Міністерство освіти і науки України
Дніпровський державний аграрно-економічний університет
Факультет обліку і фінансів

Кафедра обліку, оподаткування та управління фінансово-економічною безпекою

ДОПУСТИТИ ДО ЗАХИСТУ
В ЕКЗАМЕНАЦІЙНІЙ КОМІСІЇ:

Завідувач кафедри,
к.е.н., доцент
_____Ольга ГУБАРИК
«____» _____ 20___ р.

КВАЛІФІКАЦІЙНА РОБОТА

на тему: «Удосконалення інформаційного забезпечення системи економічної безпеки»

Освітньо-професійна програма «Управління фінансово-економічною безпекою»
Спеціальність 073 «Менеджмент»
Ступінь вищої освіти: Магістр

Здобувачка **Марина ЛУНЬОВА**

Науковий керівник,

д.держ.упр., проф. **Леся ВАСІЛЬЄВА**

Дніпро – 2025

ДНІПРОВСЬКИЙ ДЕРЖАВНИЙ АГРАРНО-ЕКОНОМІЧНИЙ УНІВЕРСИТЕТ

Факультет: Обліку і фінансів
Кафедра: Обліку, оподаткування та управління фінансово-економічною безпекою
Освітньо-професійна програма: «Управління фінансово-економічною безпекою»
Спеціальність: 073 «Менеджмент»
Ступінь вищої освіти: Магістр

З А Т В Е Р Д Ж У Ю
Зав. кафедри _____
«_____»_____ 202__р.

З А В Д А Н Н Я
на підготовку кваліфікаційної роботи

Луньовій Марині Володимирівні
(прізвище, ім'я, по батькові)

1. Тема роботи: «Удосконалення інформаційного забезпечення системи економічної безпеки»

Науковий керівник: Васільєва Леся Миколаївна, д.держ.упр., професор
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

затверджені наказом по ДДАЕУ від «14» жовтня 2025 року № 3070

2. Термін подання здобувачем роботи: 08.12.2025 р.

3. Вихідні дані до роботи: офіційні матеріали Національного банку України, інші нормативно-правові акти та література, пов'язані з темою роботи, річні звіти Акціонерного товариства «УНІВЕРСАЛ БАНК».

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити) 1. Теоретико-методичні засади інформаційного забезпечення системи економічної безпеки банківських установ. 2. Практичні аспекти формування інформаційного забезпечення системи економічної безпеки АТ «УНІВЕРСАЛ БАНК». 3. Удосконалення інформаційного забезпечення системи економічної безпеки банківських установ.

5. Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень) Інтегральна оцінка рівня складових економічної безпеки АТ «УНІВЕРСАЛ БАНК». Порівняльна оцінка ефективності управління ризиками до та після впровадження аналітичної платформи моніторингу ризиків. Протоколи реагування на кіберінциденти та навчання персоналу Основні інструменти штучного інтелекту та їх функціональне застосування в банківській системі економічної безпеки. Оцінка модулів АТ «УНІВЕРСАЛ БАНК». Карта ризиків АТ «УНІВЕРСАЛ БАНК». Концепція «єдиного вікна» інтегрованого моніторингу та управління ризиками.

Комплексна оцінка фінансового стану АТ «УНІВЕРСАЛ БАНК».

6. Консультанти розділів роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв

7. Дата видачі завдання_____лютий 2025_____

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів кваліфікаційної роботи	Термін виконання етапів роботи	Примітка
1	Теоретико-методичні засади інформаційного забезпечення системи економічної безпеки банківських установ	лютий 2025	
2	Фінансово-економічна характеристика АТ «УНІВЕРСАЛ БАНК»	березень 2025	
3	Характеристика роботи служби економічної безпеки банку та оцінка її стану за окремими складовими	квітень 2025	
4	Оцінка процесу формування інформаційного забезпечення системи економічної безпеки АТ «УНІВЕРСАЛ БАНК»	червень 2025	
5	Удосконалення інформаційного забезпечення системи економічної безпеки банківських установ	жовтень 2025	
6	Вступ. Висновки. Оформлення кваліфікаційної роботи	грудень 2025	

Здобувач _____ _____Марина ЛУНЬОВА_____
(підпис) (прізвище та ініціали)

Науковий керівник _____ _____Леся ВАСІЛЬЄВА_____
(підпис) (прізвище та ініціали)

ЗМІСТ

Р Е Ф Е Р А Т

Тема «Удосконалення інформаційного забезпечення системи економічної безпеки»

Кваліфікаційна робота: 60 ст. основного тексту, 9 табл., 14 рис., 4 додатки, 50 літературних джерел.

Об'єктом дослідження є процес інформаційного забезпечення системи економічної безпеки.

Предмет дослідження - теоретичні та практичні підходи щодо удосконалення інформаційного забезпечення системи економічної безпеки банківських установ.

Методи дослідження. Теоретична і методична основа дослідження включає широкий спектр загальновідомих методів, таких як аналіз і синтез, системний підхід, порівняння, метод візуалізаці, економіко-математичні методи та інші.

Досліджено теоретико-методичні засади інформаційного забезпечення системи економічної безпеки банківських установ. Проаналізовано фінансово-економічний стан та охарактеризовано роботу служби економічної безпеки АТ «УНІВЕРСАЛ БАНК». Проведено оцінку процесу формування інформаційного забезпечення системи економічної безпеки АТ «УНІВЕРСАЛ БАНК». Запропоновано напрями вдосконалення інформаційного забезпечення системи економічної безпеки банку. Визначено інтелектуальні технології як інструмент удосконалення інформаційного забезпечення системи економічної безпеки банківських установ. Проведено оцінювання ефективності інформаційно-аналітичної системи банку за допомогою економіко-математичних методів.

Ключові слова

ЗАБЕЗПЕЧЕННЯ, ОЦІНКА, БАНКІВСЬКІ УСТАНОВИ, РИЗИКИ, СИСТЕМА ЕКОНОМІЧНОЇ БЕЗПЕКИ, ІНФОРМАЦІЙНА БЕЗПЕКА, ІНТЕЛЕКТУАЛЬНІ ТЕХНОЛОГІЇ

ABSTRACT

Topic «Improving information provision of the economic security system»

Qualification work: 60 p. of the main text, 9 tables, 14 figures, 4 appendices, 50 literary sources.

The object of the study is the process of information provision of the economic security system.

The subject of the study is theoretical and practical approaches to improving the information support of the economic security system of banking institutions.

Research methods. The theoretical and methodological basis of the research includes a wide range of well-known methods, such as analysis and synthesis, system approach, comparison, visualization method, economic-mathematical methods and others.

The theoretical and methodological principles of information support of the system of economic security of banking institutions have been studied. The financial and economic situation was analyzed and the work of the economic security service of JSC «UNIVERSAL BANK» was characterized. The evaluation of the process of formation of information support of the economic security system of JSC «UNIVERSAL BANK» was carried out. Directions for improving the information provision of the bank's economic security system are proposed. Intelligent technologies are defined as a tool for improving the information support of the economic security system of banking institutions. The effectiveness of the bank's information and analytical system was evaluated using economic and mathematical methods.

Key words

SECURITY, EVALUATION, BANKING INSTITUTIONS, RISKS, SYSTEM OF ECONOMIC SECURITY, INFORMATION SECURITY,

INTELLECTUAL TECHNOLOGIES

ВСТУП

Актуальність теми дослідження. Ефективне функціонування банківських установ у сучасних умовах посиленої конкуренції, цифровізації фінансових послуг та зростання рівня зовнішніх і внутрішніх загроз неможливе без формування надійної системи економічної безпеки. Одним із ключових її компонентів виступає інформаційне забезпечення, яке забезпечує своєчасне отримання, оброблення та використання даних для ухвалення управлінських рішень. В умовах стрімкого розвитку кіберзлочинності, ускладнення фінансових схем, активного використання онлайн-сервісів та дистанційного банкінгу значно зростає потреба в побудові комплексної, інтегрованої та аналітично орієнтованої системи інформаційної підтримки, здатної виявляти ризики на ранніх етапах та забезпечувати стійкість банку до дестабілізуючих впливів.

Система інформаційного забезпечення економічної безпеки банківських установ передбачає формування єдиного інформаційного простору, інтеграцію внутрішніх і зовнішніх джерел даних, застосування сучасних цифрових технологій, аналітичних платформ та засобів кіберзахисту. Її якісне функціонування слугує основою для моніторингу загроз, оцінювання ризиків, запобігання фінансовим махінаціям, збереження конфіденційної інформації, а також підтримки стабільної діяльності банківського сектору. Саме тому дослідження теоретичних і практичних аспектів інформаційного забезпечення системи економічної безпеки банків є актуальним і має важливе наукове та прикладне значення.

Серед науковців які досліджують питання інформаційного забезпечення системи економічної безпеки суб’єктів підприємницької діяльності, і зокрема, банківських установ можемо виділити: Бандурка О.М., Варналій З. С., Васильців Т.Г., Гаряга Л.О., Куліш Р.Р., Диба М.О., Зубок М.І.,

Яременко С.М., Жарій Я. В., Світлична В.Ю., Сидоренко І. В., Коваленко В.В., Отенко І.П., Ролдугіна Ю.В., Ковальова І.В., Фурман В. М. та інші. Проте, надивлячись на значну увагу до даного питання, є коло питань, в т.ч інтелектуальні технології як інструмент удосконалення інформаційного забезпечення системи економічної безпеки банківських установ потребують подальшого дослідження.

