

DOI: [https://doi.org/10.25140/2411-5215-2026-1\(45\)-289-300](https://doi.org/10.25140/2411-5215-2026-1(45)-289-300)

УДК 004.89:336.71

JEL Classification: G21; O33; D81

**Ольга Володимирівна Попело**

доктор економічних наук, доцент,  
професор кафедри менеджменту та адміністрування  
Національний університет «Чернігівська політехніка» (Чернігів, Україна)  
E-mail: [popelo.olha@gmail.com](mailto:popelo.olha@gmail.com). ORCID: <https://orcid.org/0000-0002-4581-5129>

**Сергій Олександрович Кононенко**

молодший науковий співробітник,  
Національний університет «Чернігівська політехніка» (Чернігів, Україна)  
E-mail: [job.s.kononenko@gmail.com](mailto:job.s.kononenko@gmail.com). ORCID: <https://orcid.org/0000-0002-1898-2204>

**ОСНОВНІ ЗАГРОЗИ ВИКОРИСТАННЯ ТЕХНОЛОГІЙ ШТУЧНОГО ІНТЕЛЕКТУ ТА ЇХНІЙ ПОТЕНЦІЙНИЙ НЕГАТИВНИЙ ВПЛИВ НА ФУНКЦІОНУВАННЯ КРЕДИТНИХ УСТАНОВ**

*Досліджено особливості впровадження технологій штучного інтелекту в діяльність кредитних установ. Обґрунтовано необхідність збалансування використання таких технологій та людської праці в діяльності кредитних установ у процесі ухвалення управлінських рішень. Означено важливість збереження персональних даних клієнтів, що впливає на репутацію та фінансову стійкість установи. Виокремлено основні види загроз, які виникають при використанні технологій ШІ в діяльності кредитних установ. Запропоновано алгоритм управління використанням технологій штучного інтелекту в діяльності кредитних установ.*

**Ключові слова:** цифровізація; кредитні установи; загрози; технології; штучний інтелект; цифрові технології.

Рис.: 3. Бібл.: 17.

**Постановка проблеми.** На сьогодні використання технологій штучного інтелекту як цифрового інструменту все частіше перетворюється на інфраструктурний елемент функціонування кредитних установ. Протягом останніх років європейський банківський сектор дедалі частіше використовує технології ML-рішень на основі штучного інтелекту, особливо в частині впровадження моделей нейронних мереж, дерева рішень та регресійних моделей для дослідження розвитку сектору.

Проте, не зважаючи на значні переваги у питаннях використання технологій ШІ в кредитних установах, є певні загрози, які виникають через залежність від інших сторін, кібератаки, недостовірність та низьку якість даних тощо. Особливо гостро ця проблема постає саме в кредитних установах через те, що вони часто використовують різні алгоритми, які застосовуються при оцінці ймовірностей банкрутства, моніторингу шахрайства, сегментації клієнтів, аналізі документів та інше.

Якщо розглядати приклад українських кредитних установ, то їхня діяльність у сучасних умовах здійснюється під впливом операційних невизначеностей, кіберзагроз, енергетичної нестабільності, комунікаційних ризиків, що значно підвищує ризики збитковості. При цьому, погг війну та пов'язані з нею безпекові ризики, кредитні установи продовжують вектор європейського розвитку, який включає розвиток цифровізації та використання технологій ШІ. Регуляторний ландшафт ЄС вже формує нові рамки щодо функціонування кредитних установ на основі впровадження ризик-орієнтованого підходу щодо регулювання та проведення кредитних скорингів до високоризикованих AI-систем, через їх доступність до фінансових ресурсів. Тому визначення загроз використання технологій ШІ є актуальним завданням не лише з позиції технічної модернізації кредитних установ, але й з позиції фінансової стійкості, захисту клієнтів, збереження репутації, пруденційної безпеки банківського сектору.

Світовий розвиток цифровізації, крім позитивних зрушень у частині розширення доступу до послуг, швидкості обробки інформації, призводить до посилення загроз з боку кібербезпеки, захисту персональних даних. Такі трансформаційні процеси потребують підвищеної уваги до моніторингу безпеки інформаційних систем кредитних установ та удосконалення стандартів захисту даних. Крім означених аспектів, слід враховувати потреби в підвищенні кваліфікації персоналу установ, розвитку їхніх цифрових навичок, ступеня опанування новітніх технологій та методик, які використовуються в діяльності кредитних установ.

**Аналіз останніх досліджень і публікацій.** У науковій літературі багато уваги приділено різним аспектам цифровізації функціонування кредитних установ, впровадженню технологій штучного інтелекту, управлінню кредитними ризиками, удосконаленню компетентностей персоналу банківського сектору та інше. Так, у своїх роботах Н. Ткачук [12] та Л. Кльоба [4] досліджують використання нейронних мереж для прогнозування дефолтів, що дає змогу кредитним установам більш раціонально використовувати дані щодо обсягів кредитних ресурсів. Автори М. Дубина [3; 5; 17], Н. Пантелєєва [6], Я. Дроботя, Л. Бражник [2] досліджували питання використання різних продуктів на базі ШІ, а саме використання нейронних мереж для класифікації позичальників та рівнем ризику, що дало змогу встановити ефективність запровадження таких технологій, що є важливим напрямом в процесах цифровізації.

