

Штучний інтелект у банківській діяльності: конституційні гарантії прав клієнта та ризик-орієнтована модель правового регулювання в Україні

Автор: Берназюк Інна

Видання: Конституціоналіст · 2026

Дата публікації: 2026-08-12

Постійна адреса: <https://constitutionalist.com.ua/shtuchnyj-intelekt-u-bankivskij-diialnosti-konstytutsijni-harantii-prav-kliienta-ta-ryzyk-orientovana-model-pravovoho-rehuliuвання-v-ukraini/>

Відомості про автора

Берназюк І.М.,
професор кафедри права
ПВНЗ «Європейський університет»,
доктор юридичних наук,
Заслужений юрист України
ORCID: 0000-0002-8460-2687
e-mail: innabernaziuk@gmail.com
УДК 347.734:004.8:342.7

Анотація

Статтю присвячено визначенню правових засад використання штучного інтелекту (далі також – ШІ) в банківській діяльності та формуванню ризик-орієнтованої моделі його регулювання в Україні. Обґрунтовано, що інтенсивність правового регулювання має залежати не від самого факту використання штучного інтелекту, а від можливого впливу конкретної системи на права клієнта, діяльність банку та фінансову стабільність.

Доведено, що використання штучного інтелекту для оцінки кредитоспроможності, визначення істотних умов фінансової послуги, фінансового моніторингу та інших юридично значущих рішень зумовлює застосування конституційних гарантій людської гідності, рівності та недискримінації, приватності й ефективного захисту прав. У відносинах між банком і клієнтом конституційні гарантії діють передусім через позитивні обов'язки держави забезпечити належне законодавче регулювання, банківський нагляд і судовий захист.

Запропоновано для потреб українського банківського регулювання поєднати два виміри ризику: вплив системи штучного інтелекту на права клієнта та її значущість для стійкості банку чи фінансової системи. На цій основі розмежовано допоміжні, значущі та високоризикові системи. Для останніх обґрунтовано підвищені вимоги до якості даних, недискримінаційності, документування, пояснюваності, людського контролю, незалежної перевірки придатності та кіберстійкості.

Окремо обґрунтовано процесуальне значення спеціального розподілу тягаря доказування у спорах про дискримінацію, що дає змогу врахувати інформаційну нерівність між клієнтом і банком при оскарженні автоматизованого рішення. Для фінансового моніторингу розмежовано внутрішню пояснюваність рішення, необхідну для його перевірки банком, регулятором і судом, та зовнішню пояснюваність, обсяг якої може бути обмежений законом. Основною процесуальною гарантією клієнта визначено можливість отримати зрозуміле пояснення несприятливого рішення та домогтися його реального перегляду уповноваженим працівником банку.

Обґрунтовано незмінність юридичної відповідальності банку у разі залучення зовнішніх постачальників та необхідність включення ризиків штучного інтелекту до чинної системи корпоративного управління,

управління ризиками і внутрішнього контролю. Сформульовано конкретні пропозиції щодо вдосконалення законодавства про споживче кредитування та нормативно-правових актів Національного банку України.

Ключові слова: штучний інтелект, банківська діяльність, права людини, кредитоспроможність, дискримінація, приватність, пояснення рішення, людський контроль, банківський нагляд, управління ризиками.

Abstract (English)

Inna Bernaziuk. Artificial intelligence in banking: constitutional guarantees of clients' rights and a risk-based model of legal regulation in Ukraine

The article examines the legal framework for the use of artificial intelligence in banking and develops a risk-based model for its regulation in Ukraine. It argues that regulatory intensity should depend not on the mere use of artificial intelligence but on the potential impact of a particular system on clients' rights, banking institutions and financial stability.

The study establishes that artificial intelligence used for creditworthiness assessment, determination of material terms of financial services, financial monitoring and other legally significant decisions engages constitutional guarantees of human dignity, equality and non-discrimination, privacy and effective protection of rights. In relations between banks and clients, constitutional guarantees operate primarily through the State's positive obligations to ensure adequate legislation, banking supervision and judicial protection.

The article proposes combining two dimensions of risk for Ukrainian banking regulation: the impact of an artificial intelligence system on clients' rights and its significance for the stability of a bank or the financial system. On this basis, auxiliary, significant and high-risk systems are distinguished. Enhanced requirements concerning data quality, non-discrimination, documentation, explainability, human oversight, independent validation and cyber resilience are substantiated for high-risk systems.

The article also substantiates the procedural significance of the special allocation of the burden of proof in discrimination disputes, taking into account the informational asymmetry between the client and the bank. In the field of financial monitoring, a distinction is drawn between the internal reviewability of an automated decision and the scope of information that may lawfully be disclosed to the client.

The principal procedural safeguard is defined as the client's ability to obtain a meaningful explanation of an adverse decision and genuine review by an authorised bank employee. The specific limits of this safeguard in financial monitoring are identified. The continued legal responsibility of a bank where external providers are involved is substantiated, and specific proposals for improving Ukrainian consumer credit legislation and National Bank of Ukraine regulation are formulated.

Keywords: artificial intelligence, banking, human rights, creditworthiness, discrimination, privacy, explanation, human oversight, banking supervision, risk management.

Постановка проблеми

Штучний інтелект поступово стає звичайним засобом здійснення банківської діяльності. Його використовують для автоматизації внутрішніх процесів, обслуговування клієнтів, персоналізації банківських пропозицій, оцінювання кредитного ризику, виявлення шахрайських операцій і фінансового моніторингу [1; 5; 6; 11]. Відповідні технології змінюють не лише внутрішню організацію банку, а й характер взаємодії «клієнт - банк» [5]. Банк міжнародних розрахунків до сфер, у яких використання штучного інтелекту здатне підвищувати ефективність фінансових установ, відносить, зокрема, кредитування, платежі, належну перевірку клієнтів, протидію шахрайству та виконання регуляторних вимог [14].

Практика українського банківського ринку свідчить, що використання штучного інтелекту вже вийшло за межі експериментальної автоматизації та охоплює кредитування, платежі, персоналізацію послуг, протидію шахрайству й безпосередню взаємодію з клієнтом. Так, член правління ПриватБанку Дмитро Мусієнко повідомляє про застосування машинного навчання для управління кредитними ризиками та беззаставного кредитування, персоналізації пропозицій і превентивного виявлення шахрайства [51]. У червні 2026 року

ПриватБанк і Mastercard здійснили першу в Україні оплату із застосуванням Mastercard Agent Pay, у межах якої ШІ-агент був інтегрований у платіжний процес [53]. ПУМБ, за словами заступника голови правління Артура Загородникова, уже використовує ШІ-чат-асистента, ШІ-помічника з продажів, рішення для комплаєнсу та регуляторних завдань, а також захищений AI-простір для працівників [52]. На рівні інших банків ШІ застосовується для аналізу документів при кредитуванні, стягнення простроченої заборгованості та телефонного продажу кредитних продуктів; зокрема, АТ «РАДАБАНК» у тестовому режимі використовує ШІ-агента для пропонування кредитів готівкою та кредитних карток, причому зафіксовано випадок завершення угоди без участі оператора [56]. Водночас самі учасники ринку визнають ризик помилкової інтерпретації запитів і «галюцинацій» моделей та вважають передчасним повне передання штучному інтелекту остаточного прийняття рішень [56]. Отже, для України питання пояснюваності, меж автоматизації та реального людського контролю вже мають практичний характер.

Правове значення такого використання змінюється, коли результат автоматизованого аналізу стає підставою рішення щодо конкретної особи. Відмова у кредитуванні, визначення істотних умов фінансової послуги, віднесення клієнта до певної категорії ризику, зупинення операції або припинення ділових відносин здатні істотно впливати на його фактичне та правове становище. За таких умов питання виходить за межі організації банківської діяльності та безпосередньо стосується правових гарантій людської гідності, рівності, приватності й ефективного захисту прав.

