

МІНІСТЕРСТВО ВНУТРІШНІХ СПРАВ УКРАЇНИ
ЛЬВІВСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ ВНУТРІШНІХ СПРАВ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ УПРАВЛІННЯ,
ПСИХОЛОГІЇ ТА БЕЗПЕКИ
Кафедра менеджменту та економічної безпеки

ІНТЕГРАЦІЯ ШТУЧНОГО ІНТЕЛЕКТУ В СИСТЕМУ БЕЗПЕКОВОГО
МЕНЕДЖМЕНТУ БАНКУ

кваліфікаційна робота
здобувачки вищої освіти
4 курсу заочної форми навчання
Любові КАРХУТ

Науковий керівник:
кандидат економічних наук, доцент
Володимир ГОБЕЛА

Рецензент:
доктор економічних наук, професор
Галина ЛЕВКІВ

Кваліфікаційна робота допущена до захисту

«___» _____ 20__ р., протокол № _____

Завідувач кафедри менеджменту

та економічної безпеки

_____ Марта КОПИТКО

Львів
2025

АНОТАЦІЯ

КАРХУТ Л. В. Інтеграція штучного інтелекту в систему безпекового менеджменту банку. – Рукопис.

Дослідження на здобуття освітнього ступеня бакалавр за спеціальністю 073 «Менеджмент», Львів. 2025.

У першому розділі кваліфікаційної роботи досліджено теоретичні засади формування безпекового менеджменту банку. У другому розділі здійснено загальну характеристику АТ «Укрсиббанк» та його безпекового менеджменту. На основі результатів аналізу розроблено рекомендації щодо удосконалення безпекового менеджменту шляхом інтеграції штучного інтелекту.

Ключові слова: менеджмент, безпека, штучний інтелект, ризики, загрози.

ANNOTATION

KARKHUT L. V. Integration of artificial intelligence into the bank's security management system. – The manuscript.

Study on obtaining the educational bachelor degree in specialty 073 «Management». Lviv, 2025.

The first section of the qualification work examines the theoretical foundations of the formation of bank security management. The second section provides a general description of JSC "Ukrsibbank" and its security management. Based on the results of the analysis, recommendations were developed for improving security management through the integration of artificial intelligence.

Keywords: management, security, artificial intelligence, risks, threats.

ЗМІСТ

ВСТУП	4
РОЗДІЛ 1. ТЕОРЕТИЧНІ ЗАСАДИ ОРГАНІЗАЦІЇ БЕЗПЕКОВОГО МЕНЕДЖМЕНТУ БАНКУ	6
1.1. Система економічної безпеки банку як об'єкт теоретичного аналізу	6
1.2. Тенденції використання штучного інтелекту в банківських установах	11
Висновки до першого розділу	22
РОЗДІЛ 2. ЗАГАЛЬНА ХАРАКТЕРИСТИКА АТ «УКРСИББАНК» ТА СИСТЕМИ БЕЗПЕКОВОГО МЕНЕДЖМЕНТУ	25
2.1. Загальна характеристика АТ «УКРСИББАНК»	25
2.2. Аналіз фінансової діяльності АТ «УКРСИББАНК»	31
2.3. Пропозиції щодо інтеграції штучного інтелекту в безпековий менеджмент АТ «Укрсиббанк»	37
Висновки до другого розділу	43
ВИСНОВКИ	46
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ	48

ВСТУП

Обґрунтування актуальності теми дослідження. Сучасна економічна ситуація в Україні, потенційні труднощі, зумовлені пандемією та військовими діями з боку росії, а також зростаюча фінансова нестабільність на міжнародному рівні, суттєво впливають на банківські установи країни. Це може призвести до проблем з прибутковістю, фінансовою стабільністю і ліквідністю. Операційна діяльність банків в значній мірі залежить від зовнішніх факторів, які викликають значний вплив з боку навколишнього середовища. Усі чинники, які впливають на функціонування банку, вимагають від керівництва обґрунтованих та ефективних рішень, а також розробки фінансової політики та інвестиційних стратегій. Це підкреслює значущість фінансового планування для забезпечення стабільної діяльності банківських установ. Тому організація безпекового менеджменту банку є важливим аспектом теоретико-прикладних досліджень.

Актуальність зазначених питань спонукала вибір теми кваліфікаційної роботи і визначила її мету, завдання та зміст.

Аналіз останніх досліджень за тематикою проблеми. Низка науковців займалася дослідженнями у царині безпекового менеджменту банку, серед них зокрема: Башнянин Г. І., Болгар Т. М., Брежнєва-Єрмоленко О. В., Буйда К. П., Вдовенко Л. О., Вовчак О. Д., Гобела В. В., Добровольська О. В., Житар М. О., Зачосова Н. В., Калусенко В. В., Кльоба Л. Г., Коваленко В. В., Крупка І. М., Франчук В. І., незважаючи на посилену увагу до згаданої тематики низка проблем залишилася малодослідженою, зокрема формування системи безпекового менеджменту у сучасних умовах.

Мета дослідження. Мета дослідження полягає у формуванні теоретико-прикладних засад організації безпекового менеджменту в банку.

Завдання дослідження. Реалізація мети дослідження потребувала встановлення низки завдань дослідження, а саме:

- проаналізувати теоретичні засади організації безпекового менеджменту в банку;

- здійснити загальну характеристику АТ «Укрсиббанк»;
- розробити пропозиції щодо удосконалення безпекового менеджменту на АТ «Укрсиббанк».

Об’єктом дослідження є система безпекового менеджменту банку.

Предметом дослідження є теоретико-прикладні аспекти удосконалення безпекового менеджменту банку.

Перелік методів дослідження. У кваліфікаційній роботі застосовувались такі загальнонаукові методи дослідження: методи теоретичного та критичного аналізу, синтезу, статистичні методи, графічний метод, методи індукції та дедукції, теоретичного узагальнення тощо.

Інформація про практичне значення роботи, апробацію результатів дослідження (їх впровадження на підприємстві чи організації, участь у науково-практичних конференціях, публікації). Кваліфікаційна робота становить певну практичну цінність, адже запропоновані рекомендації сприятимуть удосконаленню безпекового менеджменту, що позитивно вплине на функціонування АТ «Укрсиббанк».

Структура та обсяг роботи. Кваліфікаційна робота складається із анотації українською та англійською мовами, вступу, двох розділів, висновків, списку використаних джерел (43 найменування на 5 сторінках). Загальний обсяг роботи становить 52 сторінки, із них основний текст – 42 сторінки, які містять 10 рисунків та 6 таблиць.

РОЗДІЛ 1

ТЕОРЕТИЧНІ ЗАСАДИ ОРГАНІЗАЦІЇ БЕЗПЕКОВОГО МЕНЕДЖМЕНТУ БАНКУ

1.1. Система економічної безпеки банку як об'єкт теоретичного аналізу

Сьогодні, в умовах проведення активної фази війни в Україні, фінансова стабільність банків є надзвичайно важливою для руху капіталів. Банки вступили в пандемію без значних дисбалансів, маючи достатній капітал та високу ліквідність, що дозволяє їм продовжувати кредитування для населення, малих і середніх підприємств, а також великого бізнесу. Унікальною для цього періоду є те, що українські банки не тільки не погіршили економічної ситуації, але й підтримували бізнес, що сприятиме відновленню економічного зростання в майбутньому через надання кредитів. Під час розгортання соціально-економічної кризи більшість з цих установ швидко адаптувалися до онлайн-формату роботи [2].

Сучасні вітчизняні банківські організації стикаються з нестійкістю як зовнішніх, так і внутрішніх умов, що обумовлено збільшенням кількості ризиків і загроз, які можуть загрожувати економічній стабільності кредитних закладів. На особливу увагу заслуговує проблема забезпечення надійності роботи банків, особливо під час поширення фінансових криз у світі. Однією з ключових причин таких криз є неточна оцінка ризиків і недостатній рівень контролю та регулювання у банківському секторі.

Економічна стабільність банків є важливою частиною національної безпеки держави, впливаючи значною мірою на формування економічної стратегії. У цьому контексті, захист банківських установ перетворюється на окремий вид діяльності, який вимагає належного правового оформлення та керованості.

Отже, після детального вивчення та аналізу думок різних вітчизняних і зарубіжних науковців про визначення терміну "економічна безпека банківської установи", можна зробити висновок, що єдиного підходу до визначення цього

поняття в сучасній науці не існує. Проте можна виділити такі підходи до його розгляду:

- системний підхід, що описує безпеку банків з точки зору реалізації інтересів, їх захисту, здатності протистояти загрозам та дезактивувати їх, стабільності і ефективного прогресу [7];
- процесно-функціональний підхід показує здатність банку, як суб'єкта економіки, ефективно виконувати свої функції в умовах зовнішніх та внутрішніх деструктивних впливів [9];
- економічна ефективність як здатність банківської установи отримувати економічні вигоди, забезпечувати стабільні фінансові потоки, досягати позитивних фінансових результатів та збільшувати цінність банківського бізнесу, незважаючи на загрози [11];
- ресурсна спроможність і захищеність полягають у здатності збільшувати ресурсний потенціал завдяки сталому "довірчому кредиту" з боку акціонерів, вкладників і кредиторів [15];
- збалансованість та самовідтворення з акцентом на гармонійний розвиток [16];
- комплексний (системний) підхід підкреслює важливість врахування всіх елементів, що формують основу економічної безпеки банків [19];
- конкурентоспроможність розглядається через здатність до реалізації можливостей та переваг для нейтралізації загроз і ризиків [21];
- превентивність та кризостійкість як здатність формувати ресурсний потенціал і здійснювати фінансові, операційні й інвестиційні дії на основі прогнозування та запобігання кризам і загрозам [26];
- стратегічна орієнтація, що служить основою для формування перспективних ресурсних можливостей для запобігання негативним проявам у майбутньому [27];
- ризик-орієнтованість, яка забезпечує динамічний розвиток через управління ризиками [33].

Однією з основних проблем, що постають перед сучасними банками, є те, що питання забезпечення економічної безпеки зазвичай піднімається лише тоді,

коли уникнути загрози вже неможливо. Тому важливо регулярно відстежувати як зовнішні, так і внутрішні фактори, що впливають на фінансову стабільність банку, для швидкої реакції на можливі виклики. Під час цього моніторингу виявляються ризики ззовні та зсередини. Зовнішні загрози включають несприятливі зміни на фінансових ринках, втрату довіри клієнтів та недостатнє регулювання банківської сфери. Внутрішні виклики пов'язані з неефективністю фінансового менеджменту та рівнем компетентності керівництва та співробітників, що призводить до слабого управління та безпекового менеджменту зокрема [34].

Ефективне забезпечення економічної безпеки банку спирається на вчасне виявлення як зовнішніх, так і внутрішніх загроз. Для їх запобігання важливими є посилення державного нагляду у банківському секторі, впровадження інноваційних методів та технологій для аналізу та обробки даних задля оцінки фінансової стійкості, а також належний контроль фінансів як за ресурсами, так і за роботою співробітників. Ці стратегії мають бути розроблені таким чином, щоб досягти мети з найменшими витратами ресурсів і часу [3].

Основною метою контролю в будь-якому процесі є виявлення відхилень від запланованих показників та вжиття заходів для покращення ситуації. У межах системи банківської безпеки здійснюються два типи контролю [35]. Поточний контроль фокусується на аналізі фактичних результатів, тоді як підсумковий контроль оцінює ефективність впроваджених заходів для забезпечення фінансової стабільності. Моніторяться такі показники, як ліквідність банку, рівень проблемних кредитів, адекватність капіталу та загальна валютна позиція. Результати контролю дозволяють оцінити стан інвестиційної безпеки й результативність зусиль, спрямованих на її підвищення. Варто відзначити науково-методичний підхід [39], який пропонує традиційно розділяти загрози безпеці банку на внутрішні і зовнішні (таблиця 1.1).

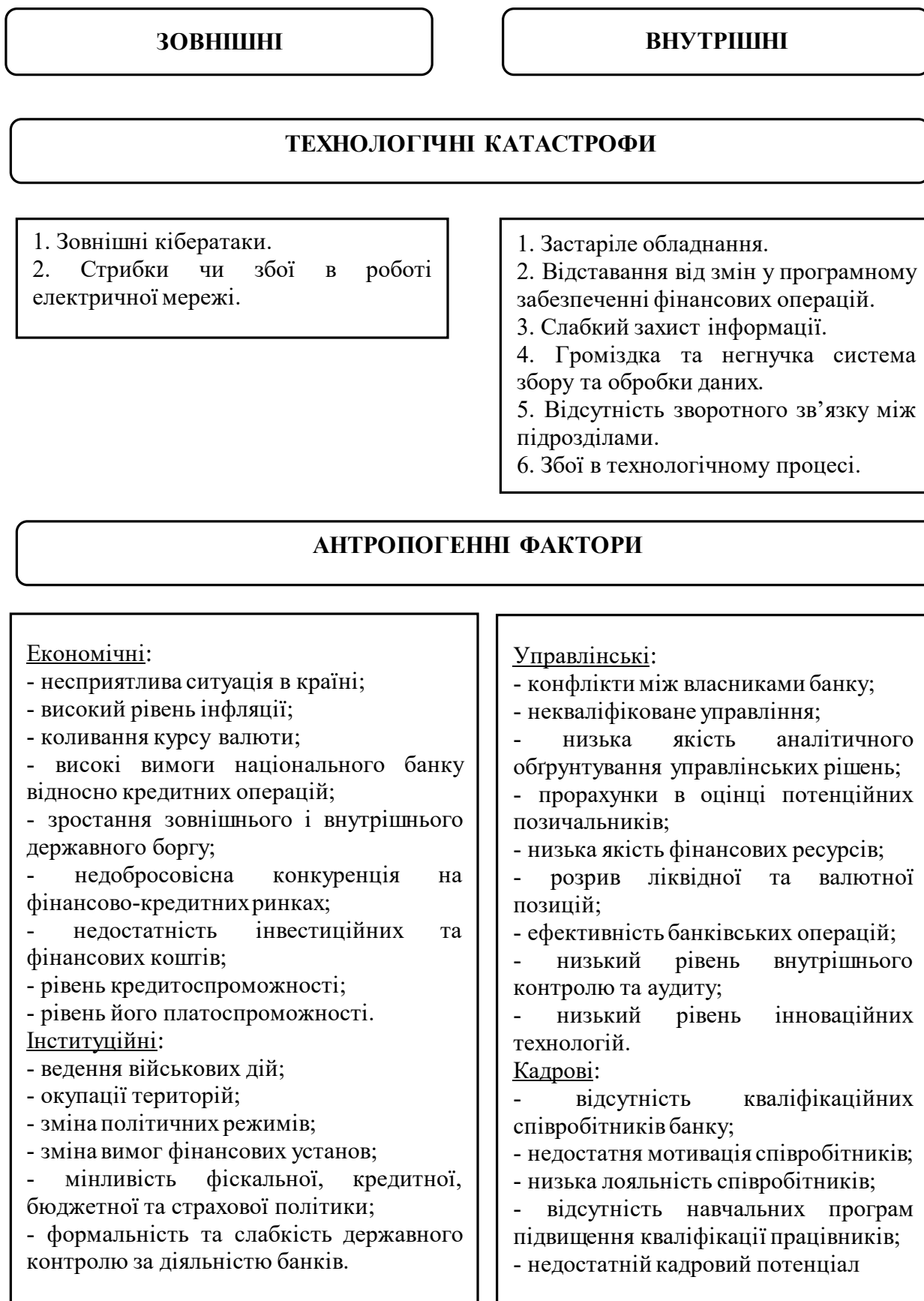


Рис. 1.1. Класифікація загроз безпеці банку

Джерело: [14; 42].