Автори Н. Данік та А. Торлопов [1] досліджують використання технологій ШІ в банківському секторі з позиції розширення цифрових рішень для покращення якості обслуговування клієнтів, напрямів захисту від кібератак, швидкість обробки великих масивів даних. Проте, незважаючи на ґрунтовні дослідження питань використання ШІ у функціонуванні кредитних установ, враховуючи швидкий розвиток цифрових технологій і для забезпечення ефективності функціонування установ, доцільно виокремити загрози застосування таких технологій у секторі.

**Виділення недосліджених частин загальної проблеми.** У наукових колах значна увага приділяється дослідженню процесів впровадження та використання технологій штучного інтелекту кредитних установ з позиції удосконалення процесів взаємодії з клієнтами, розширенню цифрових послуг, аналітики даних, напрямів кібербезпеки тощо. Проте, враховуючи швидкий розвиток цифрових рішень та особливо технологій ШІ, доцільно дослідити не тільки позитивний вплив їх використання, але й загрози, які можуть спіткати кредитні установи при неналежному використанні таких інструментів. Виокремлення таких загроз дозволить вчасно реагувати на будь-які ризики, з метою їх подальшої мінімізації або уникнення.

**Мета статті** полягає в комплексному дослідженні основних загроз використання технологій ШІ та аналізі їхнього потенційного негативного впливу на функціонування кредитних установ.

**Виклад основного матеріалу дослідження.** Якщо розглядати досвід України в напрямку розвитку технологій на базі штучного інтелекту, особливо в діяльності кредитних установ, то слід приділити увагу подвійності таких процесів. З одного боку, використання сучасних технологій відтворює європейський вектор розвитку країни та відповідності до міжнародних норм. На сьогоднішній день цифрові рішення в сфері діяльності кредитних установ дозволяють підвищити якість обслуговування, розширити перелік послуг, пришвидшити обробку даних тощо. В напрямку операційної діяльності такі технології сприяють автоматизації комплаєнс процедур, мінімізації ризику, використання різних методів визначення та мінімізації ризиків, що є особливо актуальним в умовах турбулентності та невідомості зовнішнього середовища. З іншого боку, впровадження цифрових технологій на базі штучного інтелекту, несе певні ризики, які пов'язані перш за все, з забезпечення

## ФІНАНСОВІ РЕСУРСИ: ПРОБЛЕМИ ФОРМУВАННЯ ТА ВИКОРИСТАННЯ

кібербезпеки та мінімізації шахрайства. В умовах недосконалості українського законодавства в частині забезпечення захисту персональних даних це може привести до певних ризиків, в тому числі репутаційних [10].

Застосування сучасних технологій та програмних продуктів має певні вимоги до аналітичного базису, на основі якого здійснюється розрахунок та прогнозування відповідних економічних процесів. Недосконалість інформаційного забезпечення може привести до викривлення інформації щодо платоспроможності клієнтів як в бік завищення так і в бік втрати платоспроможних клієнтів. Тому за таких умов кредитним установам важливо використовувати технології та цифрові рішення, які б забезпечували фінансову стійкість, спроможність та ефективний захист персональних даних клієнтів, що в довгостроковій перспективі забезпечує конкурентні переваги на ринку кредитних послуг.

Впровадження технологій штучного інтелекту має певні зовнішні та внутрішні загрози, які можна виокремити таким чином (рис. 1).



Рис. 1. Основні зовнішні та внутрішні загрози використанні технологій ШІ у кредитних установах

Джерело: запропоновано авторами.

Зовнішні загрози використання технологій на базі штучного інтелекту найбільше представлені кіберзагрозами та використання в несанкціонованих програмних продуктів. Розповсюдження таких загроз пов'язано зі збільшенням використання програмних продуктів кредитними установами та банківським сектором, особливо в питаннях ідентифікації клієнтів, он-лайн обслуговування тощо, оскільки такі технології можуть використовуватися зі злочинними намірами, що посилює ризик їх використання. Для забезпечення безпеки кредитні установи повинні використовувати надійні програмні продукти щодо мінімізації кіберризиків на всіх етапах функціонування системи.

Загрози, які найбільше впливають на операційну діяльність, пов'язані з концентрацією постачальників та залежністю від третіх сторін, оскільки значна частина програмних рішень і хмарних технологій розробляється глобальними технологічними компаніями. У цьому аспекті існує загроза втрати контролю за моніторингом шахрайства внаслідок перебоїв сервісу, зміни тарифів, обмеженість доступу тощо. У відповідь на це Національний банк України запровадив окремі положення щодо використання хмарних обчислень, тим самим, визначивши ці ризики регуляторно значущими [8].

Динамізм зовнішнього середовища, особливо в умовах розвитку цифрових технологій потребує відповідних підходів до управління комплаєнс-ризиками. Більшість країн ЄС вже запровадили принципи ризик-орієнтованого підходу для використання продуктів на базі ШІ як відповідь на процеси підвищеної небезпеки для галузі. Для більшості кредитних установ, які здійснюють свою діяльність із залученням міжнародних партнерів, так само потрібно запроваджувати такі принципи у своїй практиці для відповідності встановленим вимогам.