Технологічний спосіб підготовки рішення не повинен зменшувати рівень правового захисту особи. Водночас однакове посилене регулювання будь-якого використання штучного інтелекту могло б створити необґрунтовані перешкоди для розвитку банківських послуг. Тому предметом цього дослідження є правові критерії диференціації вимог до системи ШІ залежно від їх функцій і наслідків.

Стан дослідження, методологія та наукова новизна

В українській науковій літературі досліджено основні напрями використання штучного інтелекту банками, етапи його інтеграції, зміни у кредитному аналізі, персоналізації послуг та управлінні ризиками [1–4]. Є. Темченко систематизує способи використання відповідних систем у різних напрямках банківської діяльності [11], а Є. Малишко та В. Чернишов звертають увагу на пояснюваність, людський контроль, перевірку результатів і якість даних як засоби зменшення ризиків [12].

У зарубіжних дослідженнях відповідальне використання штучного інтелекту в банківській діяльності пов'язується зі справедливістю, пояснюваністю, захистом даних, безпекою та організаційною відповідальністю [7]. Системні дослідження вказують на ризики необґрунтованої диференціації, непрозорості моделей, недостатньої якості даних, кіберзагроз і залежності від зовнішніх постачальників [8; 20]. Окремий напрям утворюють юридичні праці про автоматизоване кредитне оцінювання та фінансовий моніторинг [21–23]. Конституційно-правові засади регулювання штучного інтелекту та його співвідношення з правами людини розкрито у попередніх дослідженнях [24–26].

Методологічну основу дослідження становлять формально-юридичний, порівняльно-правовий і системний методи, а також функціональний аналіз банківського регулювання. Положення національного, міжнародного та європейського права оцінюються з позицій верховенства права, юридичної визначеності, пропорційності, недискримінації та ефективності захисту прав.

Наукова новизна полягає у запропонованому для потреб українського банківського регулювання поєднанні двох самостійних вимірів ризику в межах єдиного наглядового інструменту: можливого впливу системи штучного інтелекту на права конкретного клієнта та її значущості для стійкості банку чи фінансової системи. На цій основі обґрунтовано самостійне оцінювання правозахисного і пруденційного ризиків та різницю відповідних правових і наглядових вимог.

1. Конституційні гарантії у відносинах між банком і клієнтом

Конституційний вимір використання штучного інтелекту банком потребує розмежування публічно- і приватноправових відносин. Банк у звичайних відносинах із клієнтом є приватним суб'єктом, а не органом публічної влади. Тому несприятливе кредитне рішення банку не слід механічно кваліфікувати як безпосереднє порушення ним статті 24 чи іншої норми Конституції України.

Значення конституційних гарантії у таких правовідносинах виявляється передусім через позитивні обов'язки держави забезпечити належне законодавче регулювання приватних відносин, ефективний нагляд і судовий захист. Такий підхід відповідає статті 8 Конвенції про захист прав людини і основоположних свобод та практиці ЄСПЛ, за якою позитивні обов'язки держави можуть охоплювати заходи, спрямовані на забезпечення поваги до приватного життя також у відносинах між приватними особами [19, § 23; 36, ст. 8].

Ця конструкція узгоджується зі статтею 8 Конституції України, яка закріплює верховенство Конституції та пряму дію її норм, але не перетворює кожний спір між банком і клієнтом на публічно-правовий. Статті 21 і 22 встановлюють невідчужуваність прав та забороняють при прийнятті нових законів звужувати зміст і обсяг існуючих прав, стаття 24 гарантує рівність, стаття 32 - невтручання в особисте і сімейне життя, стаття 55 - право на судовий захист, а стаття 64 визначає конституційні межі обмеження прав [27, ст. 8, 21, 22, 24, 32, 55, 64]. Використання нового способу прийняття рішення тому не може саме по собі бути підставою для зниження рівня правового захисту.

Конституційною основою такого підходу є також статті 3 і 28 Конституції України, які закріплюють особливе значення людської гідності та право кожного на її повагу [27, ст. 3, 28]. Використання автоматизованих засобів при прийнятті юридично значущих рішень не повинно позбавляти особу можливості бути почутою та права на ефективний перегляд рішення, що істотно впливає на її становище.

Конституційний Суд України у Рішенні від 1 червня 2016 року № 2-рп/2016 виходив із того, що обмеження конституційних прав повинні мати легітимну мету, бути обумовленими суспільною необхідністю та відповідати вимозі пропорційності [46, пп. 2.3–2.4 мотивувальної частини]. Для банківського використання штучного інтелекту це означає, що економічна доцільність, зменшення витрат або підвищення точності оцінювання самі по собі не можуть виправдовувати необмежене використання відомостей про особу чи позбавлення її необхідних процесуальних гарантії.

Особливого значення набуває принцип рівності. Закон України «Про засади запобігання та протидії дискримінації в Україні» від 6 вересня 2012 року № 5207-VI (далі - Закон № 5207-VI) визначає непряму дискримінацію як ситуацію, за якої внаслідок застосування формально нейтральних правових норм, критеріїв оцінки, правил, вимог чи практики для особи або групи осіб виникають менш сприятливі умови порівняно з іншими особами без належного об'єктивного виправдання [30, п. 3 ч. 1 ст. 1]. Для автоматизованого оцінювання така конструкція має безпосереднє значення: система може не використовувати захищену ознаку прямо, але враховувати інші відомості, статистично з нею пов'язані.

Тому юридична перевірка повинна охоплювати не тільки перелік використаних показників, а й наслідки їх застосування. Різне ставлення є правомірним, якщо критерій має об'єктивне виправдання, пов'язаний із законною метою оцінювання банківського ризику, а застосовані засоби є належними та необхідними [21; 30].

Практична дієвість заборони дискримінації залежить і від правил доказування. Клієнт зазвичай не має доступу до повної системи оцінювання, документації щодо її побудови та масиву даних, тому покладення на нього обов'язку довести внутрішній механізм виникнення дискримінаційного результату могло б істотно послабити судовий захист. Закон № 5207-VI гарантує право оскаржити рішення, дії чи бездіяльність, що містять ознаки дискримінації, та вимагати відшкодування завданої шкоди [30, ст. 14–15], а цивільне процесуальне законодавство передбачає спеціальне правило: після наведення позивачем фактичних даних, які підтверджують наявність дискримінації, доказування її відсутності покладається на відповідача [9, ч. 2 ст. 81]. Для спорів, що розглядаються за правилами господарського судочинства, автоматично переносити цю конструкцію немає підстав, оскільки Господарський процесуальний кодекс України аналогічного правила прямо не закріплює.

Таким чином, розвиток банківського штучного інтелекту не вимагає створення нового «конституційного права на захист від алгоритму». Необхідний рівень захисту може бути забезпечений належною конкретизацією вже існуючих конституційних гарантій у банківському, антидискримінаційному, інформаційному, споживчому та процесуальному законодавстві.

2. Приватність і межі використання даних

Результативність систем штучного інтелекту значною мірою залежить від обсягу та якості використаних даних. Однак можливість отримати точніший прогноз не є самостійною юридичною підставою для необмеженого збирання та використання інформації про клієнта.

Частина друга статті 32 Конституції України встановлює спеціальну гарантію щодо збирання, зберігання, використання та поширення конфіденційної інформації про особу [27, ч. 2 ст. 32]. Конституційний Суд України у Рішенні від 20 січня 2012 року № 2-рп/2012 зазначив, що до інформації про особисте і сімейне життя належать, зокрема, відомості про матеріальний стан, особисті майнові відносини та події професійної і ділової сфери, причому перелік конфіденційних відомостей про особу не є вичерпним [45, пп. 3.2–3.3 мотивувальної частини]. Ця правова позиція має безпосереднє значення для банківського оцінювання, яке здатне формувати висновок про особу на підставі сукупного аналізу багатьох окремих відомостей.