У результаті проведеного структурного аналізу цих загроз для комерційного банку була виконана їх класифікація. Загрози для фінансової безпеки можна класифікувати як суб'єктивні та об'єктивні. Об'єктивні причини охоплюють явища, що виникають раптово й несподівано, як-то природні катастрофи чи пандемії. Згідно з [13], "Об'єктивні причини є чинниками, які впливають на суспільство і діяльність людей, але їх не можна передбачити чи прогнозувати, як наприклад, інфляцію, банкрутство чи кібератаки" [10].

Особливість загроз для фінансової стабільності банку полягає в тому, що вони можуть бути конкретними, з чіткою ймовірністю виникнення, що збільшує ризики та дозволяє їх кількісно оцінити, або потенційними, які фактично не матеріалізуються. Наприклад, чутки про можливе злиття, встановлення державного контролю над банком чи прийняття суворого законопроекту можуть викликати паніку серед клієнтів і вкладників, спричиняючи коливання на ринках капіталу та призводячи до негативних наслідків, подібних до тих, що викликають реальні загрози.

При аналізі ризиків, пов'язаних з безпекою банків, важливо враховувати сучасні тенденції у фінансовій сфері. Загрози постійно еволюціонують, які розширюються і змінюються, при цьому з'являються нові виклики. Нестача ресурсів посилює вимоги клієнтів, у той час як впровадження нових технологій та аналітичних інструментів призводить до зростання ризиків. Тому кожен банк зобов'язаний розробити детальну стратегію, яка фокусується на поліпшенні процесів виявлення, класифікації, прогнозування й профілактики можливих загроз. Також слід впровадити систему, що включає: автоматизацію ухвалення рішень з обмеженою участю людини, використання сучасних аналітичних моделей, ефективну та гнучку співпрацю з клієнтами, а також адаптацію до змін у регуляторному середовищі та потенційних загроз з боку конкурентів і злочинців.

Основною метою комерційного банку при реалізації системи безпекових заходів є створення позитивного іміджу надійного фінансового інституту. Водночас для Національного банку України критично важливо відновити довіру до всього банківського сектора. Питання взаємозв'язку між

інструментами безпеки, а також корекція фінансових показників і результатів банківської діяльності залишаються важливими і потребують подальшого дослідження [20].

Прогнозування тривалості економічної кризи, що виникла через пандемію COVID-19, стало досить складним завданням для багатьох аналітиків. Проте, більшість міжнародних експертів доходять до єдиного висновку, що світові фінансові ринки очікують рецесію, яка може бути порівняна не лише з фінансовою кризою 2008 року, але й з глобальною депресією. За їхнім аналізом, пандемія викликала найшвидший та найзначніший економічний спад в історії, а наслідки коронавірусу залишатимуться відчутними протягом кількох десятиліть. Додатковим каталізатором для посилення цієї кризи стала війна Росії проти України, оскільки повномасштабне вторгнення 2022 року стало ще одним вагомим чинником кризових проявів не лише в Європі, але й по всьому світу.

Отже, можна зробити висновок, що "зовнішні загрози" відіграють вирішальну роль у підриві інвестиційної безпеки фінансових установ, що, в свою чергу, негативно впливає на фінансову інфраструктуру та економічну ситуацію в країні. Тривалість таких загроз може призвести до економічної кризи як для окремих фінансових установ, зокрема комерційних банків, так і для глобальної економіки в цілому [22].

Згідно з висновками експертів МВФ, у період 2022-2024 рр. пандемія COVID-19 та війна суттєво вплинула на економічну активність, і очікується, що процес відновлення буде відбуватися повільніше, ніж передбачалося раніше.

1.2. Тенденції використання штучного інтелекту в банківських установах

НТП (науково-технічний прогрес) постійно трансформує життя людей, перетворюючи окремі предмети, види діяльності, професії та цілі економічні сектори на щось застаріле і нерелевантне. Завдяки інноваціям змінюються методи виробництва товарів і послуг, попереднє розподілення професій у

суспільстві, а також структура економік багатьох країн. Наприклад, сто років тому мало хто міг уявити собі кар'єри в сферах ІТ, дизайну чи маркетингу, оскільки тодішній рівень споживання не вимагав таких професій. Сьогодні ж важко уявити людину, яка вручну добуває каміння для будівництва, хоча на початку 20 століття така праця на каменоломнях була звичною в Європі та світі.

Сучасні технології вимагають впровадження штучного інтелекту для оптимізації роботи людей. З одного боку, це дуже зручно — зникає потреба виконувати важку, неприємну та часто небезпечну роботу самостійно. З іншого боку, автоматизація усіх сфер діяльності піднімає питання, які професії зникнуть і які функції можуть бути замінені роботами або штучним інтелектом [42].

На рисунку 1.2 представимо графічно розподіл сфер за популярністю використання штучного інтелекту. Варто зауважити, що лідируючі позиції в плані застосування штучного інтелекту займають сфери інформаційних технологій, а також банківський сектор і сфера маркетингової діяльності.

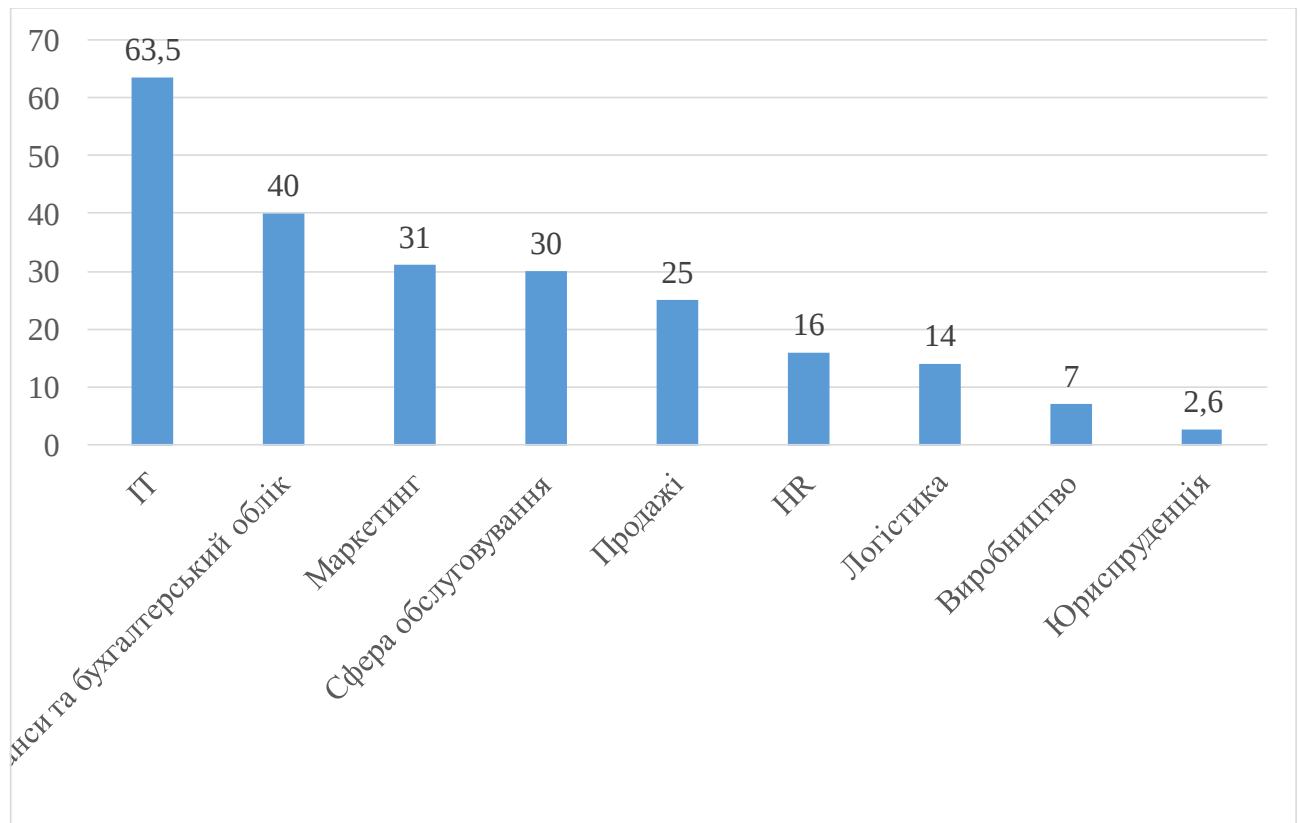


Рис. 1.2. Сфери застосування штучного інтелекту

Джерело: [25].

В Україні процес автоматизації в банківській сфері спостерігався вже досить давно. Наприклад, коли клієнт звертається до служби підтримки або на гарячу лінію свого банку, він часто чує голос автоматизованої системи, яка ставить питання для уточнення сутності запиту. Якщо виникають серйозні проблеми, запит перенаправляється до живого консультанта [29].

Ця новаційність принесла чималі переваги, такі як звільнення працівників від рутинних запитів і зниження їх навантаження. Проте, вона також має певні недоліки; наприклад, клієнти повинні чітко формулювати свої питання, що не завжди вдається через недостатнє знання банківських процесів [23]. У результаті, рекомендації, які надавалися ботами, часто виявлялися хибними або неточними, що ускладнювало задоволення запитів клієнтів. На рисунку 1.3 представлені очікування банків щодо впровадження чат-ботів у своїй діяльності.

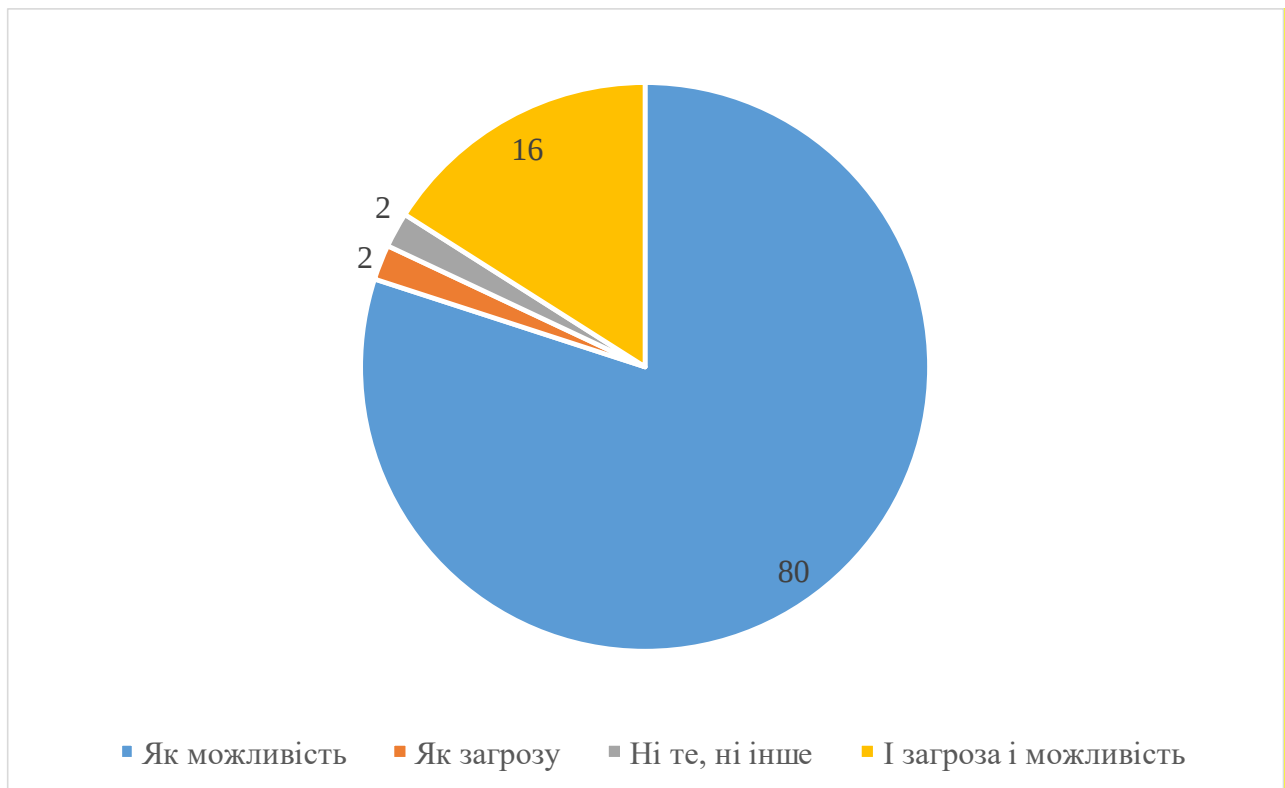


Рис. 1.3. Ставлення до штучного інтелекту фахівцями банківської сфери
Джерело: [29].