Мета і завдання дослідження. Метою кваліфікаційної роботи є обґрунтування теоретичних засад і розроблення практичних рекомендацій щодо удосконалення інформаційного забезпечення системи економічної безпеки банківських установ.

Виходячи з поставленої мети, необхідно виконати наступні завдання:

- дослідити теоретико-методичні засади інформаційного забезпечення системи економічної безпеки банківських установ;

- проаналізувати фінансово-економічний стан та охарактеризувати роботу служби економічної безпеки АТ «УНІВЕРСАЛ БАНК»;

- провести оцінку процесу формування інформаційного забезпечення системи економічної безпеки АТ «УНІВЕРСАЛ БАНК»;

- запропонувати напрями вдосконалення інформаційного забезпечення системи економічної безпеки банку;

- визначити інтелектуальні технології як інструмент удосконалення інформаційного забезпечення системи економічної безпеки банківських установ;

- провести оцінювання ефективності інформаційно-аналітичної системи банку за допомогою економіко-математичних методів.

Об’єктом дослідження є процес інформаційного забезпечення системи економічної безпеки.

Предмет дослідження - теоретичні та практичні підходи щодо удосконалення інформаційного забезпечення системи економічної безпеки банківських установ.

Методи дослідження. Теоретична і методична основа дослідження включає широкий спектр загальновідомих методів, таких як аналіз і синтез,

системний підхід, порівняння, метод візуалізації, економіко-математичні методи та інші.

Інформаційною базою для проведення дослідження слугували офіційні матеріали Національного банку України, інші нормативно-правові акти та література, пов'язані з темою роботи, річні звіти Акціонерного товариства «УНІВЕРСАЛ БАНК».

Наукова новизна одержаних результатів:

удосконалено:

- підходи щодо розробки концепції «єдиного вікна» інтегрованого моніторингу, яка відображає всі основні категорії ризиків та їхнє оновлення в режимі реального часу для оперативного управління;

набуло подальшого розвитку:

- підходи до впровадження банківського корпоративного штучного інтелект-асистента, який працює виключно у закритому, контрольованому середовищі банку (on-premise або Private Cloud);
- практичні заходи багаторівневого контролю доступу та шифрування даних: розмежування доступу; шифрування даних; моніторинг подій у реальному часі; багатофакторна аутентифікація;
- рекомендації щодо здійснення оцінювання ефективності інформаційно-аналітичної системи банку за допомогою економіко-математичних методів.

Апробація одержаних результатів. Основні положення і результати дослідження доповідались на конференціях «Облік, аудит, оподаткування та звітність у системі забезпечення економічної стійкості підприємств» (м. Дніпро, 2025 р.).

Публікації. За результатами дослідження опубліковано 1 статтю, загальним обсягом 0,6 ум. друк. арк.

Кваліфікаційна робота складається з вступу, трьох розділів, висновків, додатків, списку джерел 50 найменувань, містить 13 таблиць, 7 рисунків, 4 додатки. Основний зміст роботи викладено на 60 ст. друкованого тексту.

РОЗДІЛ 1. ТЕОРЕТИКО-МЕТОДИЧНІ ЗАСАДИ ІНФОРМАЦІЙНОГО ЗАБЕЗПЕЧЕННЯ СИСТЕМИ ЕКОНОМІЧНОЇ БЕЗПЕКИ БАНКІВСЬКИХ УСТАНОВ

1.1. Сутність та значення інформаційного забезпечення в системі економічної безпеки банківських установ

У сучасних умовах функціонування банківської системи України, які характеризуються високим рівнем невизначеності, економічною турбулентністю, посиленням фінансових ризиків і воєнними викликами, особливого значення набуває проблема забезпечення економічної безпеки банківських установ. Одним із ключових елементів системи економічної безпеки банку є інформаційне забезпечення, яке виступає основою для ідентифікації, оцінки та нейтралізації загроз, що впливають на стабільність функціонування фінансово-кредитної установи.

У контексті банківської діяльності інформаційне забезпечення – це не просто набір даних чи технічних засобів їх обробки, а комплексна система збору, аналізу, зберігання та захисту інформації, що використовується для підтримки управлінських рішень і забезпечення фінансової стійкості банку. Банківська система є одним із найбільш інформаційно насичених секторів економіки, де інформація має цінність, адже вона впливає на репутацію, довіру клієнтів, рівень ризиків, ліквідність та конкурентоспроможність установи.

У наукових працях вітчизняних дослідників, зокрема Гаряга Л.О., Куліш Р.Р. [10], Жарій Я. В., Сидоренко І. В. [14], Крамаренко К., Вінниченко О. [24] питання інформаційного забезпечення банків розглядається як центральні складова економічної безпеки, без якої неможливе ефективне управління ризиками. Так, Мордань Є.Ю., Журавка О.С., Діденко К.В., Кравченко Я.І. [35] зазначають, що інформаційна система

банку є інфраструктурною основою для ухвалення фінансових рішень і формування управлінської політики безпеки. Доцільно погодитися з висловленням Світличної В.Ю., що «одним із найважливіших критеріїв функціонування банківської системи є інформаційна безпека як всієї системи, так і її частин: центрального і комерційних банків» [43]. На думку Ролдугіна Ю.В., Ковальова І.В., інформаційне забезпечення банку виступає базисом формування аналітичного простору для управління ризиками ліквідності, кредитними ризиками та шахрайства [41].

Отже, у сфері банківського менеджменту інформаційне забезпечення економічної безпеки можна визначити як цілеспрямований процес створення, обробки, аналітичного використання та захисту інформаційних ресурсів, необхідних для підтримання стабільності фінансових потоків, збереження конфіденційності банківський даних і своєчасного реагування на ризики. Його ефективність безпосередньо визначає здатність банку запобігати кризовим ситуаціям, мінімізувати втрати від шахрайства, кіберзагроз і несанкціонованого доступу до фінансової інформації.

До прикладу Онищенко С., Глушко А. зазначають, що у сучасних умовах цифровізації банківської діяльності інформаційне забезпечення економічної безпеки набуває стратегічного значення, адже саме якість, достовірність і швидкість обробки даних визначають конкурентоспроможність фінансових установ [37]. Впровадження інтелектуальних аналітичних систем, технологій Big Data, блокчейну та штучного інтелекту дозволяє банкам здійснювати багаторівневий моніторинг транзакцій, виявляти нетипові фінансові операції, підвищувати рівень захисту клієнтських даних і забезпечувати прозорість управлінських процесів. Таким чином, інформаційна безпека стає невід’ємною складовою корпоративної стратегії, спрямованої на підвищення фінансової стійкості, довіри клієнтів і ефективності управління ризиками.

Дослідивши теоретичні аспекти щодо визначення сутності інформаційного забезпечення економічної безпеки банківських установ ми

дійшли висновку, що існують два основні підходи:

- ресурсний підхід розглядає інформацію як один із ключових економічних ресурсів банку, поряд із фінансовими, трудовими та технологічними. Прихильники цього підходу (Васильців Т.Г.[8], Захаров О. [17], Коваленко В. В. [21]) підкреслюють, що інформація має власну вартість, потребує управління, обліку, контролю й захисту;

- функціональний підхід, який підтримують Марущак А.І. [33], Лазаришина І. [26], Ліхоносова Г.С. [29], які трактують інформаційне забезпечення як сукупність організаційно-технологічних процесів, що забезпечують функціонування системи економічної безпеки банку. Тобто основна увага приділяється не лише накопиченню інформації, а її аналізу, фільтрації та використанню в управлінських рішеннях.

За допомогою табл.1.1 наведемо узагальнення наукових підходів.

Таблиця 1.1

Наукові підходи до визначення сутності інформаційного забезпечення економічної безпеки банківських установ

Автор	Зміст визначення	Основний акцент
Марущак А.І. [33]	Система формування й використання інформаційних потоків, що забезпечують фінансову стійкість банку	Управлінсько-фінансовий
Захаров О. [17]	База аналітичної інформації для виявлення, оцінки та мінімізації ризиків банківської діяльності	Аналітико-ризиковий
Коваленко В. В. [21]	Механізм інформаційного моніторингу стану фінансової та економічної безпеки банку	Контрольно-аналітичний
Васильців Т.Г.[8]	Сукупність процесів збору, аналізу та захисту інформації про внутрішні і зовнішні загрози	Захисно-технологічний
Ліхоносова Г.С. [29]	Інтеграційна складова між управлінськими, контрольними та аналітичними функціями банківської системи	Інтеграційно-системний

Як вино з таблиці, у більшості визначень інформаційне забезпечення банку трактується як динамічна управлінська система, спрямована на формування знань для прийняття рішень у сфері безпеки. Полеміка між

науковцями полягає у визначенні головної домінанти: чи є інформаційне забезпечення технічною складовою інфраструктури банку, чи воно є стратегічним ресурсом, що визначає ефективність управління ризиками.