Закон України «Про захист персональних даних» прямо поширюється на діяльність з обробки персональних даних, що здійснюється повністю або частково із застосуванням автоматизованих засобів [29, ч. 2 ст. 1]. Крім того, суб'єкт персональних даних має право знати механізм автоматичної обробки своїх даних та право на захист від автоматизованого рішення, яке має для нього правові наслідки [29, пп. 12, 13 ч. 2 ст. 8]. Відсутність спеціального закону про штучний інтелект тому не означає відсутності правових меж щодо відомостей, які банк використовує для автоматизованого оцінювання.

Порівняльно-правове значення має Загальний регламент Європейського Союзу про захист даних - Регламент (ЄС) 2016/679. Він окремо регулює рішення, що ґрунтуються виключно на автоматизованій обробці та породжують юридичні або аналогічно істотні наслідки, і встановлює інформаційні гарантії щодо логіки, значення та передбачуваних наслідків такої обробки [38, ст. 13(2)(f), 14(2)(g), 15(1)(h), 22].

У справі *Rotaru v. Romania* ЄСПЛ визнав, що систематичне зберігання і використання відомостей про особу може становити втручання у сферу приватного життя [48, §§ 43–46]. Оскільки ця справа стосувалася діяльності державного органу, її значення для банківських правовідносин полягає у визначенні змісту права, ефективний захист якого держава повинна забезпечувати також у приватних відносинах; прямого перенесення обов'язків державного органу на банк із цього рішення не впливає. Для такого горизонтального виміру додатково показовою є справа *Satakunnan Markkinapörssi Oy and Satamedia Oy v. Finland*, предметом якої було масове опрацювання персональних даних приватними суб'єктами [47].

Директива (ЄС) 2023/2225 про кредитні договори для споживачів встановлює ще докладніший стандарт: відомості для оцінювання кредитоспроможності повинні бути необхідними, пропорційними, відповідними, повними і точними, а визначені спеціальні категорії персональних даних та інформація із соціальних мереж не можуть використовуватися для такої оцінки [39, ст. 18(2)–(4)].

Для українського права виправданим є закріплення правила, за яким банк використовує для оцінювання клієнта не всі доступні відомості, здатні підвищити статистичну точність, а лише дані, необхідність та обґрунтований зв'язок яких із відповідним банківським ризиком можуть бути доведені. Особливого значення це набуває щодо нетрадиційних джерел інформації: вони можуть полегшувати доступ до фінансових послуг осіб без достатньої кредитної історії, але водночас виступати непрямими замінниками захищених характеристик [14; 21].

3. Ризик-орієнтована модель правового регулювання

Однакові правові вимоги до всіх систем штучного інтелекту були б непропорційними. Для визначення належного рівня регуляторного втручання пропонується застосовувати дві взаємопов'язані координати: інтенсивність можливого впливу на права клієнта та значущість системи для стійкості банку або фінансової системи.

Для першої координати придатним є критерій, закріплений у статті 22 Регламенту (ЄС) 2016/679, - виникнення юридичних або аналогічно істотних наслідків [38, ст. 22]. У банківських правовідносинах істотним слід вважати вплив, здатний визначити або суттєво змінити доступ особи до фінансової послуги, її істотні умови, можливість розпоряджатися коштами чи продовжувати ділові відносини з банком.

Диференціація заходів залежно від імовірності та тяжкості можливого негативного впливу відповідає Рамковій конвенції Ради Європи про штучний інтелект, права людини, демократію та верховенство права [40]. Методологія Ради Європи конкретизує цю оцінку через показники масштабу, охоплення, ймовірності та можливості усунення несприятливих наслідків [41, с. 9].

Другу координату становлять можливі наслідки для операційної та фінансової стійкості, зокрема залежність від критичних зовнішніх постачальників, поширення однакових моделей та масштаб можливого збою [14; 16, с. 15–23; 17].

Кожна координата оцінюється самостійно та визнає відповідальний зміст правових і наглядових вимог. На цій основі пропонується розмежовувати три групи систем.

Допоміжними є системи, результат яких не має визначального впливу на рішення з істотними наслідками для клієнта і які не є істотними для операційної стійкості банку. Для них достатні загальні вимоги щодо захисту інформації, належного використання, розмежування доступу та внутрішнього контролю.

Значущими є системи, результат яких істотно впливає на підготовку такого рішення, але підлягає самостійній змістовній оцінці уповноваженим працівником банку, а також системи, збій яких помітно впливає на операційну стійкість банку без прямих наслідків для конкретного клієнта. До цієї групи можуть належати засоби персоналізації пропозицій, попереднього визначення операцій для додаткової перевірки або підтримки кредитного аналізу. Для них потрібні документування, контроль якості даних, перевірка на необґрунтовану диференціацію та можливість відступити від автоматизованої рекомендації.

Високоризиковими у запропонованій секторальній класифікації є системи, результат яких безпосередньо або фактично визначає рішення з юридичними чи аналогічно істотними наслідками для клієнта або використання яких створює високий ризик для стійкості банку чи фінансової системи. Це авторська категорія для банківського регулювання, яка не є тотожною формальному поняттю високоризикової системи у Регламенті (ЄС) 2024/1689.

Дві запропоновані координати визначають не лише інтенсивність, а й зміст правових вимог. Високий вплив на права клієнта зумовлює застосування передусім правозахисних гарантій недискримінації, пояснення рішення, людського перегляду та ефективного оскарження. Висока значущість для стійкості банку або фінансової системи зумовлює насамперед пруденційні вимоги - незалежну перевірку придатності, операційну стійкість, безперервність діяльності та оцінювання залежності від зовнішніх постачальників. Одна система може мати високий показник за однією координатою та низький - за іншою.

Регламент (ЄС) 2024/1689 прямо відносить до високоризикових системи, призначені для оцінювання кредитоспроможності фізичних осіб або визначення їх кредитного рейтингу, за винятком систем виявлення фінансового шахрайства [37, ст. 6(2), Додаток III, п. 5(b)]. Частина третя статті 6 передбачає загальний механізм, за якого окрема система з Додатка III за встановлених умов може не вважатися високоризиковою, якщо вона не створює істотного ризику шкоди для здоров'я, безпеки чи основоположних прав. Проте цей виняток прямо не застосовується, якщо система здійснює профілювання фізичних осіб: у такому випадку система з Додатка III завжди є високоризиковою [37, ст. 6(3)]. Для автоматизованого кредитного оцінювання це має особливе значення, оскільки використання персональних даних для прогнозової оцінки кредитоспроможності за своїм змістом часто становить профілювання.

Отже, європейський законодавець виходить із підвищеного ризику відповідної категорії рішень і не допускає зниження рівня гарантій лише на підставі формального твердження про обмежену роль конкретної системи.

Підвищені вимоги повинні охоплювати не лише точність результату, а й якість вихідних даних та стійкість системи до зовнішнього впливу. Спотворення даних, на яких ґрунтується функціонування системи, або цілеспрямоване втручання у формування її результату створюють ризики, що не зводяться до традиційного несанкціонованого доступу [10]. Європейський банківський орган пов'язує належне використання

розширених засобів аналізу з управління даними, можливістю простеження та перевірки, справедливостю, захистом персональних даних і безпекою [42, розд. 4–5].

Перевірка придатності високоризикової системи тому повинна охоплювати походження і репрезентативність даних, стійкість до зовнішнього втручання, можливість відстежувати істотні зміни та своєчасно виявляти погіршення результатів.

4. Оцінювання кредитоспроможності та процесуальні права клієнта

Автоматизоване оцінювання кредитоспроможності є найбільш показовим випадком підвищеного правового ризику. Воно одночасно стосується договірної свободи банку, управління кредитним ризиком, захисту споживача, приватності та рівності.

Банк має право оцінювати ризик невиконання кредитного зобов'язання і не зобов'язаний укладати кредитний договір із кожним заявником. Принцип недискримінації не створює суб'єктивного права на отримання кредиту. Проте свобода кредитного рішення не означає свободи використовувати критерії, які не мають належного зв'язку з кредитоспроможністю або спричиняють необґрунтовано несприятливе становище певних категорій осіб.

