DOI: https://doi.org/10.32782/2524-0072/2026-85-193

УДК 336.71:004.83

ШТУЧНИЙ ІНТЕЛЕКТ У ФІНАНСАХ: АНАЛІЗ ПОТЕНЦІЙНИХ ЗАГРОЗ ТА ШЛЯХИ ЇХ МІНІМІЗАЦІЇ

ARTIFICIAL INTELLIGENCE IN FINANCE: ANALYSIS OF POTENTIAL THREATS AND WAYS TO MINIMIZE THEM

Малишко Євгенія Олегівна
кандидат економічних наук, доцент,
заступник директора (керівника) навчально-наукового інституту інформаційних технологій,
доцент кафедри фінансів і кредиту,
Харківський національний економічний університет імені Семена Кузнеця
ORCID: https://orcid.org/0000-0002-6691-1785

Чернишов Володимир Васильович
кандидат економічних наук, доцент,
директор навчально-наукового інституту міжнародних відносин,
доцент кафедри фінансів і кредиту,
Харківський національний економічний університет імені Семена Кузнеця
ORCID: https://orcid.org/0000-0002-8866-0075

Malyshko Yevheniia, Chernyshov Volodymyr
Simon Kuznets Kharkiv National University of Economics

У статті досліджено потенційні загрози застосування штучного інтелекту у фінансовому секторі та визначено напрями їх мінімізації. Обґрунтовано, що ШІ підвищує швидкість оброблення даних, персоналізацію фінансових послуг, якість скорингу та ефективність управління активами, однак одночасно формує нові ризики: непрозорість алгоритмічних рішень, упередженість даних, кіберзагрози, концентрацію технологічних провайдерів, юридичну невизначеність відповідальності та можливість посилення ринкової волатильності. Запропоновано комплекс запобіжних заходів, що поєднує Explainable AI, алгоритмічний аудит, human-in-the-loop, контроль якості даних, кіберстійкість, стрес-тестування моделей, регулярну перевірку якості даних і ризик-орієнтоване регулювання. Практична цінність результатів полягає у формуванні основи для безпечного впровадження ШІ у банківські та інвестиційні процеси.

Ключові слова: штучний інтелект, фінансовий сектор, ШІ-банкінг, робо-едвайзинг, алгоритмічні ризики, Explainable AI, кібербезпека, фінансова стабільність.

The article provides a comprehensive analysis of the potential threats associated with the use of artificial intelligence in the financial sector and substantiates practical ways to mitigate them. The relevance of the topic is determined by the rapid transition of banks, investment companies and fintech platforms from simple automation to predictive analytics, robo-advisory models and generative AI-based decision support. The purpose of the study is to identify the key technological, systemic, ethical and legal risks that arise when AI is integrated into financial consulting, lending, asset management and customer interaction, and to develop a set of measures that can reduce these risks without limiting useful innovation. The research methodology combines systemic and comparative analysis, classification of risks, synthesis of regulatory approaches, logical generalization and elements of scenario analysis. The study shows that AI improves the speed of data processing, reduces transaction costs, expands access to personalized financial services and increases the accuracy of operational decisions. At the same time, the article proves that the economic effect of AI cannot be considered separately from the quality of data, transparency of models, cybersecurity, accountability and consumer protection. The main threats include the black-box problem, algorithmic bias, adversarial manipulation of input data, excessive dependence on external technology providers, homogeneous trading strategies, blurred liability for automated decisions and the risk of erosion of customer trust. The practical value of the study lies in the proposed risk minimization framework based on Explainable AI, algorithmic

audit, human-in-the-loop governance, continuous model monitoring, data quality control, cybersecurity-by-design, stress testing and regulatory sandboxes. The article argues that the most sustainable model for finance is not full replacement of human expertise but hybrid intelligence, in which AI performs analytical and operational tasks while humans retain strategic, ethical and legal responsibility for critical decisions.

Keywords: artificial intelligence, financial sector, AI banking, robo-advisory, algorithmic risks, Explainable AI, cybersecurity, financial stability.