Таким чином, 80% фінансових установ по всьому світу вважають чат-ботів чудовою можливістю для підвищення бізнес-ефективності. Лише 16% сприймають чат-ботів як одночасно загрозу і можливість, тоді як всього 2%

вважають, що вони можуть нести ризик для бізнесу, створюючи загрозу злочинного доступу до важливих даних.

Однак інтеграція штучного інтелекту в банківську сферу не обмежується лише впровадженням роботів у службах підтримки. Важливо зазначити також мобільні програми, які використовують сучасні інформаційні технології для збору та аналізу індивідуальних фінансових даних, що сприяє підвищенню якості та швидкості обслуговування клієнтів.

Серед компаній, які використовують штучний інтелект для оцінки вражень банківських клієнтів та покращення їх фінансового досвіду, можна виділити [39; 40]:

- Kasisto, яка розробила платформу KAI, що слугує розмовним інтерфейсом AI, покращуючи взаємодію з клієнтами в банківській індустрії. KAI допомагає зменшити тягар на колл-центри, надаючи можливості для самообслуговування, а чат-боти з елементами штучного інтелекту пропонують фінансові поради і допомагають у щоденних фінансових справах.

- Abe AI, що виступає в ролі віртуального фінансового асистента, інтегрується з Google Home, SMS, Facebook, Amazon Alexa, а також веб- і мобільними платформами, надаючи клієнтам зручні можливості для банківського обслуговування. Цей асистент пропонує різноманітні послуги — від простих запитів до особистого фінансового управління, моніторингу витрат і бюджету.

У 2016 році компанія «Abe» представила розумного фінансового чат-бота, який допомагає користувачам складати бюджет, визначати цілі заощаджень і контролювати витрати.

- Trim — це помічник, що сприяє економії коштів, підключаючи облікові записи користувачів і аналізуючи їх витрати. Цей інноваційний сервіс може скасувати підписки, що забирають надмірні кошти, знаходити вигідні пропозиції для скасованих послуг, таких як страхування, а також вести переговори за рахунками. Trim уже допоміг своїм клієнтам заощадити понад 20 мільйонів доларів США.

Крім того, штучний інтелект підтримує фінансові установи у запобіганні кіберзагрозам і виявленні шахрайських дій — це вже стало критично важливим для кожного банку. Також штучний інтелект відіграє ключову роль у підвищенні рівня безпеки онлайн-фінансів, оскільки щодня відбувається безліч онлайн-транзакцій, під час яких користувачі переміщують кошти між рахунками, оплачують рахунки через смартфони або здійснюють покупки в Інтернеті.

Серед компаній, що забезпечують кібербезпеку великих фінансових установ з використанням штучного інтелекту, можна виділити:

- Vectra, яка розробила платформу для виявлення кіберзагроз, що застосовує штучний інтелект. Цей сервіс автоматизує процес виявлення загроз, ідентифікує непомітних зловмисників, які спеціально націлені на фінансові організації, прискорює розслідування інцидентів і навіть виявляє скомпрометовані дані.

- Платформа KYX компанії Jumio допомагає бізнесам встановлювати довіру з онлайн-клієнтами. Вона здійснює перевірку особистості клієнтів за допомогою технології розпізнавання облич та перевіряє їх на відповідність фінансовим вимогам, постійно оцінюючи ризики. Окрім того, платформа проводить аналіз ідентифікації існуючих клієнтів, використовуючи біометричну автентифікацію та моніторинг фінансових операцій.

- Платформа F5 активно використовується провідними банківськими установами у США. Зазначена фірма розробила рішення для захисту даних, цифрової трансформації та запобігання шахрайству.

- Система машинного навчання Darktrace аналізує мережеві дані та формує прогнози на основі ймовірності, виявляючи підозрілу активність до завдання шкоди найбільшим фінансовим установам у світі.

- FIS надає різноманітні рішення для банківського та фінансового сектору. Одним із інструментів на основі штучного інтелекту є центр відповідності загрозам з програмним забезпеченням C3 AI, який допомагає компаніям на ринку капіталу боротися з фінансовими злочинами. Ця платформа, що використовує машинне навчання, агрегує та аналізує клієнтські дані з різних

систем для оптимізації фінансових процесів. Крім того, FIS має рішення під назвою FIS Credit Intelligence для кредитного аналізу, яке використовує СЗ AI та технології машинного навчання для збору і оцифрування фінансових даних, надаючи інформацію про відповідність та характеристики специфічних угод у практично реальному часі [28; 30].

Завдяки штучному інтелекту та вдосконаленій аналітиці банки мають можливість зменшити ризик прострочення кредитних платежів споживачами. Фінансові установи активно взаємодіють з клієнтами, щоб запобігти простроченням і полегшити виплату кредитів у разі виникнення труднощів. Алгоритми штучного інтелекту можуть аналізувати як внутрішні, так і зовнішні джерела інформації, формуючи комплексний моніторинг фінансового стану клієнтів. Штучний інтелект дозволяє банкам брати до уваги не лише кредитну історію, але й інші фактори для оцінки кредитоспроможності позичальників.

Він здатний враховувати такі аспекти, як поведінкові звички клієнта щодо купівлі валюти та його активність в Інтернеті, щоб оцінити, як ефективно людина управляє своїми фінансами. Це означає, що деякі особи, яких раніше не допускали до кредитування через незначні прострочення минулих платежів, можуть отримати кредит, і навпаки [5; 31].

Крім того, завдяки автоматизації процесів можна значно пришвидшити схвалення кредитів, що позитивно вплине на лояльність банківських споживачів, а також надасть банкам можливість звільнити більше ресурсів для маркетингових кампаній як в онлайн, так і в офлайн форматах, залучаючи нових потенційних клієнтів.

Компанії, які використовують штучний інтелект у кредитуванні:

- Enova впроваджує штучний інтелект та машинне навчання на своїй кредитній платформі, щоб надати розширені фінансові аналітичні та кредитні оцінки споживачів. Компанія намагається обслуговувати малий бізнес і допомагати вирішувати актуальні проблеми, такі як надмірні витрати та відсутність банківських кредитів для малих підприємств.

- Ocrolus пропонує програмне забезпечення для обробки документів, яке поєднує машинне навчання з людською перевіркою.

Програма дозволяє компаніям, організаціям та фізичним особам прискорити та підвищити точність аналізу фінансових документів. Програмне забезпечення від Ocrolus здійснює аналіз банківських виписок, квитанцій про оплату, податкових документів, форм по іпотеці тощо, щоб оцінити право на отримання кредиту в сферах іпотечного кредитування, комерційного кредитування та споживчого кредитування.

– Zest AI є платформою для андеррайтингу на базі штучного інтелекту, яка допомагає компаніям оцінювати позичальників практично без кредитної інформації чи історії. Платформа використовує тисячі точкових даних і забезпечує прозорість, що дозволяє кредиторам краще оцінювати клієнтів, які можуть вважатися «ризиковими».

– Сервіс Socure розробив платформу ID+ для перевірки особи, яка використовує машинне навчання та штучний інтелект для аналізу даних з онлайну, офлайну і соціальних мереж заявника, що допомагає клієнтам відповідати суворим вимогам щодо перевірки клієнтів [6].

Впровадження штучного інтелекту дозволяє не тільки зекономити час і кошти, але й збільшити прибутки фінансових установ. Згідно з дослідженням Tata Consultancy Services (TCS), керівники банківського сектору зазначили, що інвестиції в штучний інтелект допомогли зменшити операційні витрати на 13%.

Крім того, вони відзначили збільшення середнього прибутку на 17% завдяки ініціативам впровадження штучного інтелекту [20].

Однак, крім економічних вигод та інвестицій, галузі слід звернути увагу на вплив ШІ на ринок праці. Керівники банків, які брали участь в опитуванні TCS, вказали, що інвестиції в штучний інтелект можуть привести до створення нових вакансій. Компаніям знадобиться формувати нові посади для управління і розвитку цих технологій, що вимагатиме нових навичок та підходів. У 2015 році застосування штучного інтелекту призвело до зростання кількості робочих місць у банківських відділеннях в середньому на 10%, у 2020 році — до 13%, а за прогнозами, до 2025 року цей показник зросте до 16% [29; 35].

У таблиці 1.1 представлені сфери банківської діяльності, в яких на сьогодні активно застосовується штучний інтелект. Детальніше проаналізуємо специфіку використання ШІ у цих сферах.

Таблиця 1.1.

Напрями використання технологій штучного інтелекту в банку

Напрямок використання штучного інтелекту	Особливості використання
Кібербезпека	Захист конфіденційних даних банківських установ з метою застереження витоку інформації через хакерські атаки
Чат-боти	Забезпечують цілодобовий доступ користувачів до відповідного банку. Також така технологія дає змогу зрозуміти характер клієнта та його потреби
Кредитні рішення	Системи штучного інтелекту на основі яких банк має змогу приймати більш інформаційно забезпечені, вигідні та безпечні кредитні рішення
Аналіз тенденцій ринку	Можливість обробки великих масивів даних, що дозволить прогнозувати ринкові тенденції, валюти, акції тощо та запропонувати вигідні варіанти для інвестицій
Збір та аналіз даних	Рішення на основі штучного інтелекту дають можливість зібрати та структурувати інформацію без помилок
Аналіз досвіду клієнтів	Аналізуючи досвід клієнтів, банки можуть впроваджувати нові успішні послуги для клієнтів
Управління ризиками	Штучний інтелект дає змогу визначити ризиковану пропозицію та запропонувати сучасні та ефективні рішення
Відповідність нормативним вимогам	Штучний інтелект використовується для кращого впровадження нових вимог відповідності для фінансових установ
Автоматизація процесів	Алгоритми роботизованої автоматизації процесів підвищують операційну ефективність і точність, а також знижують витрати за рахунок автоматизації завдань, що повторюються, забирають багато часу

Джерело: [29].

Фінансова система Сполучених Штатів, що є однією з найбільш розвинених економік світу, привертає увагу численних дослідників та економістів. При більш детальному вивченні банківського сектора США за останні десять років помітно значний обсяг інвестицій;

Конкурентоспроможні американські банки, які фокусуються на своєму розвитку, все частіше запроваджують рішення на основі штучного інтелекту у своїй практиці [18].

У 2023 році видання McKinsey's AI Playbook повідомило, що завдяки програмним рішенням на основі штучного інтелекту фінансові технології можуть отримати до 1 трильйона доларів США додаткової вартості. Також, JPMorgan Chase передбачає, що банківський сектор може досягти додаткових 1,5 мільярда доларів США прибутку від впровадження штучного інтелекту до кінця 2023 року.

На рисунку 3 представлена інфографіка, яка демонструє сфери, в яких банківська система США використовує технології штучного інтелекту. Таким чином, майже половину банківських ризиків у США оцінює саме штучний інтелект:

- 45% — у фінансовому аналізі;
- 37% — в управлінні інвестиціями;
- 33% — у торгівлі;
- 29% — у кредитуванні.

Цей обсяг робіт також автоматизовано в американських фінансових установах. Яскравим прикладом інтеграції ШІ у банківську систему США є технологічний чат-бот «Erica», впроваджений компанією «Bank of America». Цей віртуальний асистент щорічно обробляє в середньому до 50 мільйонів запитів і виконує ряд операцій на прохання клієнтів, таких як: надсилання сповіщень про транзакції по картах, пошук потрібних операцій у історії транзакцій, перевірка залишків на рахунках та надсилання нагадувань про заплановані платежі [17].

В сучасних умовах багато функцій у сфері банківської діяльності замінив штучний інтелект, перелік функціоналу заміненого ІІ у США наведено на рисунку 1.4.



Рис. 1.4. Функції у сфері банківської діяльності, які замінив ІІ

Джерело: [36].

Хоча існує безліч позитивних аспектів, які були раніше згадані, впровадження штучного інтелекту в діяльність банків може нести суттєві ризики. Зокрема, безпека даних може стати серйозною проблемою, оскільки всі банки працюють з чутливою інформацією своїх клієнтів, яка потребує належного захисту. При впровадженні нових технологій, організації повинні бути абсолютно впевненими в безпеці цієї інформації. Іншою складністю є висока ціна впровадження таких інновацій, а також значні витрати на їхню перевірку і утримання досвідчених фахівців, які можуть керувати цими системами. Це, в свою чергу, викликає проблему нестачі кваліфікованих кадрів. Спеціалісти в цій сфері мають володіти високими знаннями та досвідом у галузі інновацій, тому їх відбір слід проводити максимально ретельно. Таким чином, інтеграція штучного інтелекту у банківську сферу має як позитивні, так і

негативні сторони. Основні переваги та недоліки цього процесу можна знайти в таблиці 2.

Таблиця 1.2.

Наслідки впровадження штучного інтелекту в банках

Позитивні наслідки	Негативні наслідки
<i>Для банку</i>	
– зменшення витрат на робочу силу – збільшення продуктивності та ефективності роботи банківської установи – покращення управління банком	– зростання витрат на впровадження інформаційних технологій; – збільшення рівня заробітної плати для висококваліфікованих фахівців; – недостатня кількість професійних кадрів
<i>Для клієнтів</i>	
– підвищення ефективності взаємодії банківської установи та клієнтів без прив'язки до місця проживання – цілодобова чат-бот підтримка	– неможливість на 100 % забезпечити захищеність персональних даних через хакерські атаки
<i>Для інвесторів</i>	
– збільшення рівня доходу через можливість врахування великої кількості факторів та ризиків	– зменшення інвестиційної маржі внаслідок поширення застосування систем штучного інтелекту та послаблення можливостей виявити неефективність на ринку
<i>Для співробітників</i>	
– пришвидшення виконання та опрацювання запитів клієнтів – мінімізація ризику – автоматизація роботи з документами	– необхідність швидкої перекваліфікації; – звільнення працівників і, як наслідок, зростання безробіття

Джерело: [40].