Настанови Європейського банківського органу щодо надання та моніторингу кредитів вимагають, щоб у разі використання автоматизованих моделей кредитна установа розуміла їх методологію, вхідні дані, припущення, обмеження і результати, мала процедури виявлення та запобігання упередженості, забезпечувала можливість простеження результату, регулярну перевірку якості та механізми відступу від автоматизованого висновку [43, пп. 54–55]. Ці вимоги поєднують захист споживача з належним управлінням кредитним ризиком: неналежне оцінювання кредитоспроможності здатне зашкодити і позичальникові, і фінансовій стійкості кредитора [43, пп. 8–11].

Основною процесуальною гарантією має бути можливість зрозуміти основні причини несприятливого рішення та реально вплинути на його повторний розгляд.

Стаття 18(8) Директиви (ЄС) 2023/2225 передбачає у разі автоматизованого оцінювання кредитоспроможності право споживача вимагати втручання людини з боку кредитора, одержати зрозуміле пояснення оцінки кредитоспроможності та функціонування автоматизованої обробки, висловити свою позицію й вимагати перегляду оцінки та кредитного рішення [39, ст. 18(8)].

Для клієнта достатнім має бути такий обсяг інформації, який дає змогу встановити основні обставини, що істотно вплинули на рішення, перевірити правильність використаних щодо нього даних, надати додаткові відомості та звернутися за повторним розглядом. Розкриття програмного коду, технічної документації, яка не є необхідною для розуміння причин рішення, або відомостей, що становлять комерційну таємницю, для реалізації цієї гарантії загалом не потрібне.

Такий підхід до пояснення рішення відповідає Рекомендації ОЕСР щодо штучного інтелекту: особі, на яку несприятливо вплинув результат системи, повинна надаватися зрозуміла інформація, достатня для усвідомлення та оскарження відповідного результату; водночас відповідальне використання передбачає людську участь і нагляд, належну надійність та безпеку систем [44, принципи 1.2–1.4].

Людський перегляд не може бути формальністю. Уповноважений працівник банку повинен мати достатні компетенції і повноваження перевірити істотні дані, врахувати обставини, яких система не врахувала, та за наявності підстав відхилити або скоригувати автоматизований результат. Міжнародні дослідження регулювання фінансового сектору так само пов'язують реальний людський контроль із наявністю у відповідальній особи повноважень втрутитися у процес прийняття рішення та запобігти несприятливому наслідку [15, с. 18–19].

5. Фінансовий моніторинг: межі пояснення клієнтові

Використання штучного інтелекту у фінансовому моніторингу має іншу правову природу. Банк у таких правовідносинах не лише реалізує власний приватний інтерес, а виконує передбачені законом обов'язки у сфері запобігання та протидії легалізації доходів, фінансуванню тероризму та фінансуванню розповсюдження зброї масового знищення.

Закон України «Про запобігання та протидію легалізації (відмиванню) доходів, одержаних злочинним шляхом, фінансуванню тероризму та фінансуванню розповсюдження зброї масового знищення» від 6 грудня 2019 року № 361-IX (далі - Закон № 361-IX) покладає на банки відповідні обов'язки первинного фінансового моніторингу [32].

Автоматизовані системи здатні визначати нетипові операції, взаємозв'язки та інші ознаки, що потребують додаткового аналізу [14; 23]. Однак необхідно розмежовувати автоматизований сигнал про необхідність перевірки та остаточне рішення, яке істотно обмежує становище клієнта. Статистична нетиповість операції не є самостійним доказом неправомірності поведінки особи.

Межі пояснення, яке може бути надане клієнтові у фінансовому моніторингу, визначаються спеціальними законодавчими обмеженнями. Закон № 361-IX окремо регулює таємницю фінансового моніторингу як інформацію, отриману спеціально уповноваженим органом під час державного фінансового моніторингу [32, п. 59 ч. 1 ст. 1], та встановлює самостійну заборону суб'єктам первинного фінансового моніторингу й іншим визначеним особам повідомляти клієнтів і третіх осіб про подання відповідної інформації спеціально уповноваженому органу та про окремі пов'язані з цим дії [32, ч. 10 ст. 16].

Тому внутрішня перевірюваність автоматизованого рішення - спроможність банку відтворити його підстави для внутрішнього контролю, Національного банку України, спеціально уповноваженого органу чи суду - не тотожна обсягу пояснення, який відповідно до закону може бути наданий клієнтові. У випадках, визначених законом, обсяг інформації, що повідомляється клієнтові, може бути обмежений заради ефективності фінансового моніторингу.

Водночас таке обмеження не повинно перетворюватися на загальну непідконтрольність автоматизованих рішень. Законодавство в окремих випадках саме визначає допустимий обсяг інформування клієнта, зокрема щодо рішень про продовження зупинення фінансових операцій [32, ст. 23]. Отже, належна модель має одночасно забезпечувати внутрішню перевірюваність рішення, можливість регуляторного та судового контролю і додержання встановленої законом заборони розголошення окремих відомостей.

Положення про здійснення банками фінансового моніторингу, затверджене постановою Правління Національного банку України від 19 травня 2020 року № 65 (далі - Положення НБУ № 65), уже ґрунтується на ризик-орієнтованому підході та передбачає обов'язок банку документувати оцінювання ризиків і прийняті рішення [34]. Автоматизований аналіз тому може бути включений у чинний механізм фінансового моніторингу без утворення окремої паралельної системи регулювання.

6. Відповідальність банку, зовнішні постачальники та банківська таємниця

Використання штучного інтелекту не повинно змінювати загальний принцип юридичної відповідальності банку за здійснювану ним діяльність. Передання окремої аналітичної функції автоматизованій системі або зовнішньому постачальнику не звільняє банк від відповідальності перед клієнтом за прийняте банківське рішення.

Цей висновок стосується і систем, які використовують зовнішню обчислювальну інфраструктуру або моделі загального призначення. Договірна чи інша юридична відповідальність постачальника перед банком може існувати паралельно, але клієнт не повинен установлювати весь ланцюг технологічних та договірних відносин для визначення суб'єкта, відповідального перед ним за рішення щодо банківського обслуговування.

Подібний підхід обґрунтовується і щодо іншого регульованого сегмента фінансового ринку - страхування. У попередньому дослідженні було зроблено висновок, що залучення зовнішнього постачальника системи

штучного інтелекту не звільняє фінансову установу від відповідальності перед клієнтом, а людський контроль має бути змістовним: уповноважена особа повинна бути спроможною перевірити автоматизований результат і відступити від нього за наявності підстав [50]. Цей висновок підтверджує ширший для регульованих фінансових послуг принцип: використання автоматизованої системи змінює спосіб підготовки рішення, але не суб'єкта юридичної відповідальності за нього.

Для зовнішнього використання відповідних систем принципове значення має режим банківської таємниці. Закон України «Про банки і банківську діяльність» прямо відносить до неї інформацію про фізичну особу, яка має намір укласти договір про споживчий кредит, отриману під час оцінки її фінансового стану [28, п. 9 ч. 2 ст. 60].

Водночас закон допускає надання інформації, що становить банківську таємницю, приватним особам та організаціям для виконання ними функцій або надання послуг банку на підставі договору; такі особи зобов'язані не розголошувати отриману конфіденційну інформацію і не використовувати її у власних інтересах чи в інтересах третіх осіб [28, ст. 61]. Отже, залучення зовнішнього постачальника саме по собі не є несумісним із режимом банківської таємниці, але не усуває обов'язку банку контролювати правову підставу, обсяг, мету, захищеність та подальше використання переданих відомостей.

Договори із зовнішніми постачальниками мають передбачати принаймні обмеження використання отриманих даних визначеною метою, належний режим доступу, обов'язок повідомляти банк про порушення безпеки, можливість перевірки виконання встановлених вимог та припинення використання інформації після завершення відповідних правовідносин.