Постановка проблеми. Фінансовий сектор належить до сфер, у яких цифрові технології найшвидше трансформують традиційні бізнес-моделі. Банки, страхові компанії, інвестиційні посередники та фінтех-платформи дедалі активніше застосовують алгоритми машинного навчання для скорингу, виявлення шахрайства, персоналізації продуктів, управління портфелями, автоматизації комплаєнсу та комунікації з клієнтами. Якщо перший етап цифровізації був пов'язаний переважно з перенесенням стандартних операцій у дистанційні канали, то сучасний етап характеризується делегуванням алгоритмам частини аналітичних і рекомендаційних функцій, що раніше виконувалися людиною-експертом.

Поширення штучного інтелекту (ШІ) у фінансах має подвійний ефект. З одного боку, воно підвищує швидкість опрацювання великих масивів даних, знижує операційні витрати, розширює фінансову інклюзію та створює умови для глибшої персоналізації послуг. З іншого боку, фінансові рішення є високочутливими для добробуту громадян, стабільності ринків і довіри до інститутів. Тому алгоритмічна помилка, некоректний набір даних або кібератака на модель можуть мати не лише індивідуальні, а й системні наслідки. Саме це переводить дискусію про ШІ з площини технологічної ефективності у площину економічної безпеки, етики, правового регулювання та корпоративного управління.

Для України зазначена проблематика має особливу актуальність, оскільки стратегічні документи розвитку фінансового сектору орієнтують регуляторів і ринок на фінансову стабільність, інклюзію, кібербезпеку та поширення новітніх технологій [12]. В умовах євроінтеграції важливим стає узгодження національних підходів до використання ШІ з міжнародними стандартами прозорості, нагляду, захисту даних і відповідальності. Отже, ключовим науково-практичним завданням є визначення балансу між інноваційним потенціалом ШІ та ризиками, які виникають у процесі його впровадження у фінансові рішення.

Аналіз останніх досліджень і публікацій. Теоретичне підґрунтя дослідження цифрової трансформації економіки сформоване у працях Е. Бріньолфссона та Е. Макафі, які розглядають автоматизацію та інтелектуальні технології як чинник зміни продуктивності, зайнятості та структури ринків [1]. К. Шваб пов'язує розвиток ШІ з четвертою промисловою революцією, у межах якої межі між фізичними, цифровими та біологічними системами стають менш очевидними [2]. Т. Девенпорт акцентує увагу на прикладному використанні когнітивних технологій у бізнесі та наголошує, що економічний ефект ШІ залежить не лише від потужності алгоритмів, а й від управлінських процесів, якості даних і готовності організації до змін [3].

У фінансовій сфері значний внесок у вивчення робо-едвайзингу та довіри клієнтів зробили D. Belanche, L. V. Casalo та C. Flavian, які доводять, що намір користувачів застосовувати роботизованих радників залежить не лише від очікуваної корисності, а й від сприйняття ризику, довіри та зрозумілості сервісу [6]. Регуляторний і наглядовий вимір проблеми розкрито у звітах EBA, FSB, OECD та IOSCO. EBA підкреслює, що складні моделі можуть підвищувати точність прогнозів, але водночас породжують проблеми пояснюваності, інтерпретованості, якості даних, етики та відповідальності [7, с. 3-4]. FSB у 2024 р. окреслює вразливості, що можуть посилити системний ризик: залежність від третіх сторін, концентрацію постачальників, ринкові кореляції, кіберризики, модельний ризик та проблеми управління даними [8]. OECD розглядає ШІ у фінансах крізь призму фінансової стабільності, доброчесності ринку, конкуренції та захисту споживачів [9]. IOSCO пропонує практичні заходи для посередників і керуючих активами, зокрема нагляд з боку менеджменту, тестування моделей, контроль даних, прозорість і розкриття інформації клієнтам [10, с. 3-5].