Варто виокремити кілька умов для подальшого впровадження штучного інтелекту в глобальну банківську систему. Зокрема, оновлення застарілих систем. Щоб банки могли ефективно використовувати технології штучного інтелекту в своїй діяльності, необхідно модернізувати їх програмні системи. Старе обладнання без впровадження ШІ суттєво сповільнює роботу банківських установ, тому для інноваційного розвитку слід відмовитися від старих комп'ютерів, баз даних та онлайн-сховищ, переходячи на сучасні автоматизовані системи.

Розвиток мобільних додатків. Традиційні банківські рішення орієнтовані на конкретні функції. Майбутнє полягає у мобільних додатках, які виступають єдиними платформами, що об'єднують банківські послуги, покупки, платежі, інвестиції тощо. Це консольоване рішення надасть клієнтам зручність і оптимізує операції для постачальників [37].

Яскравим прикладом цього є ситуація 2022 року, коли українці, які були змушені виїхати за кордон через повномасштабне вторгнення, відчували труднощі у взаємодії з бюрократичною системою Європи. Звиклі до сучасних українських цифрових банків, онлайн-розрахунків та безготівкових покупок, вони зіткнулися з необхідністю чекати в чергах декілька місяців, щоб отримати банківську картку. Це підкреслює важливість комфорту клієнтів та їхнє бажання уникати витрат часу на процеси, які можна завершити набагато швидше.

Можливо, незабаром, крім простого аналізу даних, штучний інтелект зможе автономно створювати нові набори даних і моделювати різноманітні фінансові сценарії для банків. Це може мати критичне значення для оцінки ризиків, адже дозволить установа прогнозувати різні ринкові умови та готуватися до них.

З огляду на вже існуючий рівень персоналізації банківських послуг під індивідуального клієнта, можна очікувати, що перевірка фінансового стану споживачів за допомогою штучного інтелекту стане реальністю. Так само, як особа проходить медичне обстеження, штучний інтелект може запропонувати клієнтам фінансові перевірки, аналізуючи їхню фінансову поведінку, прогнозуючи потенційні труднощі та надаючи рекомендації для збереження їх фінансових заощаджень.

Висновки до першого розділу

Проведено аналіз теоретичних засад організації безпекового менеджменту банку та встановлено, що безпековий менеджмент банку передбачає протидію загрозам його діяльності та формуванні передумов для розвитку.

Виокремлено два типи контролю, які існують в межах банківської системи: поточний контроль (фокусується на аналізі фактичних результатів, тоді як підсумковий контроль оцінює ефективність впроваджених заходів для забезпечення фінансової стабільності; моніторяться такі показники, як ліквідність банку, рівень проблемних кредитів, адекватність капіталу та загальна валютна позиція) та підсумковий контроль (оцінює ефективність впроваджених заходів для забезпечення фінансової стабільності; моніторяться такі показники, як ліквідність банку, рівень проблемних кредитів, адекватність капіталу та загальна валютна позиція).

Виокремлено науково-методичний підхід, який пропонує традиційно розділяти загрози безпеці банку на внутрішні і зовнішні. Більш того, в результаті проведеного структурного аналізу цих загроз для банку була виконана їх класифікація на суб'єктивні та об'єктивні. Доведено, що зовнішні загрози відіграють вирішальну роль у підриві інвестиційної безпеки фінансових установ, що, в свою чергу, негативно впливає на фінансову інфраструктуру та економічну ситуацію в країні. Тривалість таких загроз може призвести до економічної кризи як для окремих фінансових установ, зокрема комерційних банків, так і для глобальної економіки в цілому.

Проведено аналіз та здійснено розподіл сфер за популярністю використання штучного інтелекту. Лідируючі щодо застосування штучного інтелекту займають сфери інформаційних технологій, а також банківський сектор і сфера маркетингової діяльності.

Проаналізовано очікування банків щодо впровадження чат-ботів у своїй діяльності. З'ясовано, що 80% фінансових установ по всьому світу вважають чат-ботів чудовою можливістю для підвищення бізнес-ефективності. Лише 16% сприймають чат-ботів як одночасно загрозу і можливість, тоді як всього 2% вважають, що вони можуть нести ризик для бізнесу, створюючи загрозу злочинного доступу до важливих даних.

Виокремлено основні сфери, в яких застосовується штучний інтелект, зокрема: кібербезпека, чат-боти, кредитні рішення, аналіз тенденцій ринку, управління ризиками, аналіз даних, відповідність нормативним документам.

Сформовано перелік функцій банківських працівників заміненіх штучним інтелектом, а саме: продажі, адміністрування, регулювання операцій, кредитування, управління ризиками, фінансовий аналіз тощо.

Проаналізовано основні переваги та недоліки впровадження штучного інтелекту в безпековий менеджмент банку для банківської установи, клієнта, інвесторів та співробітників.

РОЗДІЛ 2

ЗАГАЛЬНА ХАРАКТЕРИСТИКА АТ «УКРСИББАНК» ТА СИСТЕМИ БЕЗПЕКОВОГО МЕНЕДЖМЕНТУ

2.1. Загальна характеристика АТ «УКРСИББАНК»

Один із найбільших банків України — це фінансова установа «УкрСиббанк». Ця організація є частиною міжнародної корпоративної групи «Група БНП Паріба». Її присутність в Україні розпочалася на початку 1990-х, коли було засновано «Харківський Комерційний Банк», попередник сьогоденішнього «УкрСиббанку», який наразі входить до десятки провідних банків країни. Станом на 2023 рік, активи УкрСиббанку склали 133,6 мільярдів гривень. Банк обслуговує близько 1,9 мільйона клієнтів, зокрема 165 тисяч малих та середніх бізнесів і 2,2 тисячі великих компаній. Щодо структури власності банку, то вона складається з:

- 60% акцій належить фінансовій групі з Франції, BNP Paribas;
- 40% контролюється Європейським банком реконструкції та розвитку (ЄБРР).

Центральний офіс «УкрСиббанку» розташований у Києві, що є столицею України. Ця фінансова установа є частиною міжнародної фінансової групи з дворічною історією. Банк активно функціонує на українському ринку, пропонуючи клієнтам високу якість фінансових послуг, що відповідає найкращим традиціям європейського банківства. Його мережа налічує приблизно 260 відділень і близько 1000 банкоматів по всій країні. Крім того, «УкрСиббанк» бере участь у Фонді гарантування вкладів фізичних осіб.

З початком війни в Україні в 2022 році, банк зосередився на забезпеченні безперервного обслуговування різних клієнтів, починаючи від фізичних осіб і закінчуючи великими підприємствами, а також на гарантуванні безпеки клієнтів та своїх співробітників. У результаті банк потрапив до списку «30 надійних приватних компаній України», визнаний

одним із найстійкіших фінансових закладів країни та увійшов до рейтингу кращих роботодавців, перемігши в категорії «HR-менеджмент воєнного часу».

В ролі одного з провідних банків на українському фінансовому ринку, УкрСиббанк активно бере участь у банкоматному роумінгу та ініціативі Національного банку України під назвою POWER BANKING, яка спрямована на формування мережі резервних банківських відділень, здатних забезпечувати обслуговування клієнтів навіть за умов перебоїв у електропостачанні.

Банк реалізує різноманітні програми підтримки своїх клієнтів, такі як скасування комісій, продовження терміну дії карток та проведення інших заходів. Він також долучився до державної ініціативи «Підтримка і, в партнерстві з Mastercard, розпочав співпрацю з мережею Дія.Бізнес у містах, таких як Тернопіль, Ужгород, Одеса, Полтава та Кривий Ріг. Завдяки підтримці Групи, УкрСиббанк виділив 28,8 мільйонів гривень через платформу United24 на придбання сучасних реанімобілів, а також надає гуманітарну допомогу та активно працює над створенням платформи Глобального договору ООН в Україні під назвою Mental Help.

Банк приділяє значну увагу політиці безпеки, зокрема акцентуючи на принципах інформаційної безпеки, які є одним із основних пріоритетів у стратегії розвитку УкрСиббанку. Крім того, варто зазначити, що банк підтримує високі стандарти інформаційної безпеки для своїх клієнтів, враховуючи сучасні тенденції в сфері ІТ та вимоги Політики інформаційної безпеки АТ «УкрСиббанк».

Основна мета цієї політики полягає в захисті інформаційних ресурсів, забезпеченні безперервної роботи банку, зменшенні ризиків у сфері інформаційної безпеки, підвищенні репутації УкрСиббанку та формуванні довірчих стосунків із клієнтами.

Ключовими об'єктами в сфері інформаційної безпеки є такі категорії активів:

– інформаційні активи: будь-які дані та інформація в різних форматах, які обробляються, передаються або зберігаються, а також знання працівників і партнерів банку, бази даних, файли, документація та інструкції користувачів.

– програмне забезпечення: всі інформаційні системи та сервіси, включаючи додаткове, системне та сервісне програмне забезпечення, яке використовується співробітниками банку для виконання своїх обов'язків та взаємодії з клієнтами та іншими внутрішніми й зовнішніми системами.

– фізичні активи: персонал, ІТ-обладнання (таке як сервери, робочі станції, тонкі клієнти, планшети, смартфони, мережеві екрани, принтери, копіювальні апарати, телекомунікаційне обладнання, засоби зв'язку, маршрутизатори, комутатори, АТС, факси та модеми), носії даних (стрічки, диски та інше), меблі, приміщення, виробниче обладнання та технічні засоби.

– сервісні активи: послуги з обробки та комунікації (Інтернет, електронна пошта, канали зв'язку тощо), а також інші технічні послуги (опалення, освітлення, енергопостачання, кондиціонування, системи сигналізації та моніторингу). Це також включає всі послуги, пов'язані з отриманням, використанням, передачею та утилізацією активів, а також юридичних і фізичних осіб, установ та компаній, які надають послуги в цій сфері.

Для кожного з активів аналізуються можливі загрози та заходи для їх нейтралізації в рамках стратегії управління ризиками:

- контроль доступу;
- управління правами і привілеями;
- визначення методик автентифікації;
- чітке розмежування обов'язків і ролей;
- установлення вимог до інформаційної безпеки для кожного активу;
- впровадження політики в інформаційних системах і сервісах;
- підтримка відповідного рівня безпеки;

- проведення перевірок безпеки в інформаційних системах;
- управління випадками;
- класифікація активів та забезпечення конфіденційності даних;
- захист від шкідливих програм;
- резервне копіювання та відновлення інформації;
- дотримання ліцензійних вимог;
- контроль за виконанням вимог політики та інших аспектів інформаційної безпеки.

Отож, французький банківський конгломерат BNP Paribas в Україні функціонує у формі акціонерного товариства «УкрСиббанк», яке було засноване 28 жовтня 1991 р. згідно реєстрації юридичною адресою є – 04070, місто Київ, Подільський район, вулиця Андріївська, будинок 2/12. Код організації за ЄДРПОУ – 09807750. На рисунку Структура управління АТ «УКРСИББАНК» представлена на рисунку 2.1.

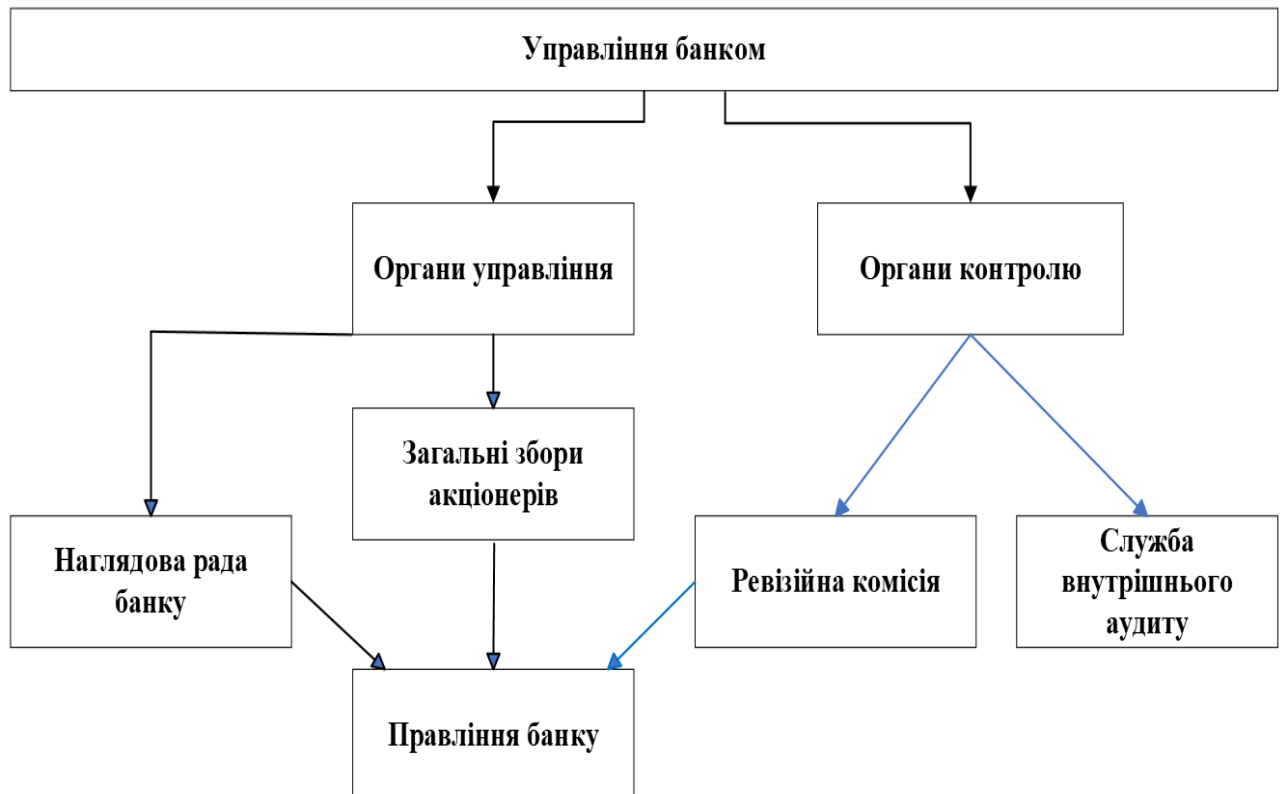


Рис. 2.1. Структура органів управління АТ «УКРСИББАНК»

Розроблено автором на основі [5].