Важливо враховувати воєнні шоки, які впливають на діяльність кредитних установ, які функціонують в межах України, оскільки такі ризики впливають на поведінку позичальників швидше, ніж адаптуються програмні моделі на базі ШІ. Так, за досить короткий термін суттєво змінилися умови функціонування бізнесу на території України, що вплинуло на релокацію бізнесу, руйнацію майна, зниження рівнів доходу позичальників, енергетичну кризу.

За таких турбулентних умов важливо відстежувати, наскільки програмні моделі враховують такі динамічні зміни для подальшого використання адекватних моделей та уникнення хибної точності, коли є розбіжності в математичних та економічних даних щодо їх адекватної інтерпретації [11]. За період військових дій банківський сектор втратив значну частину своїх активів через значні збитки та руйнацію майна, що вплинуло на можливість повернення позик клієнтами.

Вплинути на такі зовнішні події досить складно, тому до таких ризиків можливо лише адаптуватися або мінімізувати їх негативний вплив на основі використання різних інструментів прогнозування (математичні моделі, сценарні підходи тощо).

Посилення конкуренції в сфері кредитування осіб, важливу роль відіграє репутація та надійність установи, як один з факторів довіри з боку клієнтів. Тому при використанні технологій на базі штучного інтелекту повинно підкріплюватися компетенцією персоналу, що сприяє більш об'єктивному прийнятті рішень, враховуючи не тільки формальну ознаку клієнта але й відповідні особливості неформальних обставин. Найбільш такі нестандартні ситуації можуть виникати при кризових явищах, високій мінливості зовнішнього середовища, оскільки за таких умов не завжди вчасно можуть вноситися зміни в алгоритми системи, що призводить до викривлення інформації про клієнта. За сучасних умов розвитку соціальної активності та медійності клієнтів, існує загроза втрати репутації, що для кредитних установ є більшим ризиком ніж операційні збитки. Зовнішні ризики є менш контрольованими і адаптивними для діяльності кредитних установ, тому найчастіше такі загрози приймаються або мінімізуються їх негативний вплив [3; 17].

Загрози внутрішнього характеру є не менш важливими для функціонування кредитних установ, проте, на відміну від зовнішніх, на них є можливість вплинути. Так, основною внутрішньою загрозою для використання ШІ в діяльності кредитних установ є модельний ризик, який пов'язаний із послабленням функцій ризик-менеджменту. Такий ризик проявляється в некоректному визначенні ймовірності економічних криз, поведінки клієнтів. Як наслідок, для установи може бути або накопичення майбутніх збитків за рахунок лібералізації видачі кредитів, або навпаки, значне утримання кредитування що призводить до втрати надійних позичальників.

При визначенні таких ймовірностей окрім розрахункових методів, які базуються на цифровій аналітиці даних, застосовувати методи, в основі яких визначення якісних характеристик. Таке поєднання кількісних та якісних методів дозволить максимально врахувати ймовірні ризики та вигоди в діяльності кредитних установ [9].

Специфіка діяльності кредитних установ полягає в обробці аналітичного масиву даних, який є підґрунтям операційної діяльності. Тому важливо враховувати ризик неповних або зміщених даних при проведенні аналітичних досліджень з метою ухвалення управлінських рішень. Так, структура ШІ включає використання чотирьох базових опор для впровадження технологій: технологічна інфраструктура, управління масивом даних, організація та методологія розрахунків. Якщо одна з означених опор стає недостовірною, то надійність продукту на базі ШІ значно знижується [7].

Для вітчизняних кредитних установ ці ризики є актуальними, враховуючи значну релокацію бізнесу, переміщення осіб усередині країни, значну міграцію населення закордон, зниження рівня доходів клієнтів тощо. Система функціонування кредитних установ повинна бути більш гнучкою та швидко реагувати на відповідні зміни та враховувати їх у подальших розрахунках.

При оцінці кредитоспроможності клієнта досить часто виникають проблеми, які пов'язані з відтворенням дискримінаційних ефектів, які пов'язані з використанням проксі-змінних, таких як місце проживання, тип зайнятості, структура витрат тощо. З математичного погляду така аналітика платоспроможності клієнта є обґрунтованою, а з іншого – може створювати соціальні та юридичні проблеми. Клієнтоорієнтованість та прозорість ведення бізнесу потребують використання відповідного інструменту, який дозволить більш ґрунтовно відтворити напрями керованості та довіреності до даних та операцій обох учасників процесу.

Ризик втрати або порушення персональних даних на сьогодні є ключовим фактором репутації та надійності установи. Специфіка діяльності кредитних установ передбачає використання значної кількості особистої інформації клієнта, що може призвести до неправомірного їх застосування та юридичної відповідальності. За таких умов важливо дотримуватися балансу між використанням автоматизованих процесів та включенням людського фактору.

Особливо це стосується ситуацій, за яких керівництво більше покладається на результати рішень, які визначені за допомогою ШІ, ніж професійного судження спеціалістів. Не завжди моделі, які використовують ШІ, можуть бути об'єктивними в нетипових ситуаціях, що може привести до втрати прибутку або репутації установи. Потрібно зберігати баланс між технологічним використанням цифрових рішень та ефективністю корпоративного управління. Оскільки саме узгоджена робота всіх служб, відповідність компетенцій працівників сучасним вимогам цифровізації дасть змогу уникнути появи неконтрольованих ризиків.

