificial Intelligence: State of the Art and Future Research Directions. *International Journal of Production Research*. 2019. Vol. 57, No. 7. P. 2179–2202. DOI: <https://doi.org/10.1080/00207543.2018.1530476>
12. Buchanan B. G. Artificial Intelligence in Finance. The Alan Turing Institute, 2019. 40 p. URL: https://www.turing.ac.uk/sites/default/files/2019-04/artificial_intelligence_in_finance_-_ati.pdf (accessed: 22.04.2025).
13. Carbó-Valverde S., Cuadros-Solas P. J., Rodríguez-Fernández F. A Machine Learning Approach to the Digitalization of Bank Customers: Evidence from Random and Causal Forests. *PLoS ONE*. 2020. Vol. 15, No. 10. DOI: <https://doi.org/10.1371/journal.pone.0240362>
14. Davenport T. H., Ronanki R. Artificial Intelligence for the Real World. *Harvard Business Review*. 2018. Vol. 96, No. 1. P. 108–116. <https://hbr.org/webinar/2018/02/artificial-intelligence-for-the-real-world>
15. Duan Y., Edwards J. S., Dwivedi Y. K. Artificial Intelligence for Decision Making in the Era of Big Data: Evolution, Challenges and Research Agenda. *International Journal of Information Management*. 2019. Vol. 48. P. 63–71. DOI: <https://doi.org/10.1016/j.ijinfomgt.2019.01.021>
16. Feuerriegel S., Dolata M., Schwabe G. Fair AI: Challenges and Opportunities. *Business & Information Systems Engineering*. 2020. Vol. 62. P. 379–384. DOI: 10.1007/s12599-020-00650-3. <https://link.springer.com/article/10.1007/s12599-020-00650-3>
17. Gai K., Qiu M., Sun X. A Survey on FinTech. *Journal of Network and Computer Applications*. 2018. Vol. 103. P. 262–273. DOI: <https://doi.org/10.1016/j.jnca.2017.10.011>
18. Leo M., Sharma S., Maddulety K. Machine Learning in Banking Risk Management: A Literature Review. *Risks*. 2019. Vol. 7, No. 1. Article 29. DOI: <https://doi.org/10.3390/risks7010029>
19. McKinsey & Company. The State of AI in 2024: Generative AI's Breakout Year. 2024. URL: <https://www.mckinsey.com/capabilities/quantumblack/our-insights/the-state-of-ai> (accessed: 02.05.2025).
20. Petropoulos G. The Impact of Artificial Intelligence on Employment. In: *Artificial Intelligence, Automation, Economy and Society*. 2018. P. 119–132.
21. World Economic Forum. The Future of Financial Services: How Disruptive Innovations Are Reshaping the Way Financial Services Are Structured, Provisioned and Consumed. Geneva, 2015. URL: https://www3.weforum.org/docs/WEF_The_future_of_financial_services.pdf (accessed: 08.05.2025).
22. Zetzsche D. A., Buckley R. P., Arner D. W., Barberis J. N. From FinTech to TechFin: The Regulatory Challenges of Data-Driven Finance. *European Banking Institute Working Paper Series*. 2017. No. 6. 45 p. DOI: <https://doi.org/10.2139/ssrn.2959925>

AI RISKS IN BANKING AND APPROACHES TO THEIR ASSESSMENT

KHODAKEVYCH Serhii, HLADYSHENKO Mykola, KHODAKEVYCH Bohdan
Kyiv National Economic University named after V. Hetman

The article systematizes the risks that arise in the process of implementing artificial intelligence (AI) technologies in banking and substantiates methodological approaches to their assessment. The concept of "AI risks in banking" is clarified, a detailed classification of AI risks is proposed (model, data, cybersecurity, operational, ethical, reputational, and regulatory risks), and their place within the bank's overall risk system is outlined. Particular attention is paid to the interaction between AI-specific risks and traditional financial risks, such as credit, market, and liquidity risks, as well as to the risk of non-compliance with regulatory and supervisory requirements.

Based on a synthesis of international standards, regulatory guidelines, and academic literature, an integrated methodology for assessing AI risks is developed, combining quantitative (probability–impact matrices, key risk indicators, scenario analysis, and stress testing) and qualitative (algorithmic audit, bias and fairness assessment, explainable AI tools, model validation, and comprehensive model risk management frameworks) tools. The article emphasizes the importance of ensuring transparency and accountability of AI systems, defining clear lines of responsibility between business units, IT, and risk management divisions, and implementing continuous monitoring of AI models throughout their life cycle.

The study shows that effective AI risk management in banking requires institutionalizing model risk management functions, strengthening data governance and cybersecurity policies, enhancing staff competencies, and adapting regulatory requirements and internal policies to the specific nature, scale, and complexity of AI applications in the banking sector.

Keywords: artificial intelligence, banking, AI risks, model risk, data risks, cyber risk, algorithmic bias, risk management.