Залежність від зовнішніх постачальників має також пруденційне значення. Рада з фінансової стабільності звертає увагу на те, що поширення штучного інтелекту збільшує залежність фінансових установ від спеціалізованого обладнання, обчислювальної інфраструктури та зовнішніх моделей, а концентрація постачальників здатна створювати системні операційні вразливості [16, с. 16–18].

Управління такими ризиками має бути включене до чинної системи корпоративного управління банком. Положення про організацію системи управління ризиками в банках України та банківських групах, затверджене постановою Правління Національного банку України від 11 червня 2018 року № 64 (далі - Положення НБУ № 64), уже передбачає розподіл функцій, відповідальність органів управління, систему управління ризиками та внутрішнього контролю [33].

У межах цієї системи банк може вести внутрішній перелік значущих систем штучного інтелекту, визначати відповідальних осіб, установлювати рівень ризику, здійснювати попередню та періодичну перевірку придатності, документувати істотні зміни та інциденти і контролювати зовнішніх постачальників. Для систем високого ризику функції розроблення, використання та незалежної перевірки доцільно організаційно розмежовувати.

7. Системний вимір ризику та банківський нагляд

Друга координата запропонованої моделі - значущість системи для стійкості банку або фінансової системи - потребує окремого наглядового оцінювання. Система, яка майже не впливає безпосередньо на становище конкретного клієнта, може водночас бути критичною для безперервності банківської діяльності. Рада з фінансової стабільності відносить до основних вразливостей залежність від зовнішніх постачальників та їх концентрацію, кореляцію поведінки фінансових установ, кіберризиків, ризику моделей, недостатню якість даних і недоліки внутрішнього управління [16, с. 15–23].

Банк міжнародних розрахунків додатково звертає увагу на взаємопов'язаність, проциклічність і можливість виникнення єдиних точок відмови [14]. Європейський центральний банк пов'язує значний рівень проникнення штучного інтелекту та концентрацію його постачальників із підвищенням операційних і кіберризиків, концентрацією ринку, однотипністю поведінки та посиленням ринкової кореляції [17].

Це підтверджує необхідність двовимірного наглядового підходу. Система кредитного оцінювання невеликого банку може мати високий ризик для прав клієнта, але не становити істотної загрози для фінансової системи.

Натомість система управління ліквідністю або критично важливий зовнішній обчислювальний засіб може майже не впливати на права конкретного клієнта, але мати високу операційну чи системну значущість.

Рівень наглядових вимог тому повинен визначатися не одним показником «високого ризику», а сукупністю обох координат. Це дозволяє диференціювати правозахисні та пруденційні заходи й уникнути як недостатнього контролю за юридично значущими рішеннями, так і надмірного регулювання допоміжних систем.

8. Оцінювання впливу на права клієнта

Для систем високого ризику виправданим є внутрішнє оцінювання їх можливого впливу на права клієнтів до початку використання та після істотної зміни системи.

Як методологічний орієнтир може застосовуватися розроблена Радою Європи методологія оцінювання ризиків і впливу систем штучного інтелекту на права людини, демократію та верховенство права. Вона передбачає контекстний аналіз ризику, врахування позицій заінтересованих осіб, оцінювання ризиків та впливів, визначення заходів щодо їх запобігання або зменшення і подальший повторний перегляд [41]. Методологія не має обов'язкової юридичної сили і прямо допускає її адаптацію до галузевого контексту.

Оцінювання має охоплювати принаймні мету використання системи; коло осіб, на яких вона може впливати; права та законні інтереси, яких може стосуватися результат; категорії та джерела даних; можливі дискримінаційні наслідки; ступінь автоматизації; порядок людського контролю; можливість виправлення помилкового результату; заходи із захисту інформації; залежність від зовнішніх постачальників та порядок подальшого спостереження за фактичними результатами. Оцінка здійснюється з урахуванням критеріїв ризику, визначених у розділі 3 цієї статті.

Практичне значення такого механізму полягає в його перевіряюваності. Банк повинен документально підтвердити встановлені ризики, результати їх оцінювання, застосовані заходи та розподіл відповідальності. Така документація має значення для внутрішнього контролю, банківського нагляду та, за потреби, судового захисту.

9. Напрями розвитку українського правового регулювання

Україна вже має основні нормативні складові для секторального регулювання: законодавство про банки, персональні дані, недискримінацію, споживче кредитування, фінансовий моніторинг та загальні правила захисту клієнтів на ринку фінансових послуг [18; 28–34].

Закон України «Про фінансові послуги та фінансові компанії» серед принципів надання фінансових послуг закріплює управління ризиками, захист конфіденційної інформації, недопущення необґрунтованої дискримінації споживачів, контроль якості та належний розгляд звернень [18, ч. 1 ст. 5]. Права клієнта охоплюють отримання необхідної та достовірної інформації, конфіденційність і захист порушених прав [18, ст. 6]. Наглядове регулювання поєднує завдання захисту клієнтів із забезпеченням стійкості фінансового ринку [18, ст. 21, 24–25].

Біла книга Міністерства цифрової трансформації України виходить із поступової моделі формування регулювання штучного інтелекту, яка має поєднувати захист прав людини та розвиток інновацій [35]. Дискусійний документ Національного банку України 2026 року вже формує секторальні засади відповідального використання штучного інтелекту на ринку фінансових послуг і охоплює ризик-орієнтоване управління, права споживачів, вимоги до даних, операційну стійкість, організаційну відповідальність та самооцінювання [13].

Наступним кроком мають бути не загальні декларації про необхідність регулювання, а конкретні зміни.

Практична діяльність Національного банку України вже розвивається у цьому напрямі. Голова НБУ А. Пишний, узагальнюючи обговорення Банку міжнародних розрахунків щодо використання штучного інтелекту центральними банками, наголошує на доцільності починати з випробування систем із низьким ризиком і поступово розширювати їх використання, одночасно розвиваючи внутрішню компетентність, механізми

управління, стандарти перевірки моделей та процедури контролю. У Національному банку України, за його повідомленням, уже затверджено Політику відповідального використання штучного інтелекту та здійснюється випробування можливих напрямів його застосування [49].

Показово, що необхідність поєднання технологічного розвитку з належним управлінням ризиками усвідомлюється й самим банківським та фінтех-середовищем. Голова правління Української асоціації фінтех та інноваційних компаній (UAFIC) Ростислав Дюк звертає увагу не лише на потенціал ШІ, а й на етичні, правові та бізнес-ризики його впровадження, зокрема залежність від зовнішніх технологічних платформ та умов їх ліцензування [57; 59]. На інституційному рівні UAFIC послідовно включає штучний інтелект до професійного порядку денного фінансового сектору, зокрема в межах UAFIN.TECH [54], а у 2026 році спільно з Національним банком України започаткувала AI Discussion Day як майданчик діалогу регулятора та ринку щодо майбутнього регулювання використання ШІ [58]. Суміжні ризики формулюють і представники банків: директор департаменту інформаційних технологій ПУМБ Андрій Бегунов наголошує на проблемі використання конфіденційної інформації за межами захищеного інформаційного периметра банку [57], тоді як заступник голови правління UKRSIBBANK Андрій Кашперук пов'язує наступний етап розвитку мобільного банкінгу з Open Banking та використанням ШІ-агентів для надання простіших банківських послуг [55]. Така практика підтверджує доцільність ризик-орієнтованої моделі, за якої правові вимоги мають визначатися не самим фактом використання ШІ, а характером даних, ступенем автономності системи, наслідками її рішень для клієнта та рівнем залежності банку від зовнішніх постачальників.

По-перше, Закон України «Про споживче кредитування» [31] варто доповнити положенням, відповідно до якого у разі використання автоматизованої системи, що має визначальний вплив на оцінку кредитоспроможності або рішення про надання кредиту, споживач має право бути поінформованим про автоматизований характер оцінювання, отримати зрозумілу інформацію про основні причини несприятливого рішення, подати додаткові відомості та вимагати його перегляду уповноваженим працівником кредитодавця.