Отож, головними суб'єктами управління АТ «Укрсиббанк» є:

- загальні збори акціонерів;
- наглядова рада;
- правління банку.

Управління АТ «УкрСиббанк» здійснюється через Загальні збори акціонерів, до яких входять усі акціонери, незалежно від кількості та типів їх акцій. У банку немає єдиного великого акціонера. Наглядова Рада підпорядкована Загальним зборам акціонерів і надає їм звіти про управління, основні результати та діяльність банку. Головна роль ради полягає в захисті інтересів акціонерів, розробці стратегій для АТ «УкрСиббанк», забезпеченні їх ефективного виконання та контролі за реалізацією стратегічних планів.

Правління банку виконує функції виконавчого органу, який управляє стратегічними та операційними питаннями. Це колегіальний орган, відповідальний за досягнення визначених цілей та впровадження політик, затверджених Наглядовою Радою.

Правління зобов'язане звітувати перед Наглядовою Радою, надаючи їй необхідну, актуальну та точну інформацію для виконання своїх функцій.

Організаційна структура АТ «УкрСиббанк» включає Ревізійну комісію, що відповідає за моніторинг фінансово-господарської діяльності, а також Службу внутрішнього аудиту, яка виконує функції оперативного контролю.

Варто також представити структуру банку в розрізі стратегічних бізнес-напрямів [5]:

- напрямок роздрібного бізнесу;
- напрямок споживчого кредитування;
- напрямок стосовно реструктуризації та відшкодування боргів;
- напрямок операційної діяльності;
- напрямок інформаційних технологій;
- напрямок закупівельної діяльності;
- напрямок з комунікацій, корпоративної соціальної відповідальності та залученості.

Ефективність банку значно залежить від стратегії, яка застосовується в управлінні ризиками та безпекою. Визначена стратегія передбачає створення надійної та безпечної системи контролю ризиків, що ґрунтується на тривалій фінансовій практиці групи та відповідає стандартам національних регуляторів. Вона також сприяє збалансуванню зростаючих потреб бізнесу з обережним підходом до управління ризиками. Банк також отримав низку нагород та відзнак, які наведено у таблиці 2.1.

Таблиця 2.1

Нагороди та рейтинги BNP Paribas в Україні у 2020-2021 рр.

Рік	№	Нагорода, відзнака
2021	1	Рейтингове агентство «Експерт-рейтинг» підтвердило довгостроковий кредитний рейтинг банку на рівні AAA
	2	TOP-3 найбільш стійких банків України за версією популярного в Україні інтернет-видання Forinsurer.com
	3	TOP Employer 2020 в Україні та Європі у складі BNP Paribas, сертифікація Top Employer Institute
	4	№1 у рейтингу життєздатності українських банків за версією незалежного бізнес-порталу Mind.UA
	5	№2 Найкращий інтернет банк за результатами FinAwards2020
	6	№3 UKRSIB online – Найкращий мобільний банк за результатами FinAwards2020 TOP-3 кращих роботодавців фінансового сектору України за підсумками незалежного дослідження привабливості роботодавців
	7	Сертифікація Payment Card Industry Data Security Standard – міжнародний аудит безпеки за стандартом PCI DSS
	8	Програма підтримки жіночого підприємництва «Жінки в бізнесі» увійшла до першого звіту Глобального договору ООН від України про досягнення 17 цілей сталого розвитку
	9	№1 серед банків України за лояльністю вкладників
	10	Best Legal Departments 2020 за результатами незалежного дослідження «50 провідних юридичних департаментів України»
	11	№2 у рейтингу найнадійніших банків України за версією інвестиційної компанії Dragon Capital
	12	Найкращий сервіс Premium Banking в Україні за версією Mastercard №1 «Ціль сталого розвитку №3 – Міцне здоров'я і благополуччя» у конкурсі кейсів з корпоративної соціальної відповідальності
2022	1	TOP-3 в рейтингу надійності банків України за версією видання Деньги.ua
	2	Рейтингове агентство «Експерт-рейтинг» підтвердило довгостроковий кредитний рейтинг банку на рівні uaAAA за національною українською шкалою, що означає найвищий рівень кредитоспроможності (3 кв. 2021)
	3	TOP-3 найбільш стійких банків України за версією Forinsurer.com
	4	TOP-3 у рейтингу стійкості банків за підсумками 2-го кварталу 2021 року
	5	TOP-3 у рейтингу життєздатності українських банків за версією незалежного бізнес-порталу Mind.UA

Джерело: [5].

Ключовим вектором цієї стратегії є уникнення та зниження ризиків у межах визначеного рівня апетиту до ризиків та бізнес-моделі банку. АТ «УкрСиббанк» проводить свою діяльність на основі ліцензій, наданих декільком державним органам, серед яких Національний банк України, Національна комісія з цінних паперів і фондового ринку, а також Міністерство фінансів України. Додатково, банк є учасником Фонду гарантування вкладів фізичних осіб, має реєстраційне свідоцтво №086 і зосереджується на наданні послуг юридичним і фізичним особам в Україні.

Відповідно до заяв керівництва BNP Paribas, ця фінансова група має можливість виявляти та адаптуватися до змін, які впливають на щоденне життя клієнтів і суспільства в цілому, перетворюючи їх на можливості для зростання, зокрема через впровадження інноваційних технологій, що сприяють формуванню кращого майбутнього. Крім того, BNP Paribas займає високі позиції в глобальних рейтингах та займає провідні місця в фінансових рейтингах України, пропонуючи послуги світового рівня, пакетні пропозиції та комплексні рішення, які покращують та спрощують фінансові процеси.

2.2. Аналіз фінансової діяльності АТ «УКРСИББАНК»

Для оцінки основних результатів фінансової діяльності АТ «Укрсиббанк» проведемо необхідний аналіз. Управління інноваційною діяльністю вимагає, насамперед, встановлення стратегічних орієнтирів. Відповідно, формування таких орієнтирів передбачає визначення напрямків, які потребують удосконалення та розвитку. Ці напрямки можна виявити, проаналізувавши діяльність банківської установи та виявивши основні проблемні зони, які потребують поліпшення управлінського процесу та безпекового менеджменту зокрема. Рекомендаційна частина дослідження базуватиметься на цьому алгоритмі та включатиме пропозиції щодо вдосконалення безпекового менеджменту АТ «Укрсиббанк». Загалом, аналіз буде виконано в контексті оцінки фінансових показників, ефективності роботи банку, банківських операцій, а також управлінських та безпекових практик. На основі

розрахованих показників, визначимо напрямки удосконалення безпекового менеджменту АТ «Укрсиббанк».

Розпочнемо з аналізу стану і динаміки показників дохідності та витрат АТ «Укрсиббанк» за період 2021-2024 рр. (табл. 2.2).

Таблиця 2.2

Стан і динаміка показників діяльності АТ «Укрсиббанк», тис. грн.

Показник	Роки			
	2021	2022	2023	2024
Активи	78 183	108 589	141 935	169 104
Зобов'язання	68 486	95 328	124 610	147 734
Власний капітал	9 696	13 260	17 324	21 369
Процентні доходи	3 967	9 034	12 994	14 025
Процентні витрати	1 006	2 171	311	306
Комісійні доходи	2 661	2 379	2 629	2 934
Комісійні витрати	686	825	975	1 170
Витрати на персонал	2 317	2 571	3 098	3 494
Чисті доходи від банківської діяльності	6 086	11 998	14 663	14 549
Прибуток (збиток) від операційної діяльності	1 703	4 352	8 582	8 232
Прибуток (збиток) до оподаткування	1 726	4 344	8 590	8 237
Прибуток (збиток)	1 396	3 564	4 220	4 045

Джерело: розроблено автором на основі [5; 8].

Варто зауважити, що практично усі показники фінансової діяльності АТ «Укрсиббанк» зростають протягом аналізованого періоду 2021-2024 рр. перш за все, така тенденція зумовлена коронавірусною кризою 2020-2021 рр., яка суттєво вплинула на показники прибутковості діяльності банків, зокрема й Укрсиббанку. Динаміка окремих показників починає демонструвати спадну динаміку з 2024 року. Зокрема, це стосується таких показників: чисті доходи від банківської діяльності; прибуток (збиток) від операційної діяльності;

прибуток (збиток) до оподаткування; прибуток (збиток). Вважаємо, що така тенденція показників прибутковості діяльності зумовлена фінансовим «виснаженням» внаслідок російсько-української війни. Проте, варто зауважити, що реальне значення показників у 2024 році є меншим за 2023 рік, але значно вищими за 2021 рік. Скажімо, чистий прибуток за 201 та 2024 рр. зростає на 290 %; прибуток до оподаткування на 477 %; прибуток (збиток) від операційної діяльності на 483 %; чисті доходи від банківської діяльності теж на 239 %. Відповідно, підсумовуємо, що за воєнний період діяльність банку не зазнала критичних змін, а навпаки стала більш прибутковою.

Перейдемо до обчислення показників ефективності банку (табл. 2.3).

Таблиця 2.3

Алгоритм розрахунку відносних показників ефективності діяльності банку

Показник	Алгоритм розрахунку	Нормативне значення
Рентабельність активів (ROA, Return on Assets), %	Чистий прибуток / Активи*100%	> 1
Рентабельність власного капіталу (ROE, Return on Equity)	Чистий прибуток / Власний капітал*100%	> 15
Коефіцієнт надійності	Власний капітал / Зобов'язання	> 0,05
Коефіцієнт «фінансового важеля»	Зобов'язання / Власний капітал	< 20
Мультиплікатор капіталу	Активи / Власний капітал	12 – 15
Коефіцієнт достатності капіталу	Власний капітал / Активи	> 0,1
Чиста процентна маржа, %	(Процентні доходи – Процентні витрати) / Активи*100%	> 4,5
Коефіцієнт загальної ліквідності	Активи / Зобов'язання	> 1
Рентабельність витрат на персонал	Чистий прибуток / Витрати на персонал*100%	-
Продуктивність праці працівника	Чистий прибуток / середньорічна чисельність працівників	-

Джерело: [5; 8].

Оскільки, саме банківська сфера є найбільш вразливою та чутливою до подібних змін в економіці можемо припустити, ґрунтуючись на результатах проведеного аналізу, про відносну ефективність управлінської системи, зокрема в сфері антикризового менеджменту АТ «Укрсиббанк».

Для того аби обчислити показники, наведені в таблиці 2.3, необхідно також врахувати дані про склад кадрів АТ «Укрсиббанк». Таким чином, середнє число співробітників складало:

2021 р. – 4887 осіб.

2022 р. – 4920 осіб.

2023 р. – 4970 осіб.

2024 р. – 5020 осіб.

Результати розрахунків окреслених показників представимо у таблиці 2.4.

Таблиця 2.4

Аналіз відносних показників ефективності діяльності АТ «Укрсиббанк»

№	Показник	Роки			
		2021	2022	2023	2024
1	Рентабельність активів (ROA, Return on Assets), %	1,78	3,28	2,97	2,39
2	Рентабельність власного капіталу (ROE, Return on Equity)	14,4	26,9	24,36	18,92
3	Коефіцієнт надійності	0,14	0,139	0,139	0,144
4	Коефіцієнт «фінансового важеля»	7,06	7,18	7,19	6,91
5	Мультиплікатор капіталу	8,06	8,14	8,19	7,89
6	Коефіцієнт достатності капіталу	0,12	0,122	0,122	0,126
7	Чиста процентна маржа, %	3,78	6,32	8,93	8,11
8	Коефіцієнт загальної ліквідності	1,147	1,139	1,139	1,144
9	Рентабельність витрат на персонал, %	60	138	136	116
10	Продуктивність праці працівника	285	724	849	806

Джерело: розроблено автором на основі [5].

Підводячи підсумки виконаного аналізу, можна стверджувати, що впродовж 2021-2023 років більшість показників демонструють тенденцію до зростання, а раптове зниження у 2024 році зумовлене активними діями війни Росії проти України, що розпочалася в лютому 2022 року.

На рисунку 2.2. наведемо графічне відображення динаміки показників рентабельності активів та рентабельності власного капіталу. Відповідно, на рисунку 2.3 представимо графічне відображення динаміки окремих показників ефективності діяльності АТ «Укрсиббанк».