Вітчизняний контекст дослідження цифровізації фінансів розкрито у працях Т. Васильєвої, О. Кузьменко, В. Касьяненко, які аналізують вплив цифровізації на фінансову безпеку держави та банківських установ [13], а також у дослідженнях О. Дзюблюка, присвячених цифровій трансформації банківського біз-

несу та конкурентоспроможності банків [14]. Водночас у науковій літературі недостатньо систематизовано саме ризики автономізації фінансових рішень за допомогою ШІ та комплексні механізми їх мінімізації. Потребує уточнення співвідношення технологічних, правових, етичних і системних загроз, а також роль гібридних моделей управління, у яких алгоритм виконує аналітичну функцію, а людина зберігає контроль за критичними рішеннями.

Постановка завдання. Метою статті є теоретичне обґрунтування та систематизація потенційних загроз застосування штучного інтелекту у фінансовому секторі, а також визначення практичних шляхів їх мінімізації. Досягнення мети передбачає виконання таких завдань: визначити основні напрями використання ШІ у фінансових послугах; порівняти антропоцентричний та алгоритмічний підходи до фінансового консультування; класифікувати ключові загрози ШІ у фінансах; обґрунтувати систему заходів щодо їх попередження та зниження.

Об'єктом дослідження є процеси цифрової трансформації фінансових послуг, що охоплюють банківський сектор, інвестиційний консалтинг, управління активами, скоринг і клієнтські сервіси. Предметом дослідження є технологічні, економічні, етико-правові та регуляторні аспекти використання ШІ у фінансах. Методологічну основу становлять системний підхід, порівняльний аналіз, класифікація ризиків, узагальнення міжнародних регуляторних практик та логічне моделювання механізмів мінімізації загроз.

Виклад основного матеріалу дослідження. Штучний інтелект у фінансах доцільно розглядати не як окремий програмний продукт, а як сукупність методів аналізу даних, прогнозування, оптимізації та автоматизованої підтримки рішень. Найпоширенішими сферами використання ШІ є кредитний скоринг, протидія шахрайству, AML/CFT-моніторинг, персоналізація банківських продуктів, чат-боти, управління інвестиційними портфелями, алгоритмічна торгівля, оцінювання страхових ризиків і регуляторна звітність. Такі рішення ґрунтуються на різних типах даних: транзакційних історіях, демографічних характеристиках, поведінкових патернах, фінансовій звітності, макроекономічних індикаторах і ринкових сигналах.

Еволюцію ШІ у фінансовому консультуванні можна умовно поділити на три етапи. Перший етап пов'язаний із реактивною автоматизацією, коли алгоритми виконували переважно допоміжні функції: відповідали на типові запити клієнтів, здійснювали базову перевірку даних, прискорювали бек-офісні операції. Другий етап характеризується поширенням предиктивної аналітики і робо-едвайзингу, коли системи почали формувати рекомендації щодо кредитування, заощаджень або інвестиційного портфеля. Третій етап пов'язаний із генеративним ШІ та агентними системами, здатними не лише обробляти інформацію, а й ініціювати рекомендації, формувати сценарії, моделювати поведінку клієнта та здійснювати динамічне ребалансування активів у межах заданих параметрів.

Перевага ШІ полягає у масштабованості. Після розроблення та навчання моделі вартість обслуговування додаткового користувача знижується, тоді як у традиційному консалтингу кожен новий клієнт потребує часу фінансового консультанта. Крім того, алгоритм не втомлюється, не залежить від робочого графіка і може аналізувати значно більші масиви інформації, ніж людина. Однак ці переваги не означають повної заміни людської експертизи. У фінансах значення мають не лише статистичні закономірності, а й життєві обставини клієнта, правові наслідки рішення, етичні межі персоналізації та здатність пояснити логіку рекомендації.

Ключовим обмеженням ШІ є проблема «чорної скриньки». Складні нейромережі можуть формувати точні прогнози, однак пояснити, чому саме певному клієнту відмовлено у кредиті або чому портфель було перебалансовано у конкретний спосіб, буває складно. Для фінансових установ це створює проблему доказовості, адже клієнт, регулятор і внутрішній аудитор мають розуміти принаймні загальну логіку рішення. Саме тому концепція Explainable AI (XAI) стає одним із базових елементів довіри до цифрового фінансового сервісу.