Наявність зовнішніх та внутрішніх загроз щодо використання технологій штучного інтелекту в діяльності кредитних установ потребує відповідних напрямів захисту їхньої діяльності, які повинні удосконалюватися з урахуванням системності розвитку цифрових рішень. Так, основні ризики використання технологій ШІ в кредитних установах узагальнено можна представити таким чином (рис. 2).



Рис. 2. Основні ризики використання технологій ШІ в діяльності кредитних установ  
Джерело: узагальнено авторами на основі [5; 14; 15; 16].

Найбільшим ризиком при діяльності кредитних установ за умови використання цифрових технологій, є помилкова оцінка кредитоспроможності клієнта, що може привести до втрати вигідних клієнтів або навпаки, втрати прибутку установи за умови неплатоспроможності позичальника. На макрорівні в довгостроковій перспективі такі ситуації можуть привести до зниження ефективності кредитної установи та збільшення операційного ризику, що за умов посилення конкурентної боротьби значно ускладнює можливості розвитку та утримання позицій. З початком повномасштабного вторгнення у 2022 році діяльність кредитних установ та банківського сектору в Україні пов'язана з постійним ризиком. Така несприятлива безпекова ситуація вплинула на зростання кібератак на системи, збільшення операційного ризику, що пов'язано з втратою частини активів, відтоком кадрів, зменшенням операційної діяльності. За таких шоккових умов потрібно вчасно вносити зміни у алгоритми цифрових технологій для мінімізації ризиків та врахування відповідних змін у зовнішньому та внутрішньому середовищі. В умовах посилення конкуренції та зниження економічної стабільності для утримання обсягів клієнтської бази, доцільно більш залучати компетентний персонал, оскільки людський фактор є більш гнучким у прийнятті управлінських рішень ніж алгоритми технологій. Саме гнучкість по відношенню до клієнта та особистий підхід сприятиме залученню додаткових коштів, підвищенню репутації та надійності кредитної установи.

Для мінімізації загроз використання технологій ШІ в діяльності кредитних установ слід дотримуватися відповідної послідовності дій, яку узагальнено можна представити наступними етапами (рис. 3). На першому етапі здійснюється постановка мети впровадження технологій ШІ в діяльність кредитних установ, на основі чого в подальшому здійснюється формування загального контуру операційної діяльності. Визначається клієнтська база, власники, партнери, система ризик-менеджменту.