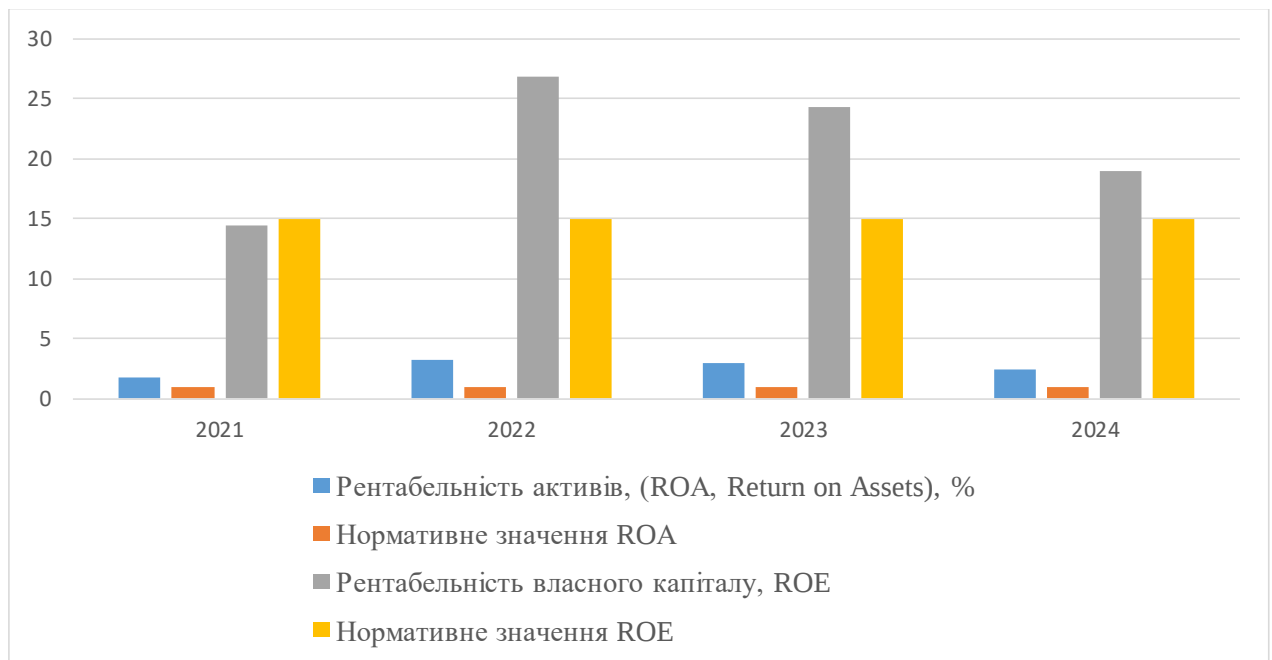


Рис. 2.2. Динаміка рентабельності активів та рентабельності власного капіталу

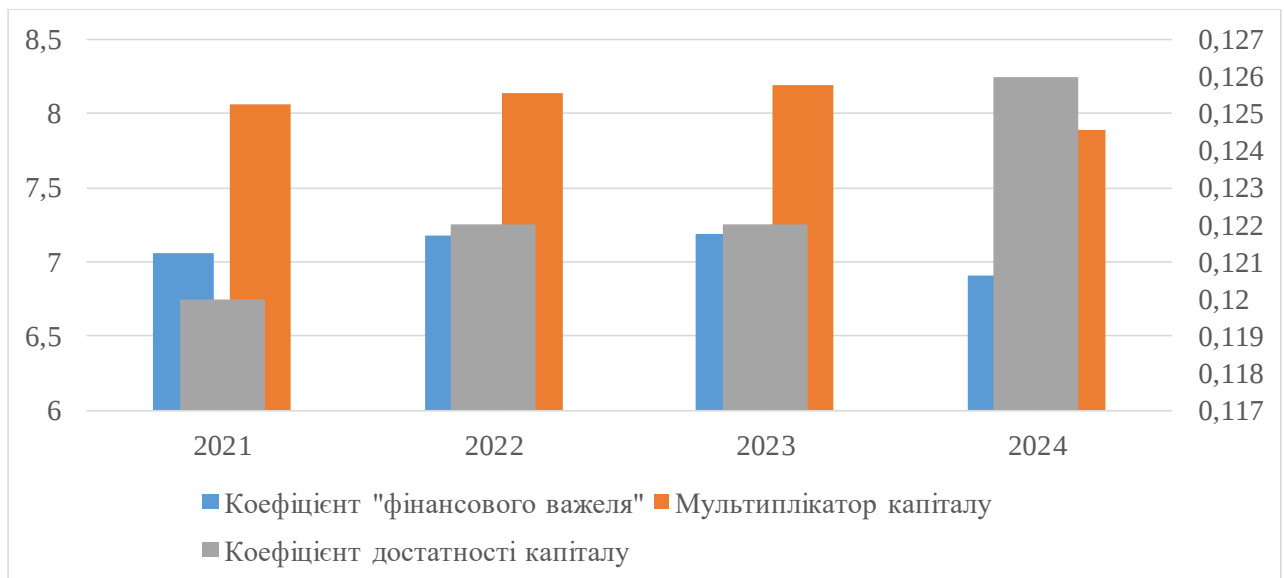


Рис. 2.3. Динаміка показників ефективності діяльності АТ «Укрсиббанк»

У цілому можна відзначити загальну тенденцію: зменшення показників рентабельності у 2021-2023 роках та невелике зростання деяких показників у 2024 році. Цю динаміку добре ілюструє рисунок 2.4.

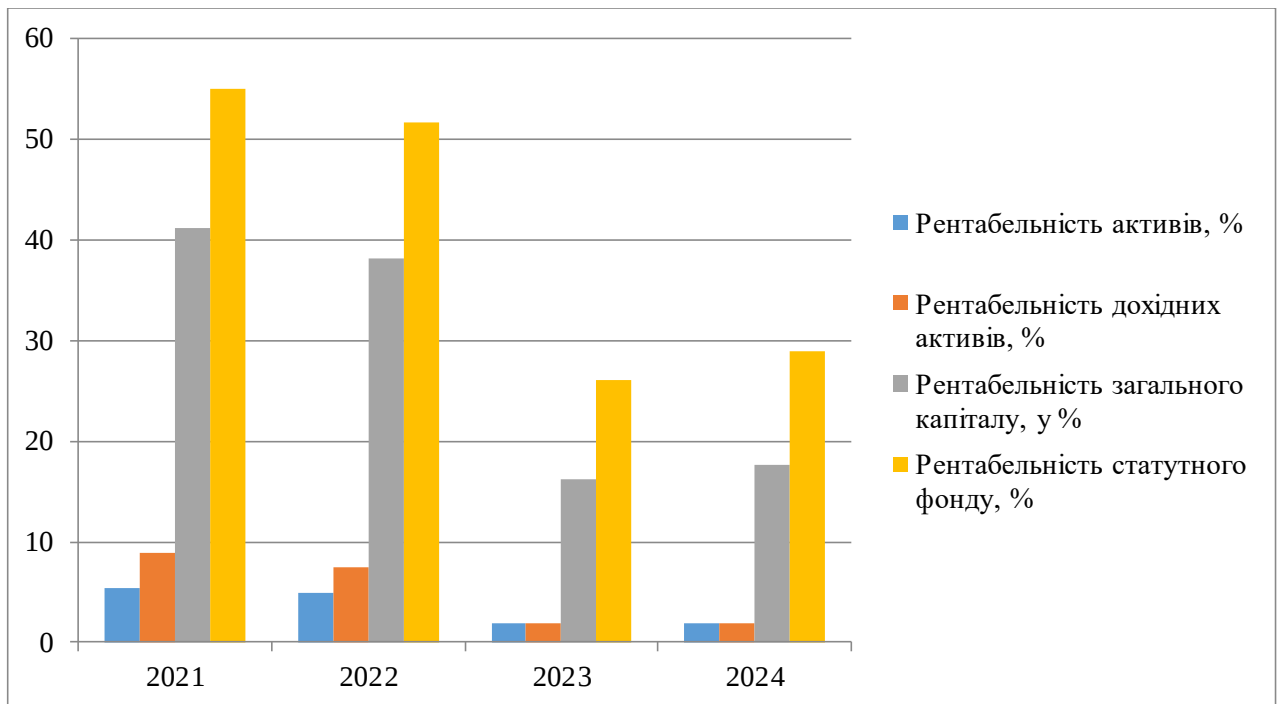


Рис. 2.4. Динаміка показників рентабельності АТ «Укрсиббанк»

Слід підкреслити, що досить позитивну динаміку серед проаналізованих показників демонструє чистий середній дохід, який у 2021 році становив 15,83%. Хоча згодом він коливався, у 2024 році він досяг 18,54%. Зниження цього показника було зумовлене скороченням процентних витрат і доходів у 2022 та 2023 роках.

Підсумовуючи проведений аналіз, можна відзначити, що АТ «Укрсиббанк» має сприятливі показники фінансової діяльності та стійкості. Організація має можливість покривати свої поточні зобов'язання власними ресурсами та компенсувати непередбачені збитки.

2.3. Пропозиції щодо інтеграції штучного інтелекту в безпековий менеджмент АТ «Укрсиббанк»

Перейдемо до формування пропозицій щодо інтеграції штучного інтелекту в безпековий менеджмент банку. Логіка побудови рекомендацій передбачатиме два етапи.

Перший етап – створення теоретичної моделі процесу безпекового менеджменту для АТ «Укрсиббанк».

Другий етап – розробка основних рекомендацій щодо інтеграції штучного інтелекту в безпековий менеджмент АТ «Укрсиббанк».

Третій етап. Формування пропозицій для удосконалення безпекового менеджменту АТ «Укрсиббанк».

Перший етап. Враховуючи результати проведеного дослідження можемо побудувати теоретичну модель функціонування безпекового менеджменту АТ «Укрсиббанк». Для досягнення цієї мети буде використано метод моделювання, зокрема моделювання за допомогою моделі IDEF0 (рис. 2.2).

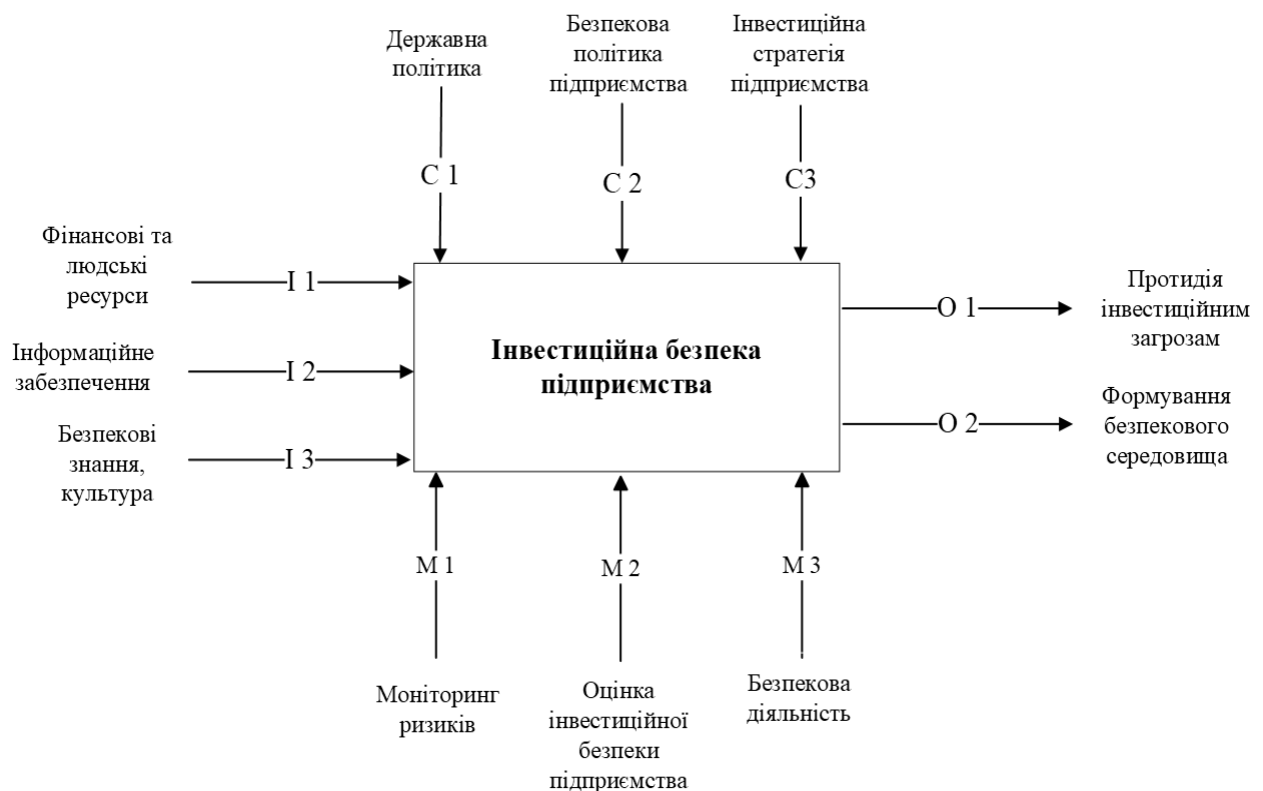


Рис. 2.2. Моделювання безпекового менеджменту банку

Джерело: розроблено автором на основі [1; 15].

Як видно з рисунку, було запропоновано модель для безпекового менеджменту АТ «Укрсиббанку», яка включає чотири площини: вхід, вихід, управління та механізм. Ця модель базується на теоретичних основах, що розкривають суть інвестиційної безпеки через призму формування безпечного середовища. Вона включає створення механізму забезпечення безпеки банку шляхом оцінки стану безпеки, постійного моніторингу ризиків, безпекової діяльності та інтеграції штучного інтелекту.

Другий етап. Передбачає розробку рекомендацій для інтеграції штучного інтелекту в безпековий менеджмент банку (рис. 2.5).