Другою групою загроз є алгоритмічна упередженість. Модель навчається на історичних даних, у яких можуть бути відображені попередні соціальні, регіональні або поведінкові нерівності. Якщо такі закономірності некритично переносяться у майбутні рішення, виникає ризик дискримінаційного скорингу, обмеження доступу до фінансування або нерівномірного ціноутворення для різних груп клієнтів. У європейському правовому полі це питання вже враховується через ризик-орієнтований підхід до регулювання ШІ, зокрема у сфері кредитоспроможності та скорингових рішень [11].

Таблиця 1

Порівняльна характеристика антропоцентричного та алгоритмічного фінансового консалтингу

Параметр порівняння	Антропоцентричний консалтинг	Алгоритмічний (ШІ) консалтинг
Швидкість реакції	Залежить від доступності консультанта та організаційних процедур	Миттєва або майже миттєва обробка запитів у режимі 24/7
Масштабованість	Обмежена кількістю фахівців і часом консультацій	Висока за рахунок автоматизації і низьких граничних витрат
Емпатія та контекст	Висока здатність враховувати життєві обставини клієнта	Обмежена даними і параметрами моделі
Ризик упередженості	Пов'язаний з людськими когнітивними помилками	Пов'язаний з якістю навчальних даних і архітектурою моделі
Прозорість відповідальності	Відносно чітка професійна та юридична відповідальність	Потребує окремого розподілу відповідальності між банком, розробником і провайдерами

Джерело: сформовано авторами на основі [3; 6; 10]

Третьою групою є кіберризики і ризики маніпулювання даними. Фінансові моделі залежать від якості вхідної інформації. Зловмисник може намагатися змінити дані, вплинути на навчальну вибірку, використати вразливості API або здійснити adversarial-атаку, коли мінімальна зміна параметрів спричиняє хибну класифікацію активу чи клієнта. У фінансах така атака здатна призвести до неправильної оцінки кредитного ризику, помилкового виявлення шахрайства або неадекватної торговельної реакції.

Четверта група загроз має системний характер. Якщо значна кількість фінансових установ використовує схожі моделі, схожі дані і схожих зовнішніх провайдерів, ринок стає більш однорідним. У кризовій ситуації це може сформувати ефект «цифрового стада»: алгоритми одночасно реагують на однаковий сигнал і підсилюють продаж активів, скорочення кредитування або переоцінку ризику. FSB прямо пов'язує такі ризики з ринковими кореляціями, концентрацією провайдерів і залежністю фінансових установ від третіх сторін [8].

П'ята група загроз стосується відповідальності. У традиційній моделі помилка фінансового консультанта або банку може бути проаналізована через професійні стандарти, посадові обов'язки та договірні відносини. У випадку самонавчальної системи відповідальність може розподілятися між банком, розробником, постачальником хмарної інфраструктури, власником даних і користувачем. Якщо цей розподіл не визначено заздалегідь, виникає правова невизначеність, що знижує довіру клієнтів і ускладнює компенсацію збитків.

Мінімізація зазначених загроз має бути комплексною. По-перше, фінансові установи повинні впроваджувати алгоритмічне управління на рівні корпоративної системи ризик-менеджменту, а не залишати його виключно у сфері IT-підрозділів. По-друге, критичні рішення мають проходити через human-in-the-loop, коли людина перевіряє рекомендацію алгоритму, особливо якщо вона впливає на доступ до кредиту, інвестиційну стратегію або захист прав споживача. По-третє, необхідні регулярні аудити моделей, контроль дрейфу даних, тестування у стресових сценаріях і протоколи аварійного відключення.

Важливе значення має якість даних. Дані повинні бути репрезентативними, актуальними, законно отриманими, очищеними від очевидних помилок і перевіреними на наявність непрямих дискримінаційних змінних. IOSCO рекомендує забезпечувати належну якість даних, тестування алгоритмів, прозорість розкриття інформації клієнтам і відповідальність керівництва за нагляд над ШІ [10, с. 4-5]. Для банківського сектору це означає, що модельний ризик має бути інтегрований у загальну систему внутрішнього контролю поряд із кредитним, операційним, ринковим і комплаєнс-ризиком.