## ФІНАНСОВІ РЕСУРСИ: ПРОБЛЕМИ ФОРМУВАННЯ ТА ВИКОРИСТАННЯ

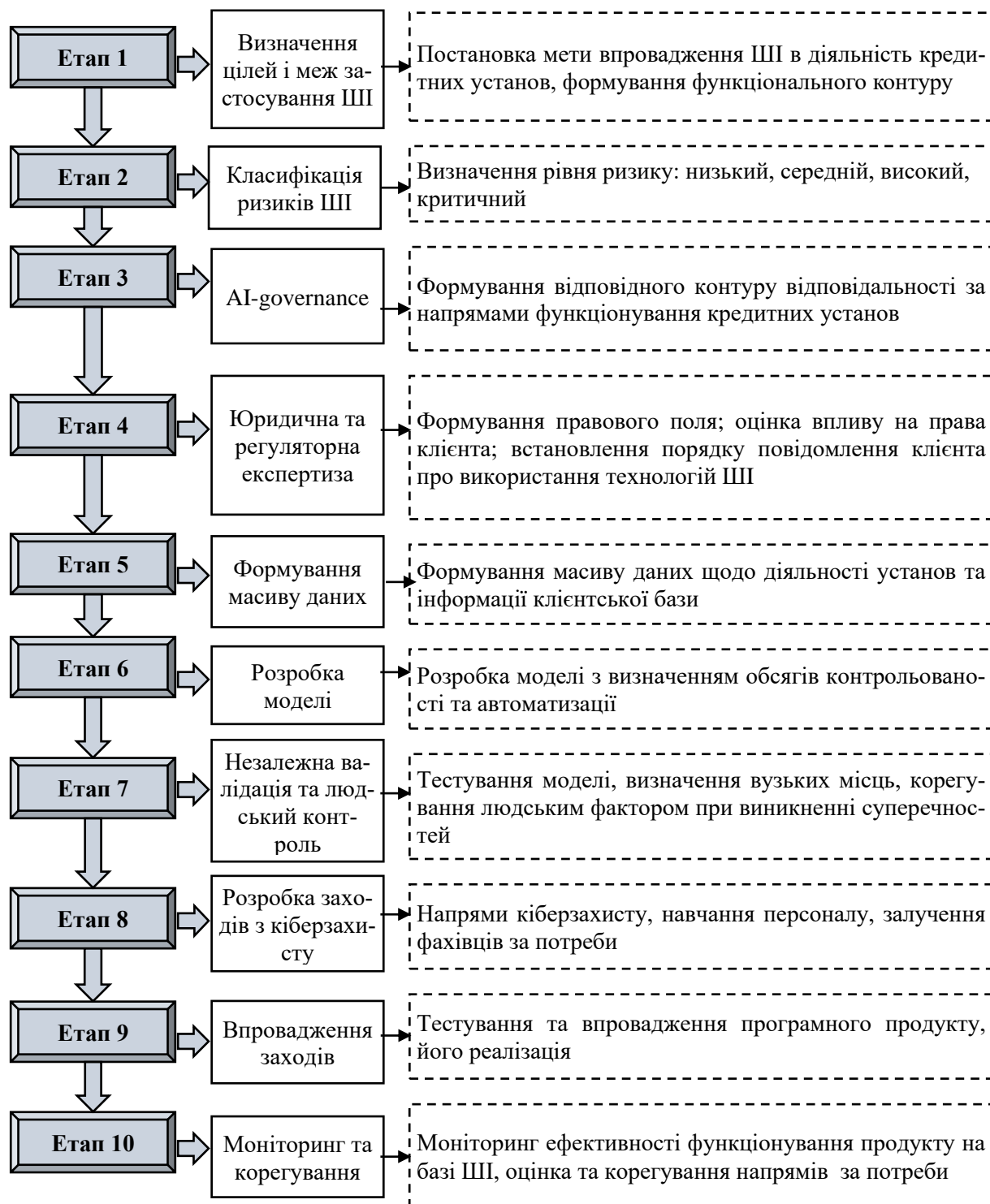


Рис. 3. Етапи мінімізації загроз використання технологій ШІ у діяльності кредитних установ

Джерело: запропоновано авторами.

Оскільки основна мета – захист від ризиків та загроз, то на другому етапі формується класифікація ризиків зовнішнього та внутрішнього характеру для подальшої розробки заходів з їх мінімізації або уникнення. За відповідними критеріями, такими як: ступінь автоматизації прийняття рішень, визначення факторів, які впливають на прийняття кредитного рішення, захист персональних даних, залежність від зовнішніх джерел тощо, визначається ступінь ймовірного ризику.

## ФІНАНСОВІ РЕСУРСИ: ПРОБЛЕМИ ФОРМУВАННЯ ТА ВИКОРИСТАННЯ

На третьому етапі формується система відповідальності за ймовірні ризики, які розподілені за зонами виникнення, розробляється система ризик-менеджменту. Важливим аспектом в діяльності кредитних установ є формування ефективної політики комплаєнсу, що дозволяє мінімізувати більшість ризиків та загроз, визначати відповідальних осіб тощо.

На четвертому етапі визначаються юридично-правові норми здійснення діяльності кредитними установами, права та обов'язки клієнтів з урахуванням особливостей використання цифрових технологій. Також доцільно зазначити, що в умовах євроінтеграції необхідно дотримуватися галузевих вимог, вимог GDPR та AI Act, систем міжнародного ризик-менеджменту. При цьому слід сформулювати політику повідомлення клієнтів про використання технологій ШІ з відповідним захистом персональних даних, щоб в подальшому уникнути юридичних спорів.

Використання цифрових технологій на базі ШІ потребує відповідного аналітичного базису, який є основою для моделювання подальших економічних процесів, які є підґрунтям прийняття управлінських рішень. Від якості та репрезентативності даних буде залежати ефективність прийнятих рішень, які в подальшому впливатимуть на розвиток кредитної установи та її фінансову стабільність. Тому потрібно досить прискіпливо та відповідально ставитися до формування інформаційного простору на базі якого працюють алгоритми в кредитних установах.

На шостому етапі здійснюється розробка самої моделі використання ШІ, яка повинна відповідати вимогам точності та керованості, особливо якщо від рішення залежить значний капітал установи або клієнта. Враховуючи це, на сьомому етапі при валідації моделі потрібно дослідити співвідношення впливу технічних факторів та людського потенціалу в питаннях прийняття рішень щодо кредитування.

Незважаючи на потужний аналітичний інструментарій використання технологій ШІ, досвід та компетентність персоналу може враховувати ймовірність настання загроз в нестандартних ситуаціях функціонування кредитних установ. Тому повна відмова від залучення людського фактору при ухваленні управлінських рішень, попри ефективність цифрових технологій є недоцільною на цьому етапі.

Будь-які цифрові рішення потребують захисту, особливо якщо це стосується персональних даних клієнтів, банківської та комерційної таємниці. Тому розробка та впровадження заходів із кіберзахисту є важливим етапом у діяльності кредитних установ. Для всебічного забезпечення безпеки даних усі працівники повинні володіти навичками поводження з інформацією для мінімізації ризиків та загроз.

Після тестування програмного продукту досліджуються всі ризики та вузькі місця з метою їх корегування, оцінки ймовірності настання негативних сценаріїв. Після усунення всіх недоліків, програмне забезпечення використовується як повноцінний додаток у діяльності кредитних установ. У подальшому воно корегується за результатами моніторингу, який проводиться безперервно. У процесі використання технологій ШІ ризик не зникає, він переходить у фазу drift risk.

Саме тому кредитні установи повинні постійно контролювати зміну клієнтського потоку, частоту помилок, відхилень від встановлених порогових значень в показниках. При цьому слід враховувати не лише внутрішні зміни, але й зовнішнє середовище, яке формує умови функціонування кредитних установ. При настанні змін у зовнішньому середовищі потрібно адаптувати моделі використання ШІ до таких умов для їх коректної роботи.