Відмітимо, що роль інформаційного забезпечення у банківській безпеці багатовимірне. Як відмічає Лісняк А. Є. [28] воно виконує функції збірки, обробки, аналізу, контролю, прогнозування та захисту даних, які стосуються як внутрішніх операцій банку, так і його зовнішнього середовища. Зокрема, можна виділити такі ключові функції:

- аналітична – забезпечує виявлення відхилень від норм діяльності, формування системи раннього попередження ризиків;

- контрольна – здійснює моніторинг виконання регламентів, лімітів та нормативів НБУ;

- прогностична – дозволяє оцінювати тенденції ринку, фінансові показники клієнтів і партнерів;

- захисна – забезпечує захист інформації від несанкціонованого доступу, кіберзагроз і маніпуляцій;

- комунікаційна – сприяє ефективному інформаційному обміну між підрозділами банку, НБУ, партнерами та клієнтами.

Інформаційне забезпечення є не лише інструментом аналітики, а й компонентом корпоративного управління, адже воно формує основу для прийняття рішень керівництвом банку щодо управління капіталом, кредитивним портфелем, валютними ризиками та ліквідністю [30].

У банківській діяльності інформаційні ресурси мають подвійну природу (рис.1.1).

Рис. 1.1. Інформаційні ресурси банку як елемент безпеки

Якість інформаційних ресурсів визначає якість управлінських рішень. Недостовірні або неповні дані призводять до помилкової оцінки ризиків, що особливо небезпечно у сфері кредитування, інвестицій та операцій з цінними паперами.

Можемо констатувати, що інформаційне забезпечення банківських установ виконує подвійну роль:

- з одного боку, воно є базою для аналітичного управління ризиками;

- з іншого - механізмом забезпечення стійкості до зовнішніх загроз, включаючи кібератаки, фішингові схеми та інформаційні маніпуляції.

У підсумку, ефективність інформаційного забезпечення визначає здатність банку адаптуватися до ринкових змін, підтримувати довіру клієнтів і зберігати стабільність діяльності навіть у кризових умовах.

Підсумовуючи викладене, можна зробити висновок, що інформаційне забезпечення в системі економічної безпеки банківських установ є інтегрованою підсистемою управління, яка забезпечує збалансоване функціонування аналітичних, технічних і захисних механізмів. Воно не лише формує інформаційні ресурси для аналізу ризиків, але й створює основу для стратегічного планування, підвищення ефективності операцій і зміцнення репутаційної безпеки банку.

З огляду на виклики сьогодення - військові дії, коливання фінансових ринків, посилення кіберзагроз інформаційне забезпечення має розглядатися не як допоміжна функція, а як стратегічний інструмент забезпечення

економічної стійкості банківської системи України.

1.2. Класифікація, структура та джерела інформації для управління економічною безпекою

Ефективне функціонування системи економічної безпеки банківських установ неможливе без надійного, повного та оперативного інформаційного забезпечення. У сучасних умовах трансформації фінансового ринку, воєнних викликів, нестабільності банківського середовища й загострення конкурентної боротьби саме якість і достовірність інформації визначають рівень стійкості фінансових інститутів, їх здатність вчасно реагувати на загрози, ухвалювати стратегічно обґрунтовані рішення й запобігати кризовим явищам.

Як відмічає Родченко С., інформаційне забезпечення безпеки банку – це комплекс процесів формування, збирання, передачі, оброблення, аналізу та використання даних, необхідних для оцінки ризиків і контролю фінансових потоків [42]. Інформація в банку виступає не лише ресурсом, а й стратегічними активом, який формує основу для забезпечення конкурентних переваг і захисту від зовнішніх та внутрішніх загроз.

В умовах війни, кібератак, макроекономічних шоків і санаційної політики питання якості інформаційних потоків набуває особливого значення. Недостовірна або несвоєчасна інформація може призвести до помилкових управлінських рішень, фінансових втрат, витоку банківської таємниці або навіть дестабілізації діяльності установи.

Інформація, що використовується для забезпечення економічної безпеки банківських установ, характеризується багатовимірністю та різноманіттям форм. У науковій літературі існують різні підходи до класифікації інформації. Так, Фурман В. М., Зачосова Н. В. пропонує ділити її за ознаками (внутрішня, зовнішня), за способом відображення (кількісна, якісна), за ступенем конфіденційності (відкрита, службова, банківська

таємниця) [48]. На відміну від цього, Зубок М.І. підкреслює, що для банківського сектору ключовим є поділ інформації за функціональною ознакою – тобто за тим, яку роль вона виконує в системі економічної безпеки – аналітичну, контрольну, моніторингову, прогнозну [18]. Узагальнюючи ці підходи, доцільно подати комплексну класифікацію інформації для управління економічною безпекою банку (табл. 1.2).

Таким чином, можемо констатувати, що інформаційна система економічної безпеки банку – це структурно впорядкований комплекс, який охоплює підсистему збору, оброблення, аналізу та зберігання інформації, що забезпечують управлінські процеси.

Таблиця 1.2

Класифікація інформації в системі економічної безпеки банківської установи

Ознака класифікації	Вид інформації	Характеристика	Значення для економічної безпеки
За джерелом виникнення	Внутрішня / зовнішня	Дані бухгалтерського обліку, управлінської звітності, інформація від клієнтів, контрагентів, НБУ, ринку	Забезпечення комплексності аналізу ризиків
За ступенем конфіден-ційності	Відкрита / обмежена / таємна	Публічна звітність, службова інформація, банківська таємниця	Контроль доступу до інформаційних ресурсів
За змістом	Фінансова / організаційна / правова / аналітична	Відображає стан активів, операцій, нормативно-правові аспекти, показники ефективності	Використовуєтьс я для діагностики фінансової стійкості
За формою представлення	Документальна / електронна / вербальна	Звіти електронні, бази даних, усні повідомлення	Забезпечення різних рівнів управління
За призначенням	Інформація стратегічного, тактичного, оперативного рівня	Дані для стратегічних рішень, поточного управління, реагування на загрози	Підвищення ефективності антикризового управління

Джерело: узагальнено автором [22, 49]

Її архітектура повинна забезпечувати цілісність даних, доступність для уповноважених осіб, багаторівневий захист і можливість аналітичного

моделювання.

Відмітимо, що за логікою побудови така система включає такі підсистеми (рис.1.2):

Як підкреслює Кульчицький І. І., система економічної безпеки сучасних банків є багатовимірною, де кожен рівень має власні канали збору й обробки інформації – від транзакцій клієнтів до макроекономічних прогнозів [25]. Ефективність функціонування такої системи залежить від інтеграції між підрозділами банку – аналітичним, безпековим, інформаційним та управлінським.

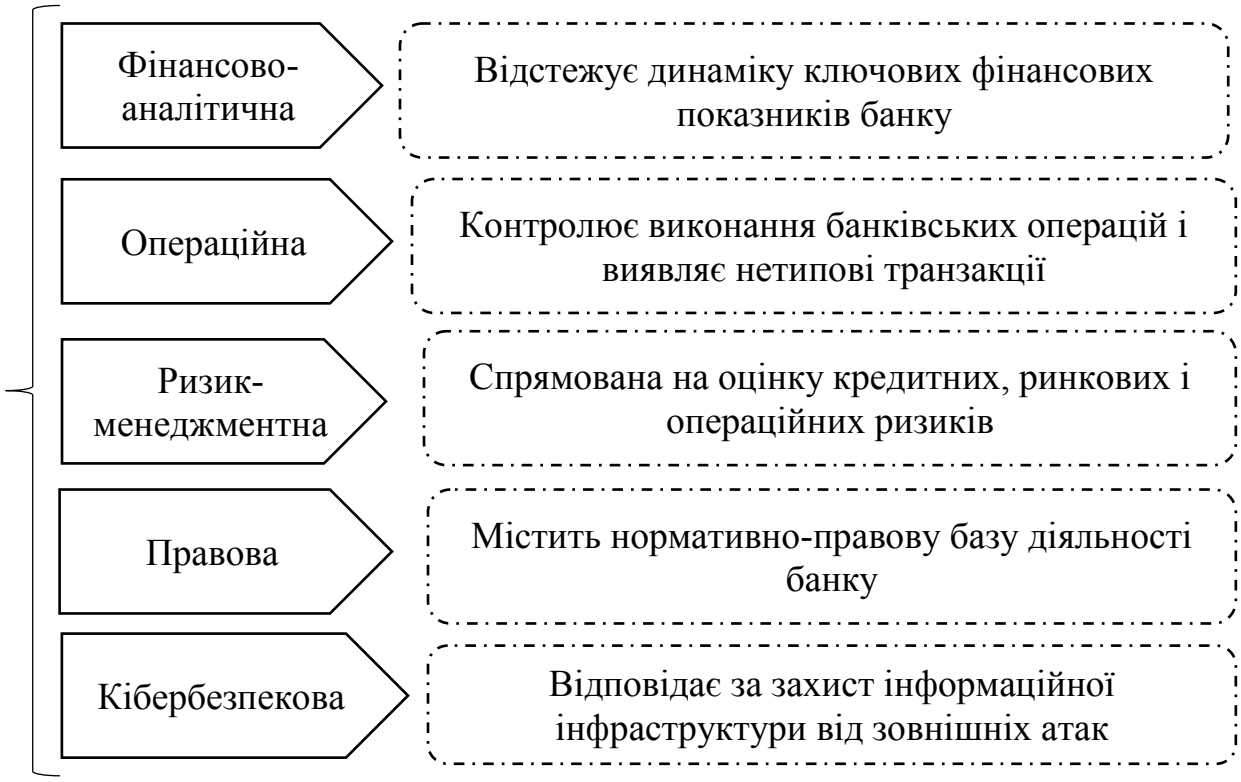

Рис. 1.2. Інформаційна система економічної безпеки банку

Джерело: сформовано автором

Основними принципами формування ефективної системи інформаційного забезпечення є:

- комплексність – охоплення всіх напрямів діяльності банку;
- оперативність – швидкість оновлення даних і реагування на загрози;
- достовірність і релевантність – використання перевірених джерел;

- безперервність – постійний моніторинг та аналіз даних;

- конфіденційність – дотримання вимог банківської таємниці;

- інтеграція – поєднання інформаційних потоків з різних систем;

- адаптивність – здатність системи швидко пристосовуватися до змін середовища.