Окремим напрямом є кіберстійкість. Принцип cybersecurity-by-design передбачає, що

Таблиця 2

Потенційні загрози ШІ у фінансах та напрями їх мінімізації

Група ризиків	Прояв у фінансових послугах	Можливі наслідки	Механізми мінімізації
Модельний ризик	Неправильна специфікація моделі, дрейф даних, переобучення	Хибний скоринг, помилкові інвестиційні рішення	Валідація, бек-тестинг, моніторинг продуктивності, stress testing
Непрозорість	Складність пояснення логіки нейромережі	Недовіра клієнтів, складність нагляду та аудиту	Explainable AI, модельні картки, журнали рішень, право на пояснення
Упередженість даних	Нерепрезентативні або історично дискримінаційні дані	Нерівний доступ до кредиту, репутаційні втрати	Data governance, fairness-тести, очищення змінних, незалежний аудит
Кіберризик	Adversarial attacks, викрадення даних, компрометація API	Фінансові збитки, шахрайство, витік персональних даних	Cybersecurity-by-design, сегментація доступів, моніторинг аномалій
Системний ризик	Однорідні алгоритми, залежність від провайдерів, синхронні ринкові реакції	Посилення волатильності, flash crash, концентрація ризику	Макропруденційний моніторинг, диверсифікація провайдерів, обмеження автономності
Правовий ризик	Нечіткий розподіл відповідальності за автоматизоване рішення	Спори з клієнтами, регуляторні санкції	Договірне закріплення відповідальності, human-in-the-loop, внутрішні політики

Джерело: сформовано авторами на основі [7-11]

захист моделі, даних, API, журналів рішень і середовища навчання закладається на етапі проєктування системи. Практично це означає сегментацію доступів, багаторівневу автентифікацію, шифрування, журналювання дій, регулярне тестування на проникнення, моніторинг аномалій та план реагування на інциденти. Для фінансових інституцій ШІ не може бути лише інструментом оптимізації; він має стати об'єктом постійного нагляду.

Регуляторний рівень мінімізації ризиків повинен поєднувати гнучкість і вимогливість. Надмірно жорстке регулювання може сповільнити інновації, але відсутність правил здатна створити недовіру та системні вразливості. Оптимальним інструментом є регуляторні «пісочниці», у яких нові моделі тестуються в обмеженому середовищі під наглядом регулятора. Такий підхід відповідає логіці розвитку фінтеху, яку Національний банк України визначав через створення інноваційної екосистеми, тестування нових проєктів, відкритий банкінг і посилення кібербезпеки [12].

У підсумку найбільш стійкою моделлю використання ШІ у фінансах є не повна автономізація, а гібридний інтелект. У такій моделі ШІ забезпечує швидкість, масштабованість, виявлення закономірностей і сценарне прогнозування, а людина відповідає за стратегічний вибір, етичну оцінку, комунікацію з клієнтом і юридичну відповідальність. Це дає змогу зберегти переваги цифровізації та водночас зменшити ризик втрати довіри, яка є базовим ресурсом фінансової системи.

Висновки. Проведене дослідження дозволяє зробити висновок, що штучний інтелект стає одним із ключових чинників трансформації фінансового сектору. Його застосування забезпечує підвищення швидкості оброблення інформації, зниження трансакційних витрат, розширення доступу до персоналізованих послуг, покращення скорингу, посилення протидії шахрайству та розвиток робоедвайзингу. Водночас ШІ створює новий клас загроз, які не можуть бути зведені лише до технічних помилок.

Основними ризиками застосування ШІ у фінансах є непрозорість алгоритмічних рішень, упередженість даних, кіберзагрози, маніпулювання вхідною інформацією, концентрація технологічних провайдерів, «цифрове стадо», правова невизначеність відповідальності та психологічний бар'єр довіри. Встановлено, що ці ризики мають взаємопов'язаний

характер: наприклад, низька якість даних посилює упередженість, непрозорість моделей ускладнює аудит, а концентрація інфраструктури підвищує системну залежність фінансових установ.