**Висновки та пропозиції.** Проведене дослідження виокремлення основних загроз використання технологій ШІ в кредитних установах має системний характер. Загрози використання ШІ у функціонування кредитних установ поділено на зовнішні та внутрішні, що дозволяє більш раціонально застосовувати методи щодо їх мінімізації чи уникнення. Впливати на фактори зовнішнього середовища для кредитних установ є проблемним

## ФІНАНСОВІ РЕСУРСИ: ПРОБЛЕМИ ФОРМУВАННЯ ТА ВИКОРИСТАННЯ

питанням, тому до таких ризиків найчастіше вони повинні адаптуватися. Внутрішні загрози є більш контрольованими та залежать від компетентності персоналу та ефективності системи ризик-менеджменту.

Основні ризики використання технологій ШІ в кредитних установах пов'язані з викривленням кредитних рішень, що зумовлені недосконалістю програмного забезпечення, низьким рівнем контрольованості людського фактору, оскільки нестандартні проблемні ситуації не завжди можна вирішити лише машинними рішеннями, без залучення професійного досвіду. Операційні та юридичні ризики, крім фінансових втрат, можуть привести до зниження репутації установи серед клієнтів, що в довгостроковій перспективі загрожує суттєвою втратою активів і прибутку.

Під час управління ризиками використання технологій ШІ в діяльності кредитних установ доцільно враховувати відповідну етапність дій з використання програмного забезпечення та напрямів ризик-менеджменту. Для ефективного впровадження цифрових технологій слід враховувати нормативні, технологічні, людські аспекти, а також розробляти систему контролю та адаптації до мінливих умов зовнішнього середовища. Основна проблематика використання сучасних цифрових рішень у діяльності кредитних установ полягає у збалансуванні залучення технологій та людського фактору.

### Список використаних джерел

1. Данік Н., Торлопов А. Вплив цифрової трансформації на банківський сектор України. *International Science Journal of Management, Economics & Finance*. 2024. Vol. 3, No. 3. Pp. 95-103. DOI: 10.46299/ij.isjmef.20240303.09.
2. Дроботя Я. А., Бражник Л. В. Діджиталізація банківської діяльності та платіжних систем. *Гроші, фінанси і кредит. Інфраструктура ринку*. 2021. Вип. 51. С. 261–267. DOI: <https://doi.org/10.32843/infrastructure51-42>.
3. Дубина М. В., Мурашківська І. А. Сутність та особливості функціонування кредитних установ України в умовах фінансової нестабільності. *Розвиток сфери фінансових послуг в умовах турбулентності національної економіки України* : колективна монографія / за заг. ред. д-ра екон. наук, проф. М. В. Дубини. Чернігів : НУ «Чернігівська політехніка», 2024. С. 7-27.
4. Кльоба Л. Г. Цифровізація – інноваційний напрям розвитку банків. *Ефективна економіка*. 2018. Вип. 12. URL: <http://www.economy.nayka.com.ua/?op=1&z=6741>.
5. Лобко О. М., Дубина М. В., Заєць О. В. Роль штучного інтелекту в стратегічному розвитку системи кредитного менеджменту банку. *Науковий вісник Національної академії статистики, обліку та аудиту*. 2024. №3-4. <https://irb.nasoa.edu.ua/server/api/core/bitstreams/a51d91ce-ba5e-40b2-851c-3147e14bb6ca/content>.
6. Пантелєєва Н. М. Технології штучного інтелекту в антикризовому управлінні банком. *Науковий вісник Херсонського державного університету. Сер.: Економічні науки*. 2019. Вип. 33. С. 193–197. <https://doi.org/10.32999/ksu2307-8030/2019-33-38>.
7. Попело О. В., Дубина М. В. Потенціал використання технології штучного інтелекту в діяльності кредитних установ. *Актуальні проблеми розвитку економіки регіону*. 2024. Вип. 20. Т. 2. DOI: <https://doi.org/10.15330/apred.2.20.232-244>.
8. Про затвердження Положення про порядок застосування технології хмарних обчислень та внесення зміни до Положення про організацію бухгалтерського обліку в банках України : Постанова Правління Національного банку України від 25.08.2025 № 99. URL: <https://zakon.rada.gov.ua/laws/show/v0099500-25#Text>.
9. Про захист персональних даних : Закон України від 01.06.2010 № 2297-VI (зі змінами). URL: <https://zakon.rada.gov.ua/laws/show/2297-17#Text>.
10. Пузирьова П., Ірнараров Д. Особливості інтеграції штучного інтелекту у банківську систему України. *Вчені записки Університету «КРОК»* 2025. №1 (77). DOI: 10.31732/2663-2209-2025-77-66-79.
11. Савіцький Л. М., Безносенко С. Ю., Горбач Р. Я. Концептуальні погляди на побудову системи захисту від кібератак із застосуванням методів штучного інтелекту в інформаційно-комунікаційних системах. *Сучасні інформаційні технології у сфері безпеки та оборони*, 2024. С. 77-85. <https://doi.org/10.33099/2311-7249/2024-49-1-77-85>.