Серед науковців існує дискусія щодо оптимального підходу до побудови інформаційної системи економічної безпеки банку. Гречка В., Островський В., Білий М. вважають, що головним є створення єдиного інформаційного простору, який об'єднує фінансову, правову й операційну інформацію [11]. Натомість Клюско Л.А., Москаленко Н.В. підкреслює, що надмірна централізація інформаційних потоків створює ризики витоку даних і потребує багаторівневих систем контролю [20]. Деякі автори, зокрема, Барановський О., Путінцева Т. пропонують орієнтуватися на гібридну модель, де частина інформації зберігається у централізованому сховищі, а частина – в окремих підсистемах із різним рівнем доступу [3]. Ми переконані, що саме такий підхід забезпечує баланс між доступністю та безпекою.

Отже, , інформаційне забезпечення економічної безпеки банківських установ є багаторівневою системою, що поєднує різні джерела, канали й типи інформації. Ефективність її функціонування залежить від якості інформаційних потоків, узгодженості між підрозділами банку та надійності захисту даних. В умовах воєнного стану, цифровізації та глобальних ризиків побудова сучасної інформаційної системи безпеки є одним із пріоритетів стратегічного управління банками України.

1.3. Інформаційна безпека як основа фінансової стабільності: досвід українських банків

В умовах російської агресії та прискореної цифровізації банківських послуг, українські фінансові установи опинилися перед новими викликами,

де кіберзагрози стали реальною загрозою для стабільності всієї банківської системи. Інформаційна безпека вже не обмежується технічними питаннями захисту серверів - вона стала критично важливим фактором, що визначає спроможність банків продовжувати роботу навіть в екстремальних умовах.

Українські банки, як частина критичної інфраструктури держави, відчули на собі, що навіть локальний збій в системах безпеки може мати каскадний ефект на всю економіку. Досвід останніх років показав пряму залежність між якістю кіберзахисту банку та його здатністю зберігати фінансову стійкість під час кризи [1].

Статистика свідчить про масштаби проблеми: якщо у 2020 році середній банк фіксував 2-3 серйозні кіберінциденти на рік, то у 2025 році ця цифра зросла до 40-45 випадків. При цьому економічні втрати від одного інциденту можуть сягати десятків мільйонів гривень, не враховуючи репутаційні ризики.

Міжнародний досвід показує, що країни з розвиненою банківською системою витрачають на кібербезпеку 8-12% від загального IT-бюджету [50]. В Україні цей показник до 2022 року становив лише 3-5%, що частково пояснює вразливість системи до масованих атак.

Мета цього дослідження - проаналізувати, як саме інформаційна безпека впливає на фінансову стабільність банків, вивчити конкретні випадки кіберінцидентів в Україні та оцінити їх економічні наслідки. Для цього використано системний підхід до аналізу ризиків та методи оцінки економічних втрат, а також порівняння вимог НБУ з міжнародними стандартами.

Регуляторні вимоги НБУ до інформаційної безпеки банків. Національний банк України суттєво посилив вимоги до кібербезпеки банків після серії масштабних атак 2016-2017 років. Ключовим документом стала Постанова №64 "Про затвердження Положення про організацію системи управління ризиками в банках України", яка вперше на законодавчому рівні закріпила вимоги до управління ризиками інформаційно-комунікаційних

технологій.

Згідно з цією постановою, банки зобов'язані створити окремий підрозділ з управління ризиками ІКТ або призначити відповідального співробітника, розробити та затвердити політику управління ризиками ІКТ, впровадити систему моніторингу та звітності про кіберінциденти, а також забезпечити регулярне тестування систем на стійкість до кібератак [3].

Особливу увагу НБУ приділяє вимогам до безперервності діяльності. Банки повинні забезпечувати відновлення критичних функцій протягом встановленого часу: система міжбанківських розрахунків має відновлюватися максимум за 2-4 години, клієнтське обслуговування - за 6-8 годин, внутрішні системи управління ризиками - за 12 годин.

Цікавим нововведенням стала вимога до проведення регулярних стрес-тестів кіберстійкості. Банки повинні моделювати сценарії різних типів атак та оцінювати свою готовність до них. Результати цих тестів подаються до НБУ щокварталу. За порушення вимог до кібербезпеки НБУ може застосовувати серйозні санкції: від попереджень до обмеження операцій банку. У 2023 році три банки отримали штрафи на загальну суму 15 мільйонів гривень за недотримання вимог до захисту персональних даних клієнтів.

Теоретичні основи зв'язку між інформаційною безпекою та фінансовою стійкістю. Традиційно фінансову стійкість банку оцінювали через показники капіталу, ліквідності та якості кредитного портфеля. Однак сучасні реалії змусили НБУ розширити це поняття, включивши операційну стійкість - здатність банку швидко відновлювати роботу після технічних збоїв чи кібератак.

Теоретичною основою цього підходу стала концепція "цифрової стійкості" (digital resilience), розроблена дослідниками фінансової стабільності. Згідно з цією концепцією, в епоху цифрових технологій фінансова стійкість банку залежить не тільки від традиційних фінансових показників, але й від здатності протистояти технологічним ризикам.

Ключовим моментом є те, що порушення інформаційної безпеки

створює не просто технічні проблеми, а системні ризики. Коли клієнти не можуть отримати доступ до своїх рахунків або сумніваються в безпеці своїх даних, це може спричинити масовий відтік депозитів. А це вже пряма загроза ліквідності банку. Дослідження показують, що банки, які пережили серйозні кіберінциденти, втрачають в середньому 15-20% клієнтської бази протягом року після інциденту. Відновлення довіри може зайняти 2-3 роки і потребувати додаткових маркетингових витрат у розмірі 5-10% від річного доходу.

НБУ в своїх вимогах чітко визначив, що банки повинні забезпечувати відновлення критичних функцій протягом встановленого часу. Цікавим є підхід до оцінки критичності інформаційних активів через фінансові критерії. Якщо збої в роботі системи можуть призвести до втрат понад 1 мільйон гривень, така система автоматично отримує статус критично важливої. Математично цей зв'язок можна виразити через формулу ризику: ризик дорівнює добутку ймовірності інциденту на потенційні втрати, де потенційні втрати включають не тільки прямі збитки, але й втрату репутації, відтік клієнтів та регуляторні санкції.

Організація управління ризиками інформаційної безпекою. Українські банки використовують модель трьох ліній захисту, яку вимагає НБУ. Ця модель запозичена з міжнародної практики та адаптована до українських реалій. Перша лінія захисту включає бізнес-підрозділи, IT-службу та департамент інформаційної безпеки, які відповідають за виявлення загроз, щоденне управління ризиками та такі завдання як моніторинг подій безпеки, реагування на інциденти та навчання користувачів.

Друга лінія представлена службою ризик-менеджменту, яка займається розробкою методів оцінки ризиків та контролем за їх виконанням. До її функцій належить створення політик інформаційної безпеки, оцінка ефективності контролів та підготовка звітності. Третя лінія - це внутрішній аудит, який забезпечує незалежну перевірку ефективності всієї системи через аудит систем інформаційної безпеки, перевірку дотримання політик та оцінку

зрілості процесів [24].

Перша лінія захисту включає не тільки технічних спеціалістів, але й всіх співробітників банку. Кожен працівник повинен розуміти основи кібербезпеки та вміти розпізнавати підозрілі активності. Для цього банки проводять регулярні тренінги - в середньому 4-6 годин на рік для кожного співробітника. Друга лінія відповідає за розробку методології оцінки ризиків, використовуючи міжнародні стандарти та адаптуючи їх до специфіки українського банківського сектору. Третя лінія забезпечує незалежну оцінку ефективності всієї системи. Внутрішні аудитори повинні мати спеціальну підготовку з кібербезпеки - більшість банків направляють своїх аудиторів на міжнародні сертифікаційні програми.

Детальний аналіз кіберінцидентів в українському банківському секторі. Досвід українських банків останніх років унікальний - жодна інша країна не стикалася з такою інтенсивністю та різноманітністю кібератак. Це дало цінний практичний досвід того, як кіберінциденти впливають на фінансову стабільність.

Найяскравішим прикладом залишається атака вірусу Petya у червні 2017 року. Хоча він не був спрямований виключно проти банків, наслідки виявилися катастрофічними для всієї фінансової системи. Petya використовував уразливість в операційній системі Windows та поширювався через мережу, шифруючи файли на заражених комп'ютерах. Особливо постраждали банки, які використовували популярне українське бухгалтерське програмне забезпечення M.E.Doc, через яке і поширювався вірус [35].