Мінімізація загроз, пов'язаних із використанням штучного інтелекту у фінансовій сфері, можлива за умови формування цілісної системи його контролю, яка передбачає прозорість алгоритмів, регулярну перевірку якості даних, постійний моніторинг роботи моделей, захист від кіберзагроз, участь людини у прийнятті критично важливих рішень та чіткий розподіл відповідальності між учасниками цього процесу. Практичне значення запропонованого підходу полягає у можливості його застосування фінансовими установами для побудови безпечної, прозорої та клієнтоорієнтованої моделі ШІ-банкінгу.

Перспективи подальших досліджень пов'язані з розробленням методик кількісної оцінки алгоритмічного ризику, формуванням стандартів аудиту ШІ-моделей у банківському секторі, адаптацією європейських регуляторних вимог до українського фінансового ринку та побудовою моделей гібридного інтелекту, у яких технологічна ефективність поєднується з етичною й правовою відповідальністю людини.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Бріньолфссон Е., Макафі Е. Друга епоха машин: робота, прогрес і процвітання в часи надзвичайних технологій / пер. з англ. Київ : Наш Формат, 2016. 312 с.

2. Шваб К. Четверта промислова революція. Харків : Клуб сімейного дозвілля, 2019. 416 с.

3. Davenport T. H. The AI Advantage: How to Put the Artificial Intelligence Revolution to Work. Cambridge, MA : MIT Press, 2018. 248 p. DOI: 10.7551/mitpress/11781.001.0001.

4. Davenport T. H., Ronanki R. Artificial Intelligence for the Real World. *Harvard Business Review*. 2018. Vol. 96, No. 1. P. 108-116.

5. OECD. Artificial Intelligence, Machine Learning and Big Data in Finance: Opportunities, Challenges, and Implications for Policy Makers. *Paris : OECD Publishing,* 2021. DOI: 10.1787/98e761e7-en.

6. Belanche D., Casaló L. V., Flavián C. Artificial Intelligence in FinTech: understanding robo-advisors adoption among customers*. Industrial Management & Data Systems.* 2019. Vol. 119, No. 7. P. 1411-1430. DOI: 10.1108/IMDS-08-2018-0368.

7. European Banking Authority. Report on Big Data and Advanced Analytics. Paris : EBA, 2020. URL: https://www.eba.europa.eu/sites/default/files/document_library/Final%20Report%20on%20Big%20Data%20and%20Advanced%20Analytics.pdf (дата звернення: 29.04.2026).

8. Financial Stability Board. The Financial Stability Implications of Artificial Intelligence. Basel : FSB, 2024. URL: https://www.fsb.org/2024/11/the-financial-stability-implications-of-artificial-intelligence/ (дата звернення: 29.04.2026).

9. OECD. OECD Business and Finance Outlook 2021: AI in Business and Finance. Paris : OECD Publishing, 2021. URL: https://www.oecd.org/en/publications/oecd-business-and-finance-outlook-2021_ba682899-en.html (дата звернення: 29.04.2026).

10. IOSCO. The Use of Artificial Intelligence and Machine Learning by Market Intermediaries and Asset Managers: Final Report. Madrid : International Organization of Securities Commissions, 2021. URL: https://www.iosco.org/library/pubdocs/pdf/IOSCOPD684.pdf (дата звернення: 29.04.2026).

11. 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. URL: https://eur-lex.europa.eu/eli/reg/2024/1689/oj/eng (дата звернення: 29.04.2026).

12. Національний банк України. Стратегія розвитку фінансового сектору України. 2025. URL: https://bank.gov.ua/ua/about/develop-strategy (дата звернення: 29.04.2026).

13. Васильєва Т. А., Кузьменко О. В., Касьяненко В. О. Моделювання впливу цифровізації на фінансову безпеку держави, банківських установ та суб'єктів господарювання. *Маркетинг і менеджмент інновацій*. 2020. № 4. С. 233-244. DOI: 10.21272/mmi.2020.4-18.