12.Ткачук Н. Діджиталізація фінансово-економічної сфери в Україні: стан та перспективи розвитку. *Економічний часопис Волинського національного університету імені Лесі Українки*. 2022. Вип. 3. С. 18–28. DOI: <https://doi.org/10.29038/2786-4618-2022-03-18-28>.

13.Холявко Н., Садчикова І. Колотюк М. Напрями використання штучного інтелекту в банківських установах. *Проблеми і перспективи економіки та управління*. 2023. С. 192-203. DOI: [https://doi.org/10.25140/2411-5215-2023-2\(34\)-192-203](https://doi.org/10.25140/2411-5215-2023-2(34)-192-203).

14.European Central Bank. The rise of artificial intelligence: benefits and risks for financial stability (05.2024). URL: [https://www.ecb.europa.eu/press/financialstabilitypublications/fsr/special/html/ecb.fsrart202405\\_02~58c3ce5246.en.html](https://www.ecb.europa.eu/press/financialstabilitypublications/fsr/special/html/ecb.fsrart202405_02~58c3ce5246.en.html).

15.Financial Stability Board. Monitoring Adoption of Artificial Intelligence and Related Vulnerabilities in the Financial Sector. URL: <https://www.fsb.org/uploads/P101025.pdf>.

16.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). URL: <http://data.europa.eu/eli/reg/2024/1689/oj>.

17.The Role and Prospects of the Use of Artificial Intelligence Technology in the Credit Activities of Banking Institutions / M. Dubyna et al. *Review of Economics and Finance*. 2023. Vol. 21. URL: <https://refpress.org/ref-vol21-a220/>.

### References

1. Danik, N., & Torlopov, A. (2024). Vplyv tsyfrovoy transformatsii na bankivskyi sektor Ukrainy [The impact of digital transformation on the banking sector of Ukraine]. *International Science Journal of Management, Economics & Finance*, 3(3), 95–103. <https://doi.org/10.46299/j.isjmef.20240303.09>.

2. Drobotia, Ya. A., & Brazhnyk, L. V. (2021). Didzhitalizatsiia bankivskoi diialnosti ta platizhnykh system [Digitalization of banking activities and payment systems]. *Market Infrastructure*, (51), 261–267. <https://doi.org/10.32843/infrastructure51-42>.

3. Dubyna, M. V., & Murashkovska, I. A. (2024). Sutnist ta osoblyvosti funktsionuvannia kredytnykh ustanov Ukrainy v umovakh finansovoi nestabilnosti [The essence and features of the functioning of credit institutions of Ukraine in conditions of financial instability]. In M. V. Dubyna (Ed.), *Rozvytok sfery finansovykh posluh v umovakh turbulentnosti natsionalnoi ekonomiky Ukrainy* (pp. 7–27). Chernihiv Polytechnic National University.

4. Kloba, L. H. (2018). Tsyfrovizatsiia – innovatsiinyi napriam rozvytku bankiv [Digitalization as an innovative direction of bank development]. *Efficient Economy*, (12). <http://www.economy.nayka.com.ua/?op=1&z=6741>.

5. Lobko, O. M., Dubyna, M. V., & Zaiets, O. V. (2024). Rol shtuchnoho intelektu v strateichnomu rozvytku systemy kredytnoho menedzhmentu banku [The role of artificial intelligence in the strategic development of the bank's credit management system]. *Scientific Bulletin of the National Academy of Statistics, Accounting and Audit*, (3-4).

6. Panteleieva, N. M. (2019). Tekhnolohii shtuchnoho intelektu v antykryzovomu upravlinni bankom [Artificial intelligence technologies in anti-crisis management of the bank]. *Scientific Bulletin of Kherson State University. Series: Economic Sciences*, (33), 193–197. <https://doi.org/10.32999/ksu2307-8030/2019-33-38>.

7. Popelo, O. V., & Dubyna, M. V. (2024). Potentsial vykorystannia tekhnolohii shtuchnoho intelektu v diialnosti kredytnykh ustanov [Potential of using artificial intelligence technology in the activities of credit institutions]. *Actual Problems of the Regional Economy Development*, 2(20), 232–244. <https://doi.org/10.15330/apred.2.20.232-244>.

8. National Bank of Ukraine. (2025). *Resolution No. 99: On approval of the Regulation on the procedure for using cloud computing technology and amending the Regulation on the organization of accounting in Ukrainian banks*. <https://zakon.rada.gov.ua/laws/show/v0099500-25>.

9. Law of Ukraine No. 2297-VI. (2010). *Pro zakhyst personalnykh danykh* [On protection of personal data]. <https://zakon.rada.gov.ua/laws/show/2297-17>.

10.Puzryiova, P., & Irnazarov, D. (2025). Osoblyvosti intehratsii shtuchnoho intelektu u bankivsku systemu Ukrainy [Features of artificial intelligence integration into the banking system of Ukraine]. *Scientific Notes of KROK University*, (1), 66–79. <https://doi.org/10.31732/2663-2209-2025-77-66-79>.