Хронологія подій розгорталася стрімко: о 10:30 надійшли перші повідомлення про заражені комп'ютери в банках, о 11:15 почалося масове поширення вірусу через корпоративні мережі, о 12:00 відбулася повна зупинка роботи платіжних систем у 60% банків, о 14:30 банки були відключені від міжнародних платіжних систем, і лише о 18:00 розпочалося часткове відновлення роботи найбільших банків.

Економічні наслідки були вражаючими. Прямі втрати банків склали близько 500 мільйонів гривень, непрямі втрати, включаючи втрачену вигоду та відтік клієнтів, перевищили 2 мільярди гривень. Витрати на відновлення систем досягли 300 мільйонів гривень, а репутаційні втрати оцінюються в 1,5 мільярда гривень. Головний урок Petya полягав не в тому, що хакери викрали гроші, а в тому, що клієнти втратили довіру та не могли проводити звичайні операції. Багато людей почали знімати готівку з рахунків, що створило додатковий тиск на ліквідність банків.

З початком повномасштабної війни українські банки стали мішенню для постійних DDoS-атак. Ці атаки мали на меті не стільки завдати прямої шкоди, скільки дестабілізувати довіру населення до банківської системи. Типова DDoS-атака на український банк характеризується одночасними запитами з 50-100 тисяч IP-адрес, внаслідок чого навантаження на сайт банку зростає в 1000-5000 разів, мобільні додатки стають недоступними, а клієнти не можуть здійснювати онлайн-операції.

Банки навчилися ефективно протистояти таким атакам через використання хмарних сервісів захисту, автоматичне перенаправлення трафіку на резервні сервери та швидке масштабування потужностей під час атак. Економічний вплив DDoS-атак виявився меншим, ніж очікувалося: середня тривалість недоступності сервісів становить 2-4 години, втрачена вигода складає 50-100 тисяч гривень за годину для середнього банку, а витрати на захист - 2-5 мільйонів гривень на рік.

Окремою категорією стали атаки, спрямовані на клієнтів банків. Шахраї створюють фальшиві сайти, що імітують банківські, або надсилають SMS з проханням ввести дані картки. У 2023 році зафіксовано понад 15 тисяч спроб фішингу проти клієнтів українських банків, середні втрати одного клієнта склали 25 тисяч гривень, а загальні втрати клієнтів перевищили 400 мільйонів гривень на рік. Банки активно протидіють цим загрозам через SMS-повідомлення про підозрілі операції, блокування підозрілих доменів та навчання клієнтів основам кібербезпеки.

Міжнародний досвід та порівняльний аналіз. Для розуміння ефективності українського підходу до кібербезпеки банків корисно порівняти його з міжнародною практикою. Європейський Союз прийняв Директиву NIS2, яка встановлює жорсткі вимоги до кібербезпеки критичної інфраструктури, включаючи банки. Основні принципи включають обов'язкове повідомлення про інциденти протягом 24 годин, регулярні аудити кібербезпеки незалежними компаніями та штрафи до 2% від річного обороту за серйозні порушення [16].

Цікаво, що українські вимоги в деяких аспектах навіть жорсткіші за європейські. Наприклад, НБУ вимагає звітувати про інциденти протягом 4 годин, тоді як в ЄС - протягом 24 годин. Американські регулятори використовують ризик-орієнтований підхід. Банки класифікуються за рівнем ризику, і для кожної категорії встановлюються відповідні вимоги. Цікавою особливістю є програма «кіберучень» - регулятори регулярно проводять імітації кібератак для перевірки готовності банків. Подібну практику НБУ почав впроваджувати з 2023 року.

Сінгапур вважається світовим лідером у сфері фінтеху та кібербезпеки. Місцевий регулятор створив спеціальну «пісочницю» для тестування нових технологій безпеки. Український досвід показує, що в умовах реальної загрози банки можуть швидко адаптуватися та впроваджувати ефективні рішення. За рівнем кіберстійкості українські банки сьогодні не поступаються європейським.

Технічні аспекти забезпечення кіберстійкості. Сучасна система кібербезпеки банку включає кілька рівнів захисту, кожен з яких виконує специфічні функції. Перший рубіж оборони - це системи, що захищають мережу банку від зовнішніх загроз: міжмережеві екрани нового покоління, системи запобігання вторгненням, антивірусні шлюзи для електронної пошти та системи фільтрації веб-трафіку. Вартість такого комплексу для середнього банку становить 5-10 мільйонів гривень, але він дозволяє блокувати 95-98% зовнішніх загроз.

Висновки до першого розділу

1. Констатовано, що у сфері банківського менеджменту інформаційне забезпечення економічної безпеки можна визначити як цілеспрямований процес створення, обробки, аналітичного використання та захисту інформаційних ресурсів, необхідних для підтримання стабільності фінансових потоків, збереження конфіденційності банківський даних і своєчасного реагування на ризики.

2. Встановлено, що комплексність, достовірність та оперативність інформаційних потоків визначають рівень фінансової стійкості банку та його здатність реагувати на зовнішні й внутрішні загрози. Формування ефективної системи інформаційного забезпечення передбачає поєднання різних типів інформації – фінансової, аналітичної, правової та організаційно – у єдиному інформаційному просторі, що забезпечує системність та повноту аналітичної підтримки управлінських процесів.

3. В умовах воєнних ризиків, цифрової трансформації та нестабільності фінансового ринку особливого значення набуває побудова адаптивної інтегрованої та захищеної інформаційної системи економічної безпеки банку. Ефективна її архітектура повинна забезпечувати баланс між доступністю даних для прийняття рішень і високим рівнем конфіденційності, що мінімізує ризики витоку інформації, що в свою чергу дозволить підвищити надійність, гнучкість і результативність управління економічною безпекою банківських установ.

4. Досвід останніх років підтвердив, що порушення інформаційної безпеки мають не лише технічний, а й системний вплив - вони здатні викликати втрату ліквідності, масовий відтік депозитів і значні репутаційні втрати. Відповідно, кіберстійкість стала невід’ємною складовою фінансової стабільності, а інвестиції у кіберзахист - стратегічним пріоритетом банківського менеджменту.

5. Підхід НБУ до управління ризиками інформаційної безпеки відповідає найкращим міжнародним практикам і навіть перевищує окремі вимоги ЄС щодо оперативності реагування. Впровадження моделі трьох ліній захисту і обов'язкових стрес-тестів кіберстійкості та вимог до безперервності діяльності підвищує рівень готовності банків до кризових ситуацій. Український досвід, сформований у надзвичайно складних умовах воєнних дій, довів, що адаптивність, інтегровані ІТ-рішення та системний моніторинг загроз здатні забезпечити ефективну протидію навіть наймасштабнішим кібератакам. Це створює основу для формування цифрово стійкої банківської системи, здатної функціонувати безперервно навіть у період глибоких національних викликів.

РОЗДІЛ 2. ПРАКТИЧНІ АСПЕКТИ ФОРМУВАННЯ ІНФОРМАЦІЙНОГО ЗАБЕЗПЕЧЕННЯ СИСТЕМИ ЕКОНОМІЧНОЇ БЕЗПЕКИ АТ «УНІВЕРСАЛ БАНК»

2.1. Фінансово-економічна характеристика АТ «УНІВЕРСАЛ БАНК»

Акціонерне товариство «УНІВЕРСАЛ БАНК» (далі АТ «УНІВЕРСАЛ БАНК») - це український комерційний банк, заснований у 1994 році. Він входить до групи ТАС і відомий як банкір-партнер мобільного додатку monobank, який працює на його базі. Банк є системно важливим, обслуговує як фізичних, так і юридичних осіб, і має штаб-квартиру в Києві. АТ «УНІВЕРСАЛ БАНК» є сучасним фінансовим інститутом, який надає широкий спектр банківських послуг.

Оцінка майна та капіталу банківських установ є ключовим етапом аналізу їх фінансового стану та економічної безпеки. Вона дозволяє визначити структуру активів і пасивів, оцінити динаміку власного та залученого капіталу, а також виявити основні тенденції зростання або зниження платоспроможності. Для АТ «УНІВЕРСАЛ БАНК» аналіз майна і капіталу за період 2020-2024 рр. є особливо актуальним у контексті оцінки стабільності фінансового становища та здатності банку ефективно здійснювати свою діяльність на ринку банківських послуг (табл.2.1).

На основі аналізу динаміки майна та капіталу АТ «УНІВЕРСАЛ БАНК» за досліджуваний період можна констатувати стійке зростання обсягів активів та джерел їх фінансування. Загальна вартість майна збільшилася на 52,1%, що свідчить про розширення операційної діяльності банку та зміцнення його фінансової позиції.

Найбільший приріст характерний для витрат майбутніх періодів та оборотних активів, однак варто звернути увагу на суттєве скорочення залишків грошових коштів та їх еквівалентів у 2023-2024 рр., що може

свідчити про зміну структуру ліквідних активів або перерозподіл ресурсів у напрямі інвестицій чи покриття поточних потреб. Необоротні активи також зросли майже на 40 %, що вказує на оновлення матеріально-технічної бази та підвищення інвестиційної активності.

Таблиця 2.1

Оцінка майна та капіталу АТ «УНІВЕРСАЛ БАНК», тис. грн.