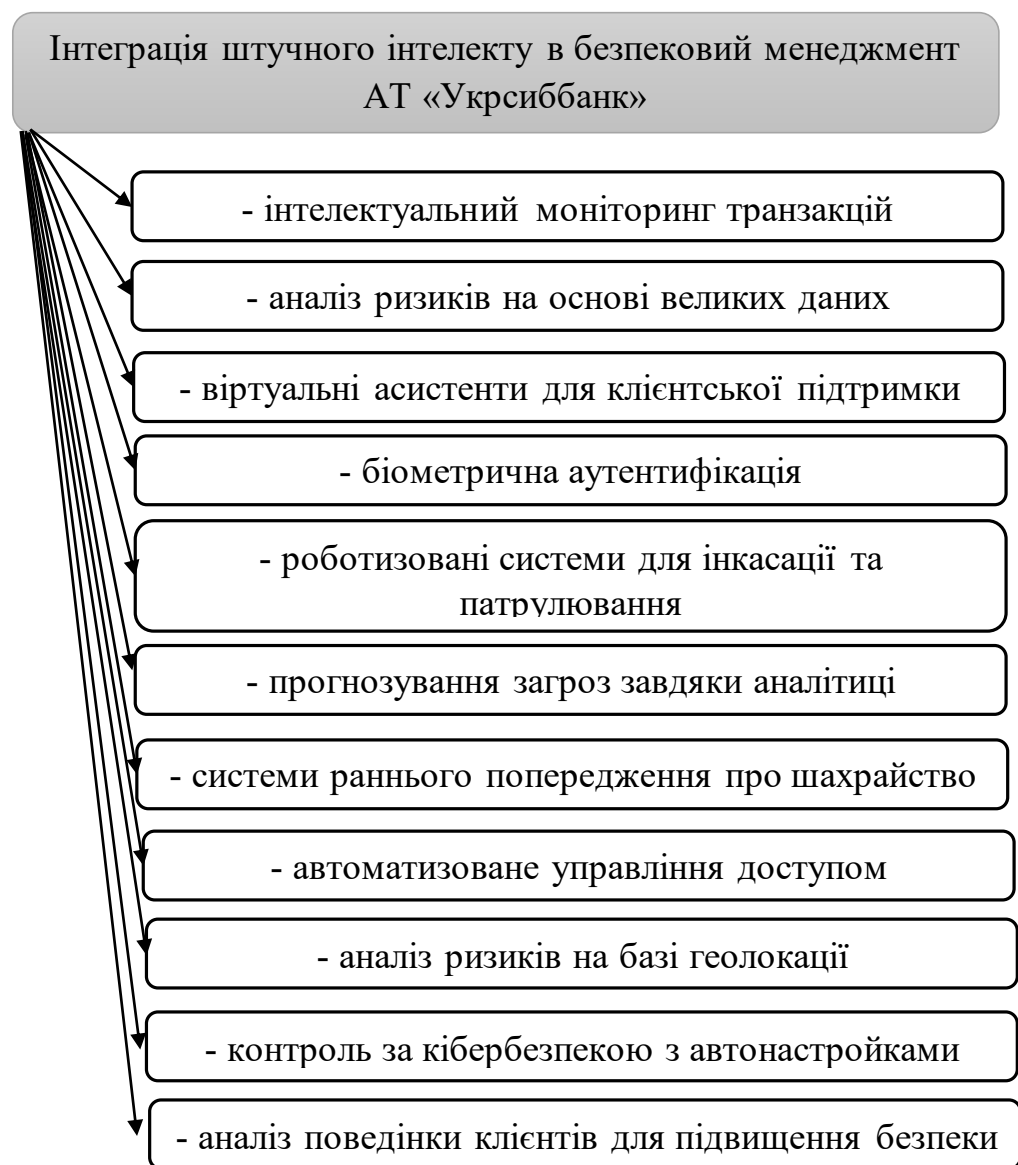


Рис. 2.5. Пропозиції щодо інтеграції ШІ в безпековий менеджмент банку

Перейдемо до конкретизації анонсованих пропозицій щодо інтеграції штучного інтелекту в безпековий менеджмент АТ «Уксіббанку».

Інтелектуальний моніторинг транзакцій. Застосування алгоритмів штучного інтелекту для автоматизованого виявлення аномальних транзакцій в реальному часі може істотно підвищити рівень безпеки фінансової установи. Системи здатні навчитися розпізнавати звичайні патерни поведінки клієнтів і виявляти відхилення, які можуть свідчити про шахрайські дії. Це дасть можливість менеджменту та фахівцям з безпеки оперативно реагувати на потенційні загрози.

Аналіз ризиків, що ґрунтується на великих даних. Штучний інтелект здатен обробляти великі обсяги інформації з метою виявлення ризиків, пов'язаних із клієнтами, продуктами та ринковими умовами. Моделі машинного навчання можуть прогнозувати обставини, що можуть призвести до фінансових втрат, що дозволить банкам уникати ризикових транзакцій.

Віртуальні асистенти для підтримки клієнтів. Розширення використання чат-ботів, заснованих на штучному інтелекті, може підвищити безпеку взаємодії клієнтів з банківськими установами. Вони здатні оперативно відповідати на питання користувачів щодо аспектів безпеки, надавати рекомендації щодо використання карток та допомагати у випадках підозрілої активності на рахунках, забезпечуючи при цьому високий рівень обслуговування.

Біометрична аутентифікація. Застосування технологій, що складаються з ІІІ для біометричної ідентифікації (наприклад, розпізнавання обличчя, відбитків пальців або голосу), може суттєво зміцнити безпеку доступу до банківських послуг. Цей метод ускладнює шахрайські дії, оскільки біометричні дані значно важче підробити порівняно з традиційними паролями.

Роботизовані рішення для інкасації та патрулювання. Застосування автономних роботизованих систем для збору готівки або патрулювання території фінансової установи може істотно посилити захист фізичних активів. Ці роботи можуть бути обладнані технологіями штучного інтелекту для

створення гнучких маршрутів та виявлення підозрілої активності, що знижує ризики фізичних атак.

Прогнозування загроз через аналіз соціальних мереж. Використання ІІІ для перегляду даних із соціальних мереж та інших публічних джерел дозволяє виявляти можливі загрози безпеці банків. Наприклад, аналіз дискусій чи коментарів може сигналізувати про потенційні фінансові злочини або протестні настрої клієнтів, що дає можливість вчасно реагувати.

Застосування штучного інтелекту в безпековому менеджменті фінансових установ може значно збільшити ефективність захисту активів та інформації, що сприяє підвищенню довіри клієнтів до банків.

Системи раннього діагностування шахрайства. Впровадження рішень на основі штучного інтелекту, які застосовують прогностичні алгоритми для виявлення ознак шахрайства ще до того, як вони перетворяться на серйозну загрозу. Ці системи здатні аналізувати історичні дані, щоб виявляти конкретні індикатори, що свідчать про можливу шахрайську діяльність.

Автоматизоване управління доступом. Застосування штучного інтелекту для динамічного моніторингу систем доступу до фізичних і цифрових активів. Виходячи з поведінки користувачів і їхніх ролей у компанії, система має можливість автоматично регулювати рівень доступу до різних ресурсів, що сприяє зменшенню ризику витоку інформації.

Аудит і відповідність за допомогою штучного інтелекту. Застосування технологій ІІІ для автоматизації процесів аудиту та перевірки дотримання нормативних вимог, що сприяє зменшенню ризику значних штрафів та санкцій за недотримання. Штучний інтелект може виявляти нетипові операції та формувати звіти для команди з питань комплаєнсу.

Інтелектуальні системи охорони. Використання відеоспостережних систем з елементами ІІІ, які здатні автоматично ідентифікувати підозрілу активність. Наприклад, такі системи можуть в реальному часі аналізувати потоки людей і виявляти аномальну поведінку, своєчасно сповіщаючи охоронців про потенційні загрози.

Навчання співробітників за допомогою віртуальної реальності. Застосування платформ віртуальної реальності (VR) для підготовки працівників до технік реагування на загрози. Інтеграція штучного інтелекту дозволяє створювати віртуальні сценарії, які вимагають ухвалення рішень у стресових ситуаціях, таким чином готуючи персонал до справжніх викликів.

Геолокаційний аналіз ризиків. Використання даних геолокації в комбінації з ІІІ для оцінки ризиків на основі місцезнаходження клієнтів. Це дає змогу виявляти аномальні транзакції в певних регіонах або в ситуаціях, пов'язаних із зонами з високим показником злочинності.

Контроль кібербезпеки з автоматичним налаштуванням. Розробка адаптивних систем захисту, які за допомогою ІІІ автоматично регулюють параметри безпеки в залежності від нових загроз у кіберпросторі. Такі системи здатні швидко реагувати на злочинні дії без необхідності людського втручання.

Аналіз клієнтської поведінки для покращення безпеки. Вивчення моделей поведінки користувачів за допомогою штучного інтелекту дозволяє ідентифікувати аномальні дії, що можуть свідчити про загрози безпеці. Наприклад, різкі зміни в способах використання рахунків або методах входу в систему можуть призвести до автоматичної перевірки.

Третій етап. На завершення нашого дослідження пропонуємо низку рекомендацій для підвищення рівня безпекового менеджменту в банках. Варто зазначити, що під час виконання фінансових операцій виникають ризики, які можуть впливати на ліквідність і знижувати ефективність використання капіталу. Для поліпшення економічної продуктивності доцільно реалізувати такі заходи:

- планування інвестиційних заходів та моніторинг їх виконання.
- регулювання та стимулювання інвестиційної діяльності.
- аналітика та прогнозування інвестицій.

Підвищення ефективності інвестиційних операцій в банківському секторі є основоположним фактором для досягнення фінансового успіху та підтримки стабільності. Нижче наведено ряд рекомендацій, які можуть сприяти вдосконаленню інвестиційної діяльності фінансової установи.

Впровадження сучасних технологій, таких як штучний інтелект (ШІ), аналітика даних, блокчейн та інші, здатне суттєво покращити автоматизацію процесів, прискорити ухвалення рішень та підвищити їхню точність.

Ретельний аналіз та вдосконалення внутрішніх процесів в банку можуть знизити непотрібні витрати та витрачений час, підвищуючи при цьому ефективність інвестиційних операцій. Дослідження можливостей для розширення фінансового портфеля та впровадження нових продуктів і послуг може сприяти збільшенню інвестиційних можливостей для банку. Більш того, розробка адаптивних і новаторських підходів до інвестування, які здатні швидко адаптуватися до коливань на ринку, відкриває нові горизонти для отримання прибутку.

Підвищення кваліфікації співробітників та їхній професійний розвиток, особливо у сфері фінансів та інвестицій, можуть сприяти створенню та реалізації більш ефективних інвестиційних стратегій. Аналіз можливостей для співпраці та укладання партнерств з іншими фінансовими установами, фінансовими технологіями або технологічними стартапами може відкрити нові перспективи для інвестицій.

Інтеграція етичних і відповідальних аспектів у процес ухвалення інвестиційних рішень може підвищити імідж банку та залучити більше клієнтів.

Розробка ефективних стратегій управління ліквідністю забезпечить більшу фінансову стабільність банку під час ринкових нестабільностей.

Запровадження адекватного механізму комунікації з регуляторами фінансового сектора може полегшити банку оперативне вирішення питань, пов'язаних з інвестиціями.

Отож, на основі результатів проведеного аналізу було сформовано рекомендації щодо інтеграції штучного інтелекту в безпековий менеджмент банку та пропозиції щодо удосконалення безпекового менеджменту АТ «Укрсиббанк».

Висновки до другого розділу

Проведено загальну характеристику АТ «Укрсиббанк». З'ясовано, що банк приділяє значну увагу політиці безпеки, зокрема акцентуючи на принципах інформаційної безпеки, які є одним із основних пріоритетів у стратегії розвитку УкрСиббанку. Більш того, банк підтримує високі стандарти інформаційної безпеки для своїх клієнтів, враховуючи сучасні тенденції в сфері ІТ та вимоги Політики інформаційної безпеки АТ «УкрСиббанк».

Виокремлено головних суб'єктів управління АТ «Укрсиббанк» загальні збори акціонерів; наглядова рада; правління банку. Вищим органом управління є загальні збори акціонерів, до яких входять усі акціонери, незалежно від кількості та типів їх акцій. У банку немає єдиного великого акціонера. Правління банку виконує функції виконавчого органу, який управляє стратегічними та операційними питаннями. Організаційна структура АТ «УкрСиббанк» включає Ревізійну комісію, що відповідає за моніторинг фінансово-господарської діяльності, а також Службу внутрішнього аудиту, яка виконує функції оперативного контролю.

В результаті проведеного аналізу фінансової діяльності АТ «Укрсиббанк» встановлено, що майже всі показники фінансової діяльності банку демонструють зростання впродовж періоду з 2021 по 2024 роки. Така позитивна динаміка, насамперед, пов'язана з впливом коронавірусної кризи 2020-2021 років, яка суттєво позначилася на прибутковості банківського сектору, в тому числі і АТ «Укрсиббанк».

Однак, починаючи з 2024 року, спостерігається спад у динаміці ряду показників, зокрема чистих доходів від банківської діяльності, прибутку (збитку) від операційної діяльності та прибутку (збитку) до оподаткування. Така тенденція, на нашу думку, є наслідком фінансового «виснаження», викликаного російсько-українською війною.

Незважаючи на це, реальні значення показників у 2024 році залишаються значно вищими, ніж у 2021 році, хоча й нижчими порівняно з 2023 роком. Наприклад, чистий прибуток за 2024 рік зріс на 290% у порівнянні з 2021

роком, прибуток до оподаткування — на 477%, прибуток (збиток) від операційної діяльності — на 483%, а чисті доходи від банківської діяльності також зросли на 239%.

Проаналізовано ключові показники ефективності діяльності банку, встановлено, що впродовж 2021-2023 років більшість показників демонструють тенденцію до зростання, а раптове зниження у 2024 році зумовлене активними діями війни росії проти України, що розпочалася в лютому 2022 року. Серед проаналізованих показників позитивну динаміку демонструє чистий середній дохід, який у 2021 році становив 15,83%. Хоча згодом він коливався, у 2024 році він досяг 18,54%. Зниження цього показника було зумовлене скороченням процентних витрат і доходів у 2022 та 2023 роках. Резюмуючи результати аналізу варто зауважити, що АТ «Укрсиббанк» має сприятливі показники фінансової діяльності та стійкості. Організація має можливість покривати свої поточні зобов'язання власними ресурсами та компенсувати непередбачені збитки.

Розроблено алгоритм для формування рекомендаційної частини кваліфікаційної роботи: перший етап – створення теоретичної моделі процесу безпекового менеджменту для АТ «Укрсиббанк»; другий етап – розробка основних рекомендацій щодо інтеграції штучного інтелекту в безпековий менеджмент АТ «Укрсиббанк»; третій етап. Формування пропозицій для удосконалення безпекового менеджменту АТ «Укрсиббанк».