14. Дзюблюк О. В. Цифрова трансформація банківського бізнесу як чинник підвищення конкурентоспроможності банків в умовах глобалізації. *Економіка та суспільство*. 2021. № 32. DOI: 10.32782/2524-0072/2021-32-61.

REFERENCES:

1. Brynjolfsson, E., & McAfee, A. (2016). Druha epokha mashyn: robota, prohres i protsvitannia v chasy nadzvychainykh tekhnolohii [The second machine age: Work, progress, and prosperity in a time of brilliant technologies]. Kyiv: Nash Format. 312 p.

2. Schwab, K. (2019). Chetverta promyslova revoliutsiia [The fourth industrial revolution]. Kharkiv: Klub simeinoho dozvillia. 416 p.

3. Davenport, T. H. (2018). The AI advantage: How to put the artificial intelligence revolution to work. MIT Press. https://doi.org/10.7551/mitpress/11781.001.0001

4. Davenport, T. H., & Ronanki, R. (2018). Artificial intelligence for the real world. *Harvard Business Review*, 96(1), 108-116.

5. OECD. (2021). Artificial intelligence, machine learning and big data in finance: Opportunities, challenges, and implications for policy makers. *OECD Publishing*. https://doi.org/10.1787/98e761e7-en

6. Belanche, D., Casaló, L. V., & Flavián, C. (2019). Artificial intelligence in FinTech: Understanding robo-advisors adoption among customers. *Industrial Management & Data Systems,* 119(7), 1411-1430. https://doi.org/10.1108/IMDS-08-2018-0368

7. European Banking Authority. (2020). Report on big data and advanced analytics. Available at: https://www.eba.europa.eu/sites/default/files/document_library/Final%20Report%20on%20Big%20Data%20and%20Advanced%20Analytics.pdf (accessed April 29, 2026).

8. Financial Stability Board. (2024). The financial stability implications of artificial intelligence. Available at: https://www.fsb.org/2024/11/the-financial-stability-implications-of-artificial-intelligence/ (accessed April 29, 2026).

9. OECD. (2021). OECD business and finance outlook 2021: AI in business and finance. OECD Publishing. Available at: https://www.oecd.org/en/publications/oecd-business-and-finance-outlook-2021_ba682899-en.html (accessed April 29, 2026).

10. IOSCO. (2021). The use of artificial intelligence and machine learning by market intermediaries and asset managers: Final report. Available at: https://www.iosco.org/library/pubdocs/pdf/IOSCOPD684.pdf (accessed April 29, 2026).

11. European Parliament and Council of the European Union. (2024). Regulation (EU) 2024/1689 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act). *Official Journal of the European Union.* Available at: https://eur-lex.europa.eu/eli/reg/2024/1689/oj/eng (accessed April 29, 2026).

12. National Bank of Ukraine. (2025). Stratehiia rozvytku finansovoho sektoru Ukrainy [Strategy of Ukrainian financial sector development]. Available at: https://bank.gov.ua/ua/about/develop-strategy (accessed April 29, 2026).

13. Vasylieva, T. A., Kuzmenko, O. V., & Kasianenko, V. O. (2020). Modeliuvannia vplyvu tsyfrovizatsii na finansovu bezpeku derzhavy, bankivskykh ustanov ta subiektiv hospodariuvannia [Modeling the impact of digitalization on the financial security of the state, banking institutions and business entities]. *Marketing and Management of Innovations*, 4, 233-244. https://doi.org/10.21272/mmi.2020.4-18

14. Dziubliuk, O. V. (2021). Tsyfrova transformatsiia bankivskoho biznesu yak chynnyk pidvyshchennia konkurentospromozhnosti bankiv v umovakh hlobalizatsii [Digital transformation of banking business as a factor of increasing bank competitiveness in the conditions of globalization]. *Ekonomika ta suspilstvo,* 32. https://doi.org/10.32782/2524-0072/2021-32-61

Дата надходження статті: 13.04.2026
Дата прийняття статті: 04.05.2026
Дата публікації статті: 13.05.2026