По-друге, у цьому Законі слід закріпити, що відомості, які використовуються для автоматизованої оцінки кредитоспроможності, мають бути необхідними, належними, актуальними та обґрунтовано пов'язаними з відповідним кредитним ризиком. Використання захищених ознак або інших показників як їх фактичних замінників не повинно призводити до необґрунтованої дискримінації.

По-третє, Положення НБУ № 64 варто доповнити вимогами щодо внутрішнього обліку значущих систем штучного інтелекту, їх класифікації за рівнем ризику, визначення відповідальних осіб, порядку попередньої та періодичної перевірки придатності, контролю фактичних результатів, документування істотних змін та інцидентів, а також оцінювання залежності від зовнішніх постачальників.

По-четверте, Положення НБУ № 65 потребує конкретизації щодо використання автоматизованих систем фінансового моніторингу. Автоматизований сигнал ризику повинен підлягати належній змістовній перевірці у випадках, коли на його підставі планується рішення з істотними наслідками для клієнта. При цьому внутрішня перевірюваність і документування рішення не повинні тлумачитися як обов'язок повідомляти клієнтові відомості, розголошення яких заборонене Законом № 361-IX.

По-п'яте, для систем, що мають високий вплив на права клієнтів, Національний банк України може рекомендувати або надалі нормативно закріпити проведення попереднього оцінювання впливу на права людини, інтегрованого в чинні процедури управління банківськими ризиками. Для систем із високою операційною або системною значущістю має додатково оцінюватися концентрація зовнішніх постачальників, можливість заміни критичного постачальника та наслідки його недоступності.

Перехід до обов'язкових вимог варто здійснювати поступово. На початковому етапі найбільш виправданими є секторальні рекомендації Національного банку України та внутрішнє самооцінювання банків; надалі - контрольоване випробування нових систем, накопичення наглядової практики та інформації про істотні інциденти. Такий випереджальний, але пропорційний підхід узгоджується з висновком Truby, Brown і Dahdal про необхідність своєчасного регуляторного втручання у фінансовому секторі без необґрунтованого стримування інновацій [22]. Обов'язкові вимоги насамперед мають поширюватися на системи з високим впливом на права людини або високою значущістю для стійкості банку чи фінансової системи [13; 15; 35; 37; 40].

Такий підхід дозволяє використати вже наявні механізми банківського нагляду замість створення окремого громіздкого регуляторного режиму. Правове регулювання має своєчасно реагувати на встановлені ризики без запровадження абстрактних заборон, які необґрунтовано випереджають технологічний розвиток.

Список використаних джерел

1. Онищенко О. В., Терновська В. С., Ковальов В. В. Штучний інтелект у банківській системі: сучасний стан, напрями застосування та ефекти цифрової трансформації. *Бізнес-навігатор*. 2026. Вип. 1 (84). С. 544–549. DOI: [10.32782/business-navigator.84-84](https://business-navigator.ks.ua/journals/2026/84_2026/86.pdf). URL: https://business-navigator.ks.ua/journals/2026/84_2026/86.pdf (дата звернення: 12.08.2026).
2. Пузирьова П. В., Ірнazarов Д. Т. Особливості інтеграції штучного інтелекту у банківську систему України. *Вчені записки Університету «КРОК»*. 2025. № 1 (77). С. 66–79. DOI: [10.31732/2663-2209-2025-77-66-79](https://snku.krok.edu.ua/index.php/vcheni-zapiski-universitetu-krok/article/download/930/911/3459). URL: <https://snku.krok.edu.ua/index.php/vcheni-zapiski-universitetu-krok/article/download/930/911/3459> (дата звернення: 12.08.2026).
3. Солодкий В. В., Поліщук Ю. А. Впровадження штучного інтелекту в українських банках та бізнесі: перспективи та застереження. *Економічний вісник*. 2023. № 2 (82). С. 119–127. DOI: [10.33271/ebdut/82.119](https://ev.nmu.org.ua/docs/2023/2/EV20232_119-127.pdf). URL: https://ev.nmu.org.ua/docs/2023/2/EV20232_119-127.pdf (дата звернення: 12.08.2026).
4. Циганова Н. В., Суляев В. В. Використання штучного інтелекту для оцінки ESG-ризиків та підтримки ухвалення рішень у сфері сталого фінансування. *Міжнародний науковий журнал «Інтернаука»*. Серія: «Економічні науки». 2025. № 3 (95). Т. 2. С. 141–148. DOI: [10.25313/2520-2294-2025-3-10844](https://irbis-nbuv.gov.ua/cgi-bin/irbis_nbuv/cgiirbis_64.exe?C21COM=2&I21DBN=UJRN&IMAGE_FILE_DOWNLOAD=1&Image_file_name=PDF%2Fmnie_2025_3%282%29__19.pdf&P21DBN=UJRN). URL: https://irbis-nbuv.gov.ua/cgi-bin/irbis_nbuv/cgiirbis_64.exe?C21COM=2&I21DBN=UJRN&IMAGE_FILE_DOWNLOAD=1&Image_file_name=PDF%2Fmnie_2025_3%282%29__19.pdf&P21DBN=UJRN (дата звернення: 12.08.2026).
5. Стащук О. В., Мартинюк Р. Специфіка застосування когнітивних технологій та штучного інтелекту в сучасній банківській діяльності. *Економічний форум*. 2021. № 3. С. 134–138. URL: https://irbis-nbuv.gov.ua/cgi-bin/irbis_nbuv/cgiirbis_64.exe?C21COM=2&I21DBN=UJRN&IMAGE_FILE_DOWNLOAD=1&Image_file_name=PDF%2Fecfor_2021_3_21.pdf&P21DBN=UJRN (дата звернення: 12.08.2026).
6. Лук'яненко Ю. В. Штучний інтелект як драйвер персоналізованого продажу в банківських відділеннях: від стратегії до реалізації. *Актуальні проблеми економіки*. 2026. № 4 (298). С. 217–224. DOI: [10.32752/1993-6788-2026-1-298-217-224](https://eco-science.net/wp-content/uploads/2026/04/4.26._topic_Yuliia-Lukianenko-217-224.pdf). URL: https://eco-science.net/wp-content/uploads/2026/04/4.26._topic_Yuliia-Lukianenko-217-224.pdf (дата звернення: 12.08.2026).
7. Ratzan J., Rahman N. Measuring responsible artificial intelligence (RAI) in banking: a valid and reliable instrument. *AI and Ethics*. 2024. Vol. 4. P. 1279–1297. DOI: [10.1007/s43681-023-00321-5](https://link.springer.com/content/pdf/10.1007/s43681-023-00321-5.pdf). URL: <https://link.springer.com/content/pdf/10.1007/s43681-023-00321-5.pdf> (дата звернення: 12.08.2026).
8. Vuković D. B., Dekpo-Adza S., Matović S. AI integration in financial services: a systematic review of trends and regulatory challenges. *Humanities and Social Sciences Communications*. 2025. Vol. 12. Art. 562. DOI: [10.1057/s41599-025-04850-8](https://www.nature.com/articles/s41599-025-04850-8). URL: <https://www.nature.com/articles/s41599-025-04850-8> (дата звернення: 12.08.2026).
9. Цивільний процесуальний кодекс України : Закон України від 18 берез. 2004 р. № 1618-IV. URL: <https://zakon.rada.gov.ua/laws/show/1618-15#Text> (дата звернення: 12.08.2026).
10. Kovačević A., Radenković S. D., Nikolić D. Artificial intelligence and cybersecurity in banking sector: opportunities and risks. *Eighth International Scientific Conference Contemporary Issues in Economics, Business and Management (EBM 2024)*. 2025. P. 425–433. DOI: [10.46793/EBM24.425K](https://doi.ub.kg.ac.rs/doi/zbornici/ebm24-425k/). URL: <https://doi.ub.kg.ac.rs/doi/zbornici/ebm24-425k/> (дата звернення: 12.08.2026).
11. Temchenko E. Artificial intelligence in banking: a comprehensive mapping of applications, challenges, and strategic implications. *Socio-Economic Relations in the Digital Society*. 2025. Vol. 3 (57). P. 5–18. DOI: [10.55643/ser.3.57.2025.622](https://www.ser.net.ua/index.php/SER/article/view/622/590). URL: <https://www.ser.net.ua/index.php/SER/article/view/622/590> (дата звернення: 12.08.2026).
12. Малишко Є. О., Чернишов В. В. Штучний інтелект у фінансах: аналіз потенційних загроз та шляхи їх мінімізації. *Економіка та суспільство*. 2026. Вип. 85. С. 1565–1571. DOI: [10.32782/2524-0072/2026-85-193](https://economyandsociety.in.ua/index.php/journal/article/view/7971/7950). URL: <https://economyandsociety.in.ua/index.php/journal/article/view/7971/7950> (дата звернення: 12.08.2026).
13. Національний банк України. Дискусійний документ з етичного та відповідального використання штучного інтелекту учасниками ринку фінансових послуг України. Київ : НБУ, 2026. 20 с. URL: https://bank.gov.ua/admin_uploads/article/Discussion_paper_AI-2026-03-24.pdf (дата звернення: 12.08.2026).
14. Bank for International Settlements. Artificial intelligence and the economy: implications for central banks. *BIS Annual Economic Report 2024*. Basel : Bank for International Settlements, 2024. Ch. III. P. 91–120. URL: <https://www.bis.org/publ/arpdf/ar2024e3.pdf> (дата звернення: 12.08.2026).
15. Crisanto J. C., Leuterio C. B., Prenio J., Yong J. Regulating AI in the financial sector: recent developments and main challenges. *FSI Insights on Policy Implementation*. No. 63. Basel : Bank for International Settlements, 2024. URL:

<https://www.bis.org/fsi/publ/insights63.pdf> (дата звернення: 12.08.2026).

16. Financial Stability Board. The Financial Stability Implications of Artificial Intelligence. Basel : Financial Stability Board, 2024. 40 p. URL: <https://www.fsb.org/uploads/P14112024.pdf> (дата звернення: 12.08.2026).
17. Leitner G., Singh J., van der Kraaij A., Zsámboki B. The rise of artificial intelligence: benefits and risks for financial stability. Financial Stability Review. Frankfurt am Main : European Central Bank, May 2024. URL: https://www.ecb.europa.eu/press/financial-stability-publications/fsr/special/html/ecb.fsrart202405_02~58c3ce5246.en.html (дата звернення: 12.08.2026).
18. Про фінансові послуги та фінансові компанії : Закон України від 14 груд. 2021 р. № 1953-IX. URL: <https://zakon.rada.gov.ua/laws/show/1953-20#Text> (дата звернення: 12.08.2026).
19. X and Y v. the Netherlands, no. 8978/80, judgment of 26 March 1985. European Court of Human Rights. HUDOC. URL: <https://hudoc.echr.coe.int/eng?i=001-57603> (дата звернення: 12.08.2026).
20. Kuanova L. A., Otegen A. N. Artificial intelligence in banking risk management: a bibliometric analysis. International Journal of Financial Studies. 2026. Vol. 14, Iss. 4. Art. 93. DOI: 10.3390/ijfs14040093. URL: <https://www.mdpi.com/2227-7072/14/4/93/pdf> (дата звернення: 12.08.2026).
21. Langenbucher K. Responsible A.I.-based Credit Scoring – A Legal Framework. European Business Law Review. 2020. Vol. 31, No. 4. P. 527–572. DOI: 10.54648/EULR2020022. URL: https://www.researchgate.net/publication/360071274_Responsible_AI-based_Credit_Scoring_-_A_Legal_Framework (дата звернення: 12.08.2026).
22. Truby J., Brown R., Dahdal A. Banking on AI: mandating a proactive approach to AI regulation in the financial sector. Law and Financial Markets Review. 2020. Vol. 14, No. 2. P. 110–120. DOI: 10.1080/17521440.2020.1760454. URL: <https://www.tandfonline.com/doi/full/10.1080/17521440.2020.1760454> (дата звернення: 12.08.2026).
23. Turksen U., Benson V., Adamyk B. Legal implications of automated suspicious transaction monitoring: enhancing integrity of AI. Journal of Banking Regulation. 2024. Vol. 25. P. 359–377. DOI: 10.1057/s41261-024-00233-2. URL: <https://link.springer.com/article/10.1057/s41261-024-00233-2> (дата звернення: 12.08.2026).
24. Берназюк І. М. Штучний інтелект як нова реальність та його потенційний вплив на конституційно-правове регулювання в Україні. Аналітично-порівняльне правознавство. 2025. № 1. С. 76–82. DOI: 10.24144/2788-6018.2025.01.11. URL: <https://journal-app.uzhnu.edu.ua/article/view/323365/313600> (дата звернення: 12.08.2026).
25. Берназюк І. М. Штучний інтелект і права людини: виклики для Європейської конвенції з прав людини. Аналітично-порівняльне правознавство. 2025. № 3, ч. 1. С. 89–99. DOI: 10.24144/2788-6018.2025.03.1.12. URL: <https://journal-app.uzhnu.edu.ua/article/view/332656/321655> (дата звернення: 12.08.2026).
26. Берназюк І. М. Рамкова Конвенція Ради Європи про штучний інтелект у контексті захисту прав людини: виклики та значення для України. Науковий вісник Ужгородського національного університету. Серія: Право. 2026. Вип. 93, ч. 3. С. 18–30. DOI: 10.24144/2307-3322.2026.93.3.2. URL: <https://visnyk-pravo.uzhnu.edu.ua/article/view/354445/340733> (дата звернення: 12.08.2026).
27. Конституція України : Закон України від 28 червня 1996 р. № 254к/96-ВР. URL: <https://zakon.rada.gov.ua/laws/show/254к/96-вр#Text> (дата звернення: 12.08.2026).
28. Про банки і банківську діяльність : Закон України від 7 грудня 2000 р. № 2121-III. URL: <https://zakon.rada.gov.ua/laws/show/2121-14#Text> (дата звернення: 12.08.2026).
29. Про захист персональних даних : Закон України від 1 червня 2010 р. № 2297-VI. URL: <https://zakon.rada.gov.ua/laws/show/2297-17#Text> (дата звернення: 12.08.2026).
30. Про засади запобігання та протидії дискримінації в Україні : Закон України від 6 вересня 2012 р. № 5207-VI. URL: <https://zakon.rada.gov.ua/laws/show/5207-17#Text> (дата звернення: 12.08.2026).
31. Про споживче кредитування : Закон України від 15 листопада 2016 р. № 1734-VIII. URL: <https://zakon.rada.gov.ua/laws/show/1734-19#Text> (дата звернення: 12.08.2026).
32. Про запобігання та протидію легалізації (відмиванню) доходів, одержаних злочинним шляхом, фінансуванню тероризму та фінансуванню розповсюдження зброї масового знищення : Закон України від 6 грудня 2019 р. № 361-IX. URL: <https://zakon.rada.gov.ua/laws/show/361-20#Text> (дата звернення: 12.08.2026).
33. Про затвердження Положення про організацію системи управління ризиками в банках України та банківських групах : постанова Правління Національного банку України від 11 червня 2018 р. № 64. URL: https://bank.gov.ua/ua/legislation/Resolution_11062018_64 (дата звернення: 12.08.2026).
34. Про затвердження Положення про здійснення банками фінансового моніторингу : постанова Правління Національного банку України від 19 травня 2020 р. № 65. URL: https://bank.gov.ua/ua/legislation/Resolution_19052020_65 (дата звернення: 12.08.2026).