В межах анонсованого алгоритму сформовано теоретичну модель функціонування безпекового менеджменту АТ «Укрсиббанк», за допомогою моделі IDEF0. Модель включає чотири площини: вхід, вихід, управління та механізм. Ця модель базується на теоретичних основах, що розкривають суть інвестиційної безпеки через призму формування безпечного середовища. Вона включає створення механізму забезпечення безпеки банку шляхом оцінки стану безпеки, постійного моніторингу ризиків, безпекової діяльності та інтеграції штучного інтелекту.

Розроблено рекомендації для інтеграції штучного інтелекту в безпековий менеджмент банку, а саме: інтелектуальний моніторинг транзакцій; аналіз

ризиків на основі великих даних; віртуальні асистенти для клієнтської підтримки; біометрична аутентифікація; роботизовані системи для інкасації та патрулювання; . прогнозування загроз завдяки аналітиці соціальних мереж; системи раннього попередження про шахрайство; аналіз ризиків на базі геолокації; контроль за кібербезпекою з автонастройками; аналіз поведінки клієнтів для підвищення безпеки.

Сформовано рекомендації для підвищення рівня безпекового менеджменту в банках, а саме: впровадження передових технологій, таких як штучний інтелект (ШІ), аналітика даних, блокчейн та інших; розробка адаптивних та інноваційних інвестиційних стратегій; підвищення кваліфікації співробітників та їхній розвиток, особливо у сфері фінансів та інвестицій; вивчення можливостей для співпраці та створення партнерств з іншими фінансовими установами, фінтех-компаніями або технологічними стартапами може відкрити нові інвестиційні перспективи.

ВИСНОВКИ

На основі проведеного аналізу теоретичних засад організації безпекового менеджменту банку встановлено, що безпековий менеджмент є критично важливим для протидії загрозам та формування умов для подальшого розвитку установи.

З'ясовано, що в банківській системі виділяються два типи контролю: поточний, який акцентує увагу на аналізі фактичних результатів, та підсумковий, що оцінює ефективність впроваджених заходів для забезпечення фінансової стабільності. Довели, що обидва типи контролю сприяють моніторингу важливих показників, таких як ліквідність, рівень проблемних кредитів та адекватність капіталу.

Сформовано науково-методичний підхід до класифікації загроз для безпеки банку на внутрішні та зовнішні, де зовнішні загрози мають вирішальне значення у зниженні інвестиційної безпеки. Доведено, що тривалі зовнішні загрози можуть призвести до економічної кризи, впливаючи не лише на комерційні банки, а й на глобальну економіку в цілому.

Проаналізовано сфери застосування штучного інтелекту, де лідирують інформаційні технології, банківський сектор та маркетинг.

З'ясовано, що 80% банків у світі розглядають чат-ботів як можливість для підвищення ефективності бізнесу, в той час як лише 2% вважають їх потенційною загрозою.

Виокремлено основні сфери, де застосовується штучний інтелект, включаючи кібербезпеку, чат-боти та аналіз ризиків. Сформовано перелік функцій, які можуть бути автоматизовані за рахунок технологій ШІ, таких як продажі та фінансовий аналіз.

Проаналізовано переваги та недоліки впровадження штучного інтелекту в безпековий менеджмент, що стосуються не тільки банківських установ, але й клієнтів, інвесторів та співробітників.

Таким чином, сформулювавши всі ці висновки, можна стверджувати, що інтеграція інноваційних технологій, зокрема штучного інтелекту, є необхідною для підвищення ефективності безпекового менеджменту в банківській системі.

Встановлено, що банк приділяє значну увагу політиці безпеки, акцентуючи на принципах інформаційної безпеки, які є одним із основних пріоритетів в його стратегічному розвитку.

З'ясовано, що основними суб'єктами управління банку є загальні збори акціонерів, наглядова рада та правління. Виявлено, що банківська структура не має єдиного великого акціонера, а правління виконує роль виконавчого органу, що управляє стратегіями та операціями.

Доведено, що позитивна динаміка фінансових показників АТ «Укрсиббанк» у період з 2021 по 2024 роки, насамперед, пов'язана з впливом коронавірусної кризи 2020-2021 років. Наприкінці аналізованого періоду відзначено спад у кількох показниках, що може бути зумовлено фінансовим виснаженням через російсько-українську війну.

Сформовано позитивні результати аналізу фінансової діяльності: чистий прибуток, прибуток до оподаткування та чисті доходи від банківської діяльності демонструють значне зростання порівняно з 2021 роком.

Розроблено алгоритм для формування рекомендацій щодо інтеграції штучного інтелекту в безпековий менеджмент, включаючи три основні етапи: створення теоретичної моделі процесу, розробка рекомендацій та формування пропозицій щодо вдосконалення.

Сформовано теоретичну модель функціонування безпекового менеджменту, яка ґрунтується на принципах інвестиційної безпеки та включає в себе механізм забезпечення безпеки, оцінку ризиків та моніторинг.

Розроблено конкретні рекомендації для інтеграції штучного інтелекту, такі як інтелектуальний моніторинг транзакцій та віртуальні асистенти для підтримки клієнтів, які можуть суттєво підвищити рівень безпеки.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Hobela V., Podra O., Batyuk B., Levkiv H., & Hynda O. (2022). The Ukrainian economy offshoring: estimation of factors' impact and developing measures to combat. *Business: Theory and Practice*, 23(2), 347–356. <https://doi.org/10.3846/btp.2022.14509>
2. Ortynskiy V., Tsymbaliuk M., Hobela, V., Kashchuk M. (2021). Legal support of socio-economic development model genesis in post-industrial society. *Фінансово-кредитна діяльність: проблеми теорії та практики*. Том 5. № 40. С. 535–545. <https://doi.org/10.18371/fcaptp.v4i35.245212>
3. Андрушків Т. Депозитна політика комерційного банку та напрями її вдосконалення. *Українська наука: минуле сучасне, майбутнє*. 2012. №. 17. С. 3–13.
4. Аржевітін С. Сукупні заощадження населення в умовах державного регулювання ресурсного потенціалу банків України. *Економіст*. 2020. № 10. С. 20–22.
5. АТ «Укрсиббанк» : веб-сайт. URL: <http://my.ukrsibbank.com> (дата звернення: 16.04.2025).
6. Бартош О. Депозитна політика банку та основні етапи її формування. *Вісник УБС НБУ*. 2008. № 3. С. 97–101.
7. Башнянин Г. І. Система управління інвестиційними ризиками банку. *Науковий вісник НЛТУ*. 2015. Випуск 21.14. С. 332–336.
8. Бездітко Ю. М. Вплив банків з іноземним капіталом на показники діяльності банківської системи України. *Гроші, фінанси та кредит*. 2017. №4. С. 115–119.
9. Болгар Т. М. Фінансова безпека банків в умовах ринкової трансформації економіки України: автореф. дис. ... канд. екон. наук: 08.00.08 / Т.М. Болгар. Суми, ДВНЗ "УАБС НБУ", 2009. 21 с.
10. Брежнєва-Єрмоленко О. В., Золотарьова О. В., Москаленко К. О. Детермінанти інвестиційної діяльності комерційних банків. *Економіка і суспільство*. 2018. № 19. С. 948–954.

11. Буйда К. Проактивне управління кредитними ризиками в банківській системі України. *Економіст*. 2016. № 12. С. 18–21.
12. Вдоенко Л. О. Кредитна політика системно важливих банків в Україні *Екооміка. Фінанси. Менеджмент: актуальні питання науки і практики*. № 11. 2018. С. 73–83.
13. Волкова Н. І. Сутність інноваційної кредитної політики банку. *Економіка і організація управління. Збірник наукових праць*. Випуск № 5. 2015. С. 3–12.
14. Гнедіна К. В. Стратегія: сутність, переваги, методи та прийоми формування. *Бізнес Інформ*. 2019. №2. С. 14–20. URL: <https://doi.org/10.32983/2222-4459-2019-2-14-20> (дата звернення: 28.03.2025).
15. Гобела В. В., Леськів Г. З., Фляк В. М. Моделювання системи ризик-орієнтованого управління підприємством. *Вісник ЛьвДУВС. Серія економічна*. 2023. Вип. 2. С. 10–20.
16. Гобела В. В., Халіна О. В., Сидоренко Я. А. Сутність фінансової розвідки в безпековому просторі держави. *Ефективна економіка*. 2024. № 7. <https://doi.org/10.32702/2307-2105.2024.7.77>
17. Гребенюк Н. В. Формування технологій стратегічного управління банком, ураховуючи його функціональні особливості. *Науковий вісник Ужгородського національного університету. Серія: Міжнародні економічні відносини та світове господарство*. Випуск 7, частина 1, 2016. С. 92–95.
18. Добровольська О. В., Острініна О. П., Лопаткіна А. О. Аналіз сучасного стану активів та пасивів комерційного банку. *Науковий вісник Херсонського державного університету*. Випуск 27. Частина 3. 2017. С. 28–32.
19. Єщенко М., Михайличенко В. Розроблення стратегії і тактики управління підприємством у сучасній Україні. *Галицький економічний вісник*. Вип. 3 (64), 2020. С. 157-162. URL: https://doi.org/10.33108/galicianvisnyk_tntu (дата звернення: 10.03.2025).

20. Житар М. О., Ананьєва Ю. В. Державна політика регулювання та стимулювання інвестиційної діяльності банків України. *Науковий вісник Ужгородського Університету*. 2019. № 1 (53). С. 163–167.
21. Зачосова Н. В. Особливості забезпечення фінансової безпеки комерційних банків в Україні. *Науковий вісник: Фінанси, банки, інвестиції*. 2011. № 4. С. 74–78.
22. Ілляшенко Н. С., Шипуліна Ю. С., Мельник Ю. М. Формування «системної карти» стратегічного управління розвитком. *Актуальні проблеми економіки*. 2017. № 1. с. 119-128. URL: http://nbuv.gov.ua/UJRN/ape_2017_1_14 (дата звернення: 10.03.2025).
23. Калусенко В. В. Аналіз інвестиційного портфеля банків України та стратегія управління ним. *Збірник наукових праць Університету державної фіскальної служби України*. 2019. № 1. С. 63–78.
24. Кащєєва В. Ю., Швидкий В. О. Управління рентабельністю банку на основі факторного аналізу. *Науковий вісник Херсонського державного університету*. Випуск 15, частина 4. 2015. С. 114–117.
25. Киш Л. М. Стратегічне управління, як основна частина менеджменту підприємства. 2019. Випуск 38-1. URL: http://bses.in.ua/journals/2019/38_1_2019/23.pdf (дата звернення: 10.03.2025).
26. Кльоба Л. Г. Ризик-менеджмент банківської інвестиційної діяльності. *Вісник Національного банку України*. 2010. № 1. С. 44–47.
27. Коваленко В. В. Система ризик-менеджменту кредитно-інвестиційного діяльності в банках. *Інфраструктура ринку*, 2019. Вип. 37. С. 584–590.
28. Ковшар А.І. Шляхи удосконалення депозитної політики на сучасному етапі *Фінанси України*. 2009. № 7. С. 13–18.
29. Колеснік Я. В. Статистична оцінка ефективності стратегічного управління банківською діяльністю. URL: 10.31767/su. 1(88)2020.01.06 (дата звернення: 22.04.2025).
30. Костоґриз В. Г. Інновації банків з іноземним капіталом у банківській системі України. *Науковий вісник Херсонського державного університету*. 2016. Вип. 16(2). С. 108–111.

31. Крамар І. Ю., Мариненко Н. Ю. Передумови інтернаціоналізації машинобудівних підприємств. *Галицький економічний вісник*. 2018. Том 55. №2. С. 27–40.
32. Крупка І. М. Фінансово-економічна безпека банківської системи України та перспективи розвитку національної економіки. *Бізнесінформ*. 2012. № 6. С. 168–175.
33. Лавров Р. В. Ризики комерційного банку та ризик-менеджмент в умовах фінансово-економічної нестабільності. *Науковий вісник ЧДІЕУ*. 2011. № 2 (10). С. 196–201.
34. Лук'янов В. С. Сучасні фінансові ринки / В.С. Лук'янов. Київ : Знання, 2016. 479 с.
35. Луців Б. Л., Заславська О. І. Оцінка ризиків кредитно-інвестиційної діяльності комерційних банків України. *Світ фінансів*. 2013. № 1. С. 18–28.
36. Макаренко Ю. П., Самойлова Д. О. Теоретичні аспекти управління кредитним портфелем банківської установи. *Економіка та держава*. 2020. № 6. С. 87–91.
37. Марченко О. В. Оцінка кредитно-інвестиційної діяльності банку. *Молодий вчений*. 2017. № 2 (42). С. 277–294.
38. Менеджмент інвестиційної діяльності : підручник / [М. П. Бутко, І.М. Бутко, М. Ю. Дітковська та ін.]; за заг. ред. М. П. Бутка. Київ : Центр учбової літератури, 2018. 480 с.
39. Озерчук О. В. Управління інвестиційним портфелем банків в Україні: теоретичні та прикладні аспекти. *Наукові праці НДФІ*, 2019. № 1 (86). С. 85–100.
40. Приказюк Н., Сацюк М. Банки з іноземним капіталом в Україні: суперечності та перспективи розвитку. *Економічний аналіз*. 2020. Том 30. № 1. Частина 1. С. 183–191.
41. Франчук В. І., Гобела В. В. Моделювання безпекового середовища підприємства крізь призму інвестиційної безпеки. *Цифрова економіка та економічна безпека*. 2023. № (9 (09)). С. 85–89.

42. Харченко Т. О. Стратегічне управління банківською структурою в умовах трансформації банківської системи. URL: DOI: 10.30525/978-9934-588- 61-7-38 (дата звернення: 10.01.2025).