Види активів та пасивів	2020 р.	2021 р.	2022 р.	2023 р.	2024 р.	2024 р. у % до 2020 р.
Майно - усього	764,010	834,455	940,440	1,036,275	1,162,070	152.10
Необоротні активи	18,050	20,260	22,020	23,630	25,190	139.56
Основні засоби	12,000	12,000	13,000	13,500	14,000	116.67
Оборотні активи	745,960	814,195	913,420	1,002,645	1,121,880	150.39
Запаси	150	180	200	220	250	166.67
Поточна дебіторська заборгованість	80,700	95,830	1,070	1,215	1,360	1.69
Гроші, їх еквіваленти та поточні фінансові інвестиції	665,000	718,000	802,000	52,000	60,000	9.02
Інші оборотні активи	500	600.0	700	800	900	180.00
Витрати майбутніх періодів	100	150.0	200	850	950	950.00%
Капітал- усього	764,010	834,455	940,440	1,036,275	1,062,070	139.01
Власний капітал	87,110	101,175	120,780	135,235	149,650	171.79
Зареєстрований (пайовий) капітал	10,000	10,000	10,000	10,000	10,000	100.00
Зобов'язання і забезпечення	696,900	733,280	819,660	901,040	1,012,420	145.27
Довгострокові зобов'язання	6,650	7,930	9,210	10,490	11,770	176.99
Поточні зобов'язання	690,250	725,350	810,450	885,550	990,650	143.52
Поточна кредиторська заборгованість	1,990	2,395	2,800	3,205	3,610	181.41

Джерела формування капіталу також демонструють позитивну динаміку. Загальний капітал збільшився майже на 40 %, при цьому власний капітал зріс на 71,8 %, що є позитивним сигналом щодо фінансової стійкості та автономії банку. Зобов’язання зросли на 45 %, що є очікуваним явищем для банківського сектору та вказує на розширення залучених коштів. Особливо швидко зростали довгострокові зобов’язання (+77 %), що свідчить про активні довгострокові програми фінансування та кредитування. Загалом

структура активів і пасивів АТ «УНІВЕРСАЛ БАНК» характеризується збалансованістю, стабільністю і позитивною тенденцією розвитку, хоча окремі зміни в складі оборотних активів потребують додаткової уваги з позицій ліквідності та ризик-менеджменту.

Фінансові результати діяльності АТ «Універсал Банк» за 2020–2024 рр. свідчать про значне зростання масштабу операційної діяльності та підвищення ефективності роботи банку (рис.2.1).

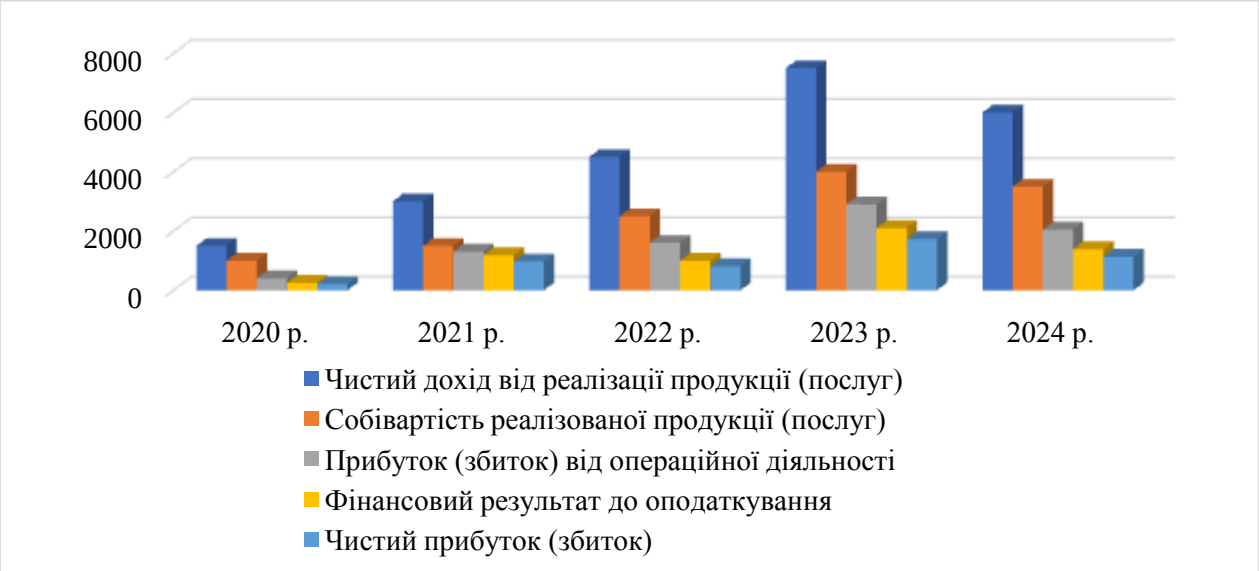

Рис. 2.1. Фінансові результати діяльності АТ «УНІВЕРСАЛ БАНК», тис. грн.

Чистий дохід від реалізації збільшився у 4 рази, що демонструє активне розширення обсягу наданих послуг та зростання клієнтської бази. Позитивною тенденцією є стабільне нарощування фінансових та інвестиційних доходів, хоча витрати за цими напрямами зростали ще швидше, що може свідчити про підвищення вартості залучених ресурсів або активізацію інвестиційної діяльності.

Фінансовий результат до оподаткування та чистий прибуток також демонструють суттєве зростання. Чистий прибуток зріс майже в 5 разів порівняно з 2020 р., що свідчить про ефективне управління доходами та витратами. Проте частка чистого прибутку в чистому доході коливається, знижуючись після піку у 2021 році, що вказує на збільшення витратного навантаження та необхідність оптимізації витрат. Динаміка рентабельності

загалом свідчить про здатність банку ефективно генерувати прибуток, проте потребує посилення контролю за фінансовими та інвестиційними витратами для забезпечення стабільного зростання рентабельності в довгостроковій перспективі.

За допомогою додатку В проведемо оцінку ліквідності, платоспроможності та оборотності оборотних активів АТ «УНІВЕРСАЛ БАНК» за 2020-2024 рр. Аналіз ліквідності банку демонструє нерівномірні тенденції та суттєві структурні зміни в складі активів і зобов'язань. Високоліквідні активи (А1) у 2023-2024 рр. різко скоротилися, що знизило їх рівень до 9 % від показника 2020 р., і це може свідчити про перерозподіл ресурсів у довгострокові вкладення або значне зростання потреби в операційних витратах. При цьому найбільш строкові зобов'язання зростали стабільно, що формує ризики для миттєвої ліквідності. Середньострокові активи, хоча й зросли в 2024 р. порівняно з 2020 р., у проміжні роки різко зменшувалися. Що також знижує фінансову гнучкість. Низьколіквідні активи демонструють прогнозоване, поступове зростання. У сукупності така динаміка свідчить про необхідність оптимізації структури активів для забезпечення повного покриття короткострокових зобов'язань.

Щодо платоспроможності, банк зберігає стабільно високі значення коефіцієнтів загальної ліквідності та загальної платоспроможності: вони значно перевищують нормативи і мають позитивну тенденцію. Проте коефіцієнти абсолютної та проміжної ліквідності різко знизилися у 2023-2024 рр., що є сигналом ризику недостатнього обсягу найбільш ліквідних активів для швидкого покриття поточних зобов'язань. Незважаючи на це, загальна структура активів дозволяє банку отримувати високий рівень покриття всіх зобов'язань. Таким чином, АТ «УНІВЕРСАЛ БАНК» загалом залишається платоспроможним, однак йому необхідно посилити контроль за миттєвою та поточною ліквідністю для забезпечення стабільної фінансової стійкості в умовах ринкових коливань.

Комплексна оцінка фінансового стану АТ «УНІВЕРСАЛ БАНК»

(додаток Б) свідчить про стабільно високий рівень фінансової стійкості та ефективності діяльності. Інтегрований показник протягом аналізованого періоду перебуває у межах 7,48-7,84 балів, що відповідає рейтингу «А» - високий фінансовий стан. Показники ліквідності залишаються на достатньому рівні, хоча коефіцієнт швидкої ліквідності у 2023-2024 рр. різко зменшився, що сигналізує про певні ризики щодо забезпечення миттєвої платоспроможності. Ділова активність демонструє нерівномірні коливання: значне покращення оборотності дебіторської заборгованості у 2023-2024 рр. та стабільно висока оборотність запасів компенсують зниження загальної оборотності активів у попередні роки.

Показники фінансової незалежності свідчать про достатній рівень автономії банку, хоча частка фінансування активів за рахунок власного капіталу залишається помірною. Динаміка частки власних оборотних коштів має позитивну тенденцію до зростання, що підвищує фінансову стійкість у короткостроковому періоді. Загалом комплексна оцінка підтверджує, що банк має стабільний, ефективний та збалансований фінансовий стан, здатний забезпечувати виконання своїх зобов’язань і підтримувати високу ділову активність. Однак подальше вдосконалення ліквідності, зокрема швидкої, залишається важливим завданням для мінімізації фінансових ризиків.

2.2. Характеристика роботи служби економічної безпеки банку та оцінка її стану за окремими складовими

Система економічної безпеки АТ «УНІВЕРСАЛ БАНК» є невід’ємною складовою загальної системи корпоративного управління, спрямованого на забезпечення стабільного функціонування банківської установи, мінімізацію ризиків фінансових втрат, запобігання шахрайству та деструктивним впливам внутрішніх і зовнішніх загроз. Її діяльність організована відповідно до вимог НБУ, положень внутрішніх нормативних документів і принципів ризик-орієнтованого управління.

Організаційна структура системи економічної безпеки банку передбачає функціонування Департаменту економічної безпеки, Департаменту ризиків. А також низки спеціалізованих управлінь і відділів, які взаємодіють між собою у процесі збору, аналізу та обробки інформації про фінансові, операційні та репутаційні загрози (рис. 2.2).

Рис. 2.2. Організаційна структура
системи економічної безпеки АТ «УНІВЕРСАЛ БАНК»

Департамент економічної безпеки підпорядковується безпосередньо Правлінню банку, що забезпечує високий рівень незалежності та можливості оперативного прийняття рішень. Департамент здійснює організацію системи економічної безпеки банку, координує діяльність підрозділів, затверджує плани і звіти, здійснює аналітичний контроль за станом економічної безпеки, проведення поглибленого фінансового аналізу, розробкою індикаторів безпеки, моделювання ризиків, участь у внутрішніх аудитах, підготовка

аналітичних довідок тощо.

Департамент ризиків відповідає за розробку та впровадження політики ризик-менеджменту; контроль за якістю ризикових операцій; звітність перед Правлінням банку, аналіз кредитного портфеля, розробка політики управління ризиками, контроль рівня прострочених заборгованостей, оцінювання кредитоспроможності позичальників, розрахунок резервів, моніторинг ризиків за клієнтськими групами, обробка статистичних даних, формування аналітичних таблиць і дашбордів, підготовка звітності для керівництва.

Відділ інформаційно-аналітичної безпеки – захист інформаційних ресурсів, моніторинг кіберзагроз, аудит інформаційних систем, контроль політики доступу.

Служба внутрішніх розслідувань проводить виявлення фактів шахрайства, службових зловживань; проведення службових перевірок; координація дій з правоохоронними органами.

Служба фізичної та кадрової безпеки забезпечує охорону об’єктів банку; контроль доступу персоналу; перевірка кандидатів під час працевлаштування.

Всі ці процеси регламентуються внутрішніми документами. Це Положення про Фінансовий департамент, Положення про Департамент ризиків, Положення про Департамент економічної безпеки. Також є різні Інструкції та Регламенти щодо проведення фінансового аналізу, оцінки ризиків, процедур розслідувань. Наприклад, є внутрішні методики оцінки кредитних ризиків, процедури моніторингу операційних ризиків, регламент дій при виявленні шахрайства.

Важливим аспектом ефективності структури є вертикальна підпорядкованість, яка забезпечує оперативне прийняття рішень і контроль за реалізацією політики безпеки. Водночас міждепартаментна взаємодія формує горизонтальні зв’язки, необхідні для швидкого обміну інформацією про ризики та загрози.

Всі ці процеси регламентуються внутрішніми документами. Це Положення про Фінансовий департамент, Положення про Департамент ризиків, Положення про Департамент економічної безпеки. Також є різні Інструкції та Регламенти щодо проведення фінансового аналізу, оцінки ризиків, процедур розслідувань. Наприклад, є внутрішні методики оцінки кредитних ризиків, процедури моніторингу операційних ризиків, регламент дій при виявленні шахрайства.

Відмітимо, що рівень організації системи економічної безпеки АТ «УНІВЕРСАЛ БАНК» досить високий. Виявлення загроз відбувається постійно, а аналіз є доволі глибоким. Використовуються різні методики складання аналітичних документів, наприклад, звітність про ризики будується на базі міжнародних стандартів, таких як Basel III для банків. Інформаційно-аналітичні документи чітко структуровані, містять ключові показники, аналіз відхилень, прогнозні дані та конкретні рекомендації. Наприклад, для оцінки ризиків, пов'язаних з діяльністю конкретного клієнта, аналітики можуть використовувати його фінансову звітність, кредитну історію, інформацію з відкритих джерел, аналіз галузі.

Завдяки функціональному поділу на аналітичний, інформаційний, розслідуваний і ризикоорієнтований напрями, АТ «УНІВЕРСАЛ БАНК» має змогу своєчасно реагувати на зміни у внутрішньому та зовнішньому середовищі, мінімізуючи вплив негативних факторів на фінансово-господарську діяльність.

Діагностика рівня безпеки АТ «УНІВЕРСАЛ БАНК» здійснюється за багатьма складовими, що дозволяє отримати повну картину. Розрахуємо деякі показники, які допоможуть оцінити рівень безпеки за окремими складовими (табл. 2.2). Фінансова складова характеризується високим рівнем ефективності діяльності банку, що підтверджується показниками рентабельності активів (2,3%), рентабельність власного капіталу (15,6%) та достатності капіталу (12%). Це свідчить про фінансову стійкість, здатність виконувати зобов’язання та формувати стабільні доходи.

Інформаційна складова перебуває на високому рівні завдяки впровадженню сучасних систем кібербезпеки, шифрування даних і сертифікації інформаційних процесів за міжнародними стандартами ISO/IEC 27001. Витрати на ІТ-захист становлять близько 2,4 % доходів банку, що забезпечує належний рівень цифрової безпеки.

Таблиця 2.2

Інтегральна оцінка рівня складових
економічної безпеки АТ «УНІВЕРСАЛ БАНК», 2024 р.

Складова економічної безпеки	Середній інтегральний показник	Рівень безпеки
Фінансова	0,78	Високий
Інформаційна	0,80	Високий
Інтелектуальна	0,80	Високий
Кадрова	0,85	Високий
Техніко-технологічна	0,83	Високий
Правова	0,88	Високий
Інноваційна	0,85	Високий
Силова	0,90	Високий
Середній інтегральний рівень безпеки	0,85	Високий

Інтелектуальна складова визначається високим освітнім рівнем працівників (понад 95% мають вищу освіту), активною участю у тренінгах і впровадження власних ШТ-рішень у сфері клієнтського обслуговування. Це створює інтелектуальний потенціал, здатний до генерування інновацій.

Кадрова складова має високий рівень завдяки стабільності персоналу (плинність кадрів – лише 5,2%), високому рівню кваліфікації, наявності системи професійного розвитку та мотиваційних механізмів. Це забезпечує стійкість банківських процесів і зниження рівня ризику кадрових втрат.

Техніко-технологічна складова підтримується за рахунок використання сучасних банківських систем (CRM, AML, Risk-monitoring), хмарних рішень і регулярного оновлення технічної інфраструктури. Частка ІТ-інвестицій у витратах становить 4,1 %, що забезпечує цифрову адаптивність банку.

Правова складова залишається однією з найсильніших – банк повністю дотримується нормативів НБУ, має ефективну систему комплаєнс-контролю

та мінімальні судові ризики. Це свідчить про високу юридичну захищеність діяльності банку.

Інноваційна складова відзначається активним розвитком цифрових сервісів - впроваджено п’ять нових продуктів протягом року, понад 90 % операцій здійснюються онлайн. Використання технологій штучного інтелекту у скорингових системах підвищує точність оцінки клієнтських ризиків.

Силова складова також має високий рівень: у всіх відділеннях банку функціонує система відеоспостереження, охорона та контроль доступу, відсутні зареєстровані інциденти безпеки протягом року.

За результатами розрахунків інтегральний показник економічної безпеки АТ «УНІВЕРСАЛ БАНК» становить 0,85, що відповідає високому рівню безпеки. Це свідчить про ефективне функціонування системи управління ризиками, стабільний фінансовий стан та здатність банку адаптуватися до зовнішніх загроз.

Отже, система економічної безпеки АТ «УНІВЕРСАЛ БАНК» виконує стратегічно важливу роль у забезпеченні фінансової стабільності та конкурентоспроможності банку. Її діяльність базується на принципах системності, багаторівневості та безперервного моніторингу ризиків. Висока професійна підготовка персоналу, розподіл функцій між департаментами, а також впровадження цифрових аналітичних інструментів дозволяють банку ефективно реагувати на внутрішні та зовнішні загрози. Надалі доцільним є подальший розвиток автоматизованих модулів контролю ризиків, інтеграція аналітичних платформ у систему корпоративного управління та посилення міждепартаментної взаємодії для підвищення ефективності економічної безпеки банку.

2.3. Оцінка процесу формування інформаційного забезпечення системи економічної безпеки АТ «УНІВЕРСАЛ БАНК»

Банківські установи, зокрема АТ «УНІВЕРСАЛ БАНК», є об’єктами підвищеного ризику, адже оперують значними обсягами конфіденційних даних клієнтів, корпоративною інформацією та здійснюють безперервні електронні фінансові операції. Будь-яке порушення цілісності або конфіденційності даних може призвести не лише до фінансових втрат, але й до зниження довіри клієнтів та репутаційних ризиків. Система інформаційної безпеки АТ «УНІВЕРСАЛ БАНК» будується на принципах комплексності, багаторівневості та відповідності міжнародним стандартам (ISO/IEC 27001, ISO/IEC 22301) та вимогам НБУ. Основними завданнями системи є:

- захист інформаційних ресурсів від несанкціонованого доступу, втрати або модифікації;

- забезпечення цілісності та доступності даних у режимі реального часу;

- мінімізація ризиків, пов’язаних з кіберзагрозами та внутрішніми помилками персоналу;

- підтримка відповідності нормативними актам щодо захисту персональних даних (GDPR та українське законодавство).

Саме тому створення ефективного департаменту інформаційної безпеки є ключовою умовою стабільного функціонування банку та виконання ним регуляторних вимог НБУ, а також міжнародних стандартів, таких як ISO/IEC 27001.

Департамент інформаційної безпеки АТ «УНІВЕРСАЛ БАНК» виконує стратегічну роль у формуванні, реалізації та контролі комплексного підходу до управління ризиками безпеки, де кожен підрозділ виконує чітко визначені функції – від методологічного та начального забезпечення до технічного захисту, моніторингу інцидентів і контролю дотримання законодавства у сфері персональних даних. Така багаторівнева система управління дозволяє не лише запобігати кіберзагрозам, а й забезпечувати оперативне реагування на потенційні інциденти та їх наслідки.

В результаті дослідження встановлено, що структура Департаменту

інформаційної безпеки АТ «УНІВЕРСАЛ БАНК» побудована за принципом функціонального розподілу повноважень і відповідності між окремими управліннями (рис. 2.3). Така модель забезпечує системність управління інформаційною безпекою (ІБ) та дозволяє ефективно реалізувати як стратегічні, так і оперативні завдання з кіберзахисту.

Рис. 2.3. Організаційна структура
Департаменту інформаційної безпеки АТ «УНІВЕРСАЛ БАНК»

Управління методології інформаційної безпеки виконує стратегічну і координуючу функцію у сфері розробки й впровадження політик, стандартів, процедур і методологій ІБ. Основною його метою є побудова ефективної системи управління інформаційною безпекою (СУІБ, ISMS), що відповідає міжнародним вимогам ISO/IEC 27001.

До основних завдань управління належать: проведення оцінки ризиків ІБ, розробка заходів з їх мінімізації, координація внутрішніх аудитів, а також забезпечення відповідності внутрішніх політик банку чинним законодавчим та регуляторним вимог. Таким чином, цей підрозділ формує концептуальну основу системи безпеки та забезпечує її безперервне вдосконалення.

Ефективність будь-якої системи ІБ значною мірою залежить від рівня обізнаності та поведінкової культури персоналу. Управління навчання ІБ

відповідає та поведінкової культури персоналу. Управління навчання ІБ відповідає за підвищення компетенцій співробітників у сфері кібербезпеки шляхом організації тренінгів, семінарів, тематичних курсів і симуляцій фішингових атак.

Ключовими напрямами роботи є розробка навчальних програм для різних категорій працівників, оцінювання рівня знань, формування «кіберкультури» та розвиток корпоративної відповідальності за дотриманням політик безпеки. Це управління є вважливою ланкою профілактики внутрішніх загроз та помилок користувачів, які часто стають причиною інцидентів ІБ.

Підрозділ управління кваліфікованого надавача електронних довірчих послуг забезпечує діяльність банку як кваліфікованого надавача електронних довірчих послуг, відповідно до Закону України «Про електронні довірчі послуги». Основним завданням є управління інфраструктурою відкритих ключів, випуск, зберігання та відкликання кваліфікованих сертифікатів електронних підписів і печаток. Крім того, управління відповідає за експлуатацію апаратних засобів криптографічного захисту, а також за дотриманням стандартів криптостійкості та процедур автентифікації користувачів. Його діяльність має критичне значення для забезпечення правової значимості електронних документів і транзакцій, що здійснюються в цифровому середовищі.

Управління технічного захисту та безпеки ІБ реалізує технічну складову кіберзахисту банку. Основні завдання полягають у впровадженні, адмініструванні та підтримці функціонування засобів технічного контролю: міжмережевих екранів (Firewall), систем виявлення та запобігання вторгненням (IDS/IPS), систем захисту від витоку даних (DLP) і рішень управління доступом (IAM). Крім того, підрозділ здійснює тестування на проникнення (penetration testing), оцінку рівня захищеності інформаційних ресурсів та моніторинг ефективності захисних механізмів. Результати роботи цього управління безпосередньо впливають на стійкість ІТ-інфраструктури

банку до зовнішніх кібератак і технічних збоїв.

Функціонування центру моніторингу безпеки та реагування на інциденти є основою оперативного управління кіберінцидентами. Підрозділ здійснює цілодобовий збір, аналіз і кореляцію подій інформаційної безпеки, виявляє аномальну активність і потенційні загрози. До його складу входить команда реагування на інциденти CSIRT, яка проводить розслідування інцидентів, цифрову криміналістику (forensic analysis), відновлення систем після атак, а також координує взаємодію з національними та міжнародними структурами (CERT, НБУ, правоохоронними органами). Ефективність роботи SOC/CSIRT є критичною для мінімізації наслідків кібератак і швидкого відновлення стабільної роботи банківських сервісів.

З огляду на посилення законодавчих вимог у сфері захисту персональних даних (GDPR, Закон України «Про захист персональних даних»), управління Privacy виконує функції контролю дотримання прав клієнтів на конфіденційність і прозору обробку їхніх даних. До його обов’язків належать розробка політик приватності, проведення оцінок впливу на захист даних (DPIA), управління згодами на обробку даних, ведення реєстрів потоків ПД і реагування на інциденти, пов’язані з їх порушенням.

За допомогою рис. 2.4 відобразимо схему основних інформаційних потоків банку.

Рис. 2.4. Схема основних інформаційних потоків АТ «УНІВЕРСАЛ БАНК»

Відповідно до даної схеми клієнтські дані – це основа для операцій і аналітики, без їх захисту банк піддається репутаційним та фінансовим ризикам. Операційні дані – включають всі транзакції та внутрішні бухгалтерські записи, вони формують основу управлінських рішень. Управлінські та аналітичні дані – забезпечують стратегічне та тактичне управління, оцінку ризиків і контроль економічної безпеки. Департамент ІБ – захищає всі потоки, координує реагування на інциденти та підвищує обізнаність персоналу. Як наслідок та кінцевий результат інтеграції всіх потоків і роботи Департаменту ІБ – це економічна безпека банку.

Для оцінки рівня ефективності інформаційного забезпечення було використано комплексний підхід. Що включає технічний, організаційний та навчальний компоненти (табл.2.3).

Таблиця 2.3

Оцінка рівня ефективності інформаційного забезпечення АТ «УНІВЕРСАЛ БАНК»

Критерій	Оцінка (1–5)	Коментар
Технічний захист	4	Високий рівень захисту, але

		потрібна більша автоматизація SOC
Організаційна ефективність	4	Структура чітка, взаємодія між управліннями задовільна
Навчання та обізнаність персоналу	3	Потрібне регулярне оновлення програм і тренінгів
Відповідність законодавству	5	Політики та процедури повністю відповідають стандартам
Інтеграція з бізнес-процесами	4	Добра інтеграція, але можливі покращення в автоматизації звітності

При цьому інтегральний показник ефективності 4 з 5, що свідчить про стабільну та ефективну систему, яка потребує вдосконалення в навчанні персоналу та автоматизації процесів.

Отже, Департамент інформаційної безпеки АТ «УНІВЕРСАЛ БАНК» забезпечує комплексне інформаційне забезпечення системи економічної безпеки банку. Така організаційна структура дозволяє поєднати методологічний, технічний та освітній підходи, забезпечуючи цілісність, доступність і конфіденційність інформаційних ресурсів. Оцінка ефективності показала високий рівень захищеності банку, хоча потребує вдосконалення у сфері автоматизації SOC.

Висновки до другого розділу

1. АТ «УНІВЕРСАЛ БАНК» - це український комерційний банк, заснований у 1994 році. Він входить до групи ТАС і відомий як банкір-партнер мобільного додатку monobank, який працює на його базі. Банк є сучасним фінансовим інститутом, який надає широкий спектр банківських послуг як фізичним, так і юридичним особам. Комплексна оцінка фінансового стану АТ «УНІВЕРСАЛ БАНК» свідчить про стабільно високий рівень фінансової стійкості та ефективності діяльності. Інтегрований показник протягом аналізованого періоду перебуває у межах 7,48-7,84 балів, що відповідає рейтингу «А» - високий фінансовий стан.

2. Встановлено, що структура системи економічної безпеки банку передбачає функціонування Департаменту економічної безпеки, Департаменту ризиків. А також низки спеціалізованих управлінь і відділів, які взаємодіють між собою у процесі збору, аналізу та обробки інформації про фінансові, операційні та репутаційні загрози. Організаційна структура Департаменту інформаційної безпеки АТ «УНІВЕРСАЛ БАНК» побудована на засадах інтегрованого управління ризиками, взаємодії технічних, організаційних і правових механізмів захисту. така модель забезпечує комплексний підхід до кібербезпеки – від розробки політик до оперативного реагування на інциденти.

3. Відмітимо, що рівень організації системи економічної безпеки АТ «УНІВЕРСАЛ БАНК» досить високий. Виявлення загроз відбувається постійно, а аналіз є доволі глибоким. Використовуються різні методики складання аналітичних документів, наприклад, звітність про ризики будується на базі міжнародних стандартів, таких як Basel III для банків. Інформаційно-аналітичні документи чітко структуровані, містять ключові показники, аналіз відхилень, прогнозні дані та конкретні рекомендації. Наприклад, для