35. Біла книга з регулювання штучного інтелекту в Україні / Міністерство цифрової трансформації України. Київ, 2024. URL: <https://storage.thedigital.gov.ua/files/a/ba/d5da75c2613e331bb89258f950adcbae.pdf> (дата звернення: 12.08.2026).
36. Конвенція про захист прав людини і основоположних свобод : міжнародний договір від 4 листопада 1950 р. URL: https://zakon.rada.gov.ua/laws/show/995_004#Text (дата звернення: 12.08.2026).
37. Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act). Official Journal of the European Union. 2024. L, 2024/1689. URL: <https://eur-lex.europa.eu/eli/reg/2024/1689/oj/eng> (дата звернення: 12.08.2026).
38. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). Official Journal of the European Union. 2016. L 119. P. 1–88. URL: <https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng> (дата звернення: 12.08.2026).
39. Directive (EU) 2023/2225 of the European Parliament and of the Council of 18 October 2023 on credit agreements for consumers and repealing Directive 2008/48/EC. Official Journal of the European Union. 2023. L, 2023/2225. URL: <https://eur-lex.europa.eu/eli/dir/2023/2225/oj/eng> (дата звернення: 12.08.2026).
40. Council of Europe Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law : CETS No. 225, Vilnius, 5 September 2024. URL: <https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treaty-num=225> (дата звернення: 12.08.2026).
41. Council of Europe. HUDERIA: Human Rights, Democracy and the Rule of Law Impact Assessment for AI Systems. Strasbourg : Council of Europe, 2026. URL: <https://rm.coe.int/prems-002726-gbr-2006-huderia-texte-web-a4/48802ba7b1> (дата звернення: 12.08.2026).
42. European Banking Authority. Report on Big Data and Advanced Analytics. Paris : European Banking Authority, 2020. URL: https://www.eba.europa.eu/sites/default/files/document_library/Final%20Report%20on%20Big%20Data%20and%20Advanced%20Analytics.pdf (дата звернення: 12.08.2026).
43. European Banking Authority. Guidelines on Loan Origination and Monitoring. EBA/GL/2020/06. Paris : European Banking Authority, 2020. URL: <https://www.eba.europa.eu/activities/single-rulebook/regulatory-activities/credit-risk/guidelines-loan-origination-and-monitoring> (дата звернення: 12.08.2026).
44. OECD. Recommendation of the Council on Artificial Intelligence. OECD/LEGAL/0449. Adopted 22 May 2019; amended 3 May 2024. Paris : OECD, 2019–2024. URL: <https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449> (дата звернення: 12.08.2026).
45. Рішення Конституційного Суду України від 20 січ. 2012 р. № 2-рп/2012 у справі № 1-9/2012 за конституційним поданням Жашківської районної ради Черкаської області щодо офіційного тлумачення положень частин першої, другої статті 32, частин другої, третьої статті 34 Конституції України. URL: <https://zakon.rada.gov.ua/laws/show/v002p710-12#Text> (дата звернення: 12.08.2026).
46. Рішення Конституційного Суду України від 1 черв. 2016 р. № 2-рп/2016 у справі № 1-1/2016 за конституційним поданням Уповноваженого Верховної Ради України з прав людини щодо відповідності Конституції України (конституційності) положення третього речення частини першої статті 13 Закону України «Про психіатричну допомогу». URL: <https://zakon.rada.gov.ua/laws/show/v002p710-16#Text> (дата звернення: 12.08.2026).
47. Satakunnan Markkinapörssi Oy and Satamedia Oy v. Finland [GC], no. 931/13, judgment of 27 June 2017. European Court of Human Rights. HUDOC. URL: <https://hudoc.echr.coe.int/eng?i=001-175121> (дата звернення: 12.08.2026).
48. Rotaru v. Romania [GC], no. 28341/95, judgment of 4 May 2000. European Court of Human Rights. HUDOC. URL: <https://hudoc.echr.coe.int/eng?i=001-58586> (дата звернення: 12.08.2026).
49. Пишний А. Г. Головний меседж для всіх, хто впроваджує ШІ. NV. 2025. 1 липня. URL: <https://nv.ua/ukr/opinion/shtuchnyi-intelekt-u-bankingu-andriy-pishniy-zasterigaye-vid-nadmirmoji-doviri-do-instrumentu-50526307.html> (дата звернення: 12.08.2026).
50. Берназюк І. М. Штучний інтелект у страхуванні: правові межі алгоритмічного оцінювання ризику, ціноутворення та прийняття рішень щодо страхових виплат. Конституціоналіст. 2026. URL: <https://constitutionalist.com.ua/shtuchnyi-intelekt-u-strakhuvanni-pravovi-mezhi-alhorytmichnoho-otsiniuvannia-ryzkyu-tsinoutvorennya-ta-pryjniattia-rishen-shchodo-strakhovykh-vyplat> (дата звернення: 12.08.2026).
51. ПриватБанк. ШІ-асистенти, інновації в управлінні ризиками, ефективніше виявлення шахрайства завдяки AI - Дмитро Мусієнко про тренди діджитал-банкінгу. 2026. 23 квіт. URL: <https://privatbank.ua/news/2026/4/23/shi-asistenti-innovaciji-v-upravlinni-ryzikami-efektivnishe-viyavlennya-shahraystva-zavdyaki-ai-dmitro-musiyenko-pro-trendi-didzhital-bankingu> (дата звернення: 12.08.2026).

52. Перший Український Міжнародний Банк. Заступник голови правління ПУМБ Артур Загородников представив банк на XII Legal Banking Forum. 2026. 20 лют. URL: <https://about.pumb.ua/presscenter/news/item/7973-fuib-deputy-chairman-of-the-management-board-artur> (дата звернення: 12.08.2026).
53. ПриватБанк. Mastercard та ПриватБанк здійснили першу в Україні оплату, виконану ШІ-агентом. 2026. 23 черв. URL: <https://privatbank.ua/news/2026/6/23/mastercard-ta-privatbank-zdiysnili-pershu-v-ukrajini-oplatu-vikonanu-shi-agentom> (дата звернення: 12.08.2026).
54. Українська асоціація фінтех та інноваційних компаній. Майбутнє фінансів: що очікує українців у 2025 році обговорили на конференції UAFIN.TECH. 2024. 13 груд. URL: https://fintechua.org/uafintech_2024 (дата звернення: 12.08.2026).
55. UKRSIBBANK BNP Paribas Group. «Мобільна індустрія у майбутньому зміниться» - заступник голови правління, директор із питань роздрібного бізнесу Андрій Кашперук. 2025. 30 лип. URL: <https://ukrsibbank.com/news-post/mobile-industry-will-change-future> (дата звернення: 12.08.2026).
56. Банки довіряють ШІ продаж кредитів і дзвінки клієнтам. Фінансовий клуб. 2026. 1 лип. URL: <https://www.finclub.net/news/banky-doviraiut-shi-prodazh-kredytiv-i-dzvinky-kliientam.html> (дата звернення: 12.08.2026).
57. Захист конфіденційних даних - один із найбільших ризиків штучного інтелекту. Фінансовий клуб. 2024. 30 квіт. URL: <https://finclub.net/news/zakhyst-konfidentsiinykh-danykh-odyn-iz-naibilshykh-ryzykiv-shtuchnoho-intelektu.html> (дата звернення: 12.08.2026).
58. Штучний інтелект у фінансовому секторі: як НБУ регулюватиме використання ШІ банками та фінтехами. Fintech Insider. 2026. 30 квіт. URL: <https://fintechinsider.com.ua/shtuchnyj-intelekt-u-finansovomu-sektori-yak-nbu-regulyuvaty-me-vykorystanny-a-shi-bankamy-ta-fintehamy> (дата звернення: 12.08.2026).
59. 10 питань експерту: Ростислав Дюк, голова правління UAFIC, про підсумки року в FinTech та прогнози на 2024. Fintech Insider. 2023. 29 груд. URL: <https://fintechinsider.com.ua/10-pytan-ekspertu-rostyslav-dyuk-golova-pravlinnya-uafic-pro-pidsumk-y-roku-v-fintech-ta-prognozy-na-2024> (дата звернення: 12.08.2026).

Файли матеріалу

Оригінальний файл автора