11.Savytskyi, L. M., Beznosenko, S. Yu., & Horbach, R. Ya. (2024). Kontseptualni pohliady na pobudovu systemy zakhystu vid kiberatak iz zastosuvanniam metodiv shtuchnoho intelektu v informatsiino-komunikatsiinykh systemakh [Conceptual views on building a cyberattack protection system using artificial intelligence methods in information and communication systems]. *Modern Information Technologies in the Sphere of Security and Defence*, 77–85. <https://doi.org/10.33099/2311-7249/2024-49-1-77-85>.

12.Tkachuk, N. (2022). Didzhytalizatsiia finansovo-ekonomichnoi sfery v Ukraini: stan ta perspektyvy rozvytku [Digitalization of the financial and economic sphere in Ukraine: State and development prospects]. *Economic Journal of Lesya Ukrainka Volyn National University*, (3), 18–28. <https://doi.org/10.29038/2786-4618-2022-03-18-28>.

13.Kholiavko, N., Sadchykova, I., & Kolotiuk, M. (2023). Napriamy vykorystannia shtuchnoho intelektu v bankivskykh ustanovakh [Directions for the use of artificial intelligence in banking institutions]. *Problems and Prospects of Economics and Management*, 192–203. [https://doi.org/10.25140/2411-5215-2023-2\(34\)-192-203](https://doi.org/10.25140/2411-5215-2023-2(34)-192-203).

14.European Central Bank. (2024). *The rise of artificial intelligence: Benefits and risks for financial stability*. [https://www.ecb.europa.eu/press/financialstabilitypublications/fsr/special/html/ecb.fsrart202405\\_02~58c3ce5246.en.html](https://www.ecb.europa.eu/press/financialstabilitypublications/fsr/special/html/ecb.fsrart202405_02~58c3ce5246.en.html).

15.Financial Stability Board. (2025). *Monitoring adoption of artificial intelligence and related vulnerabilities in the financial sector*. <https://www.fsb.org/uploads/P101025.pdf>.

16.European Parliament & Council of the European Union. (2024). *Regulation (EU) 2024/1689 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act)*. <http://data.europa.eu/eli/reg/2024/1689/oj>.

17.Dubyna, M., Bazilinska, O., Panchenko, O., Sadchykova, I., Kozlianchenko, A., & Tarasenko, A. (2023). The role and prospects of the use of artificial intelligence technology in the credit activities of banking institutions. *Review of Economics and Finance*, 21. <https://refpress.org/ref-vol21-a220/>.

Дата першого надходження статті до видання: 02.02.2026

Дата прийняття статті до друку після рецензування: 09.02.2026

УДК 004.89:336.71

### **Olha Popelo**

Doctor of Economic Sciences, Associate Professor,  
Professor of the Department of Management and Administration  
Chernihiv Polytechnic National University (Chernihiv, Ukraine)  
E-mail: [popelo.olha@gmail.com](mailto:popelo.olha@gmail.com). ORCID: <https://orcid.org/0000-0002-4581-5129>

### **Serhii Kononenko**

Junior Research Associate,  
Chernihiv Polytechnic National University (Chernihiv, Ukraine)  
E-mail: [job.s.kononenko@gmail.com](mailto:job.s.kononenko@gmail.com). ORCID: <https://orcid.org/0000-0002-1898-2204>

## **MAIN THREATS OF THE USE OF ARTIFICIAL INTELLIGENCE TECHNOLOGIES AND THEIR POTENTIAL NEGATIVE IMPACT ON THE OPERATION OF CREDIT INSTITUTIONS**

*The features of the implementation of artificial intelligence technologies in the activities of credit institutions are studied. The need to balance the use of such technologies and human labor in the activities of credit institutions when making management decisions is substantiated. The importance of preserving personal data of clients is determined, which affects the reputation and financial stability of the institution. The main types of threats that arise when using AI technologies in the activities of credit institutions are identified. An algorithm for managing the use of artificial intelligence technologies in the activities of credit institutions is proposed. It is studied that the threats of using AI in the functioning of credit institutions can be divided into external and internal, which allows for more rational application of methods for their minimization or avoidance. It is emphasized that influencing external environmental factors for credit institutions is a more problematic issue, therefore, credit institutions most often have to adapt to such risks. It is established that internal threats are more controllable and depend on the competence of personnel and the effectiveness of the risk management system. It was analyzed that the main risks of using*

---

**ФІНАНСОВІ РЕСУРСИ: ПРОБЛЕМИ ФОРМУВАННЯ ТА ВИКОРИСТАННЯ**

---

*AI technologies in credit institutions are associated with the distortion of credit decisions, which arise due to software imperfections, low level of controllability of the human factor; since non-standard problem situations cannot always be solved only by machine solutions, without involving professional experience. Operational and legal risks, in addition to financial losses, can lead to a decrease in the institution's reputation among clients, which in the long term threatens with a significant loss of assets and profits. It was established that to manage the threats of using AI technologies in the activities of credit institutions, it is advisable to take into account the appropriate phasing of actions for implementing software and risk management areas. It was proven that the integration of AI technologies into the activities of credit institutions is generally a promising direction that contributes to more effective management of financial risks, however, for their effective implementation, regulatory, technological, human aspects should be taken into account, as well as a system of control and adaptation to changing environmental conditions should be developed.*

**Keywords:** digitalization; credit institutions; threats; technologies; artificial intelligence; digital technologies.

**Fig.:** 3. **References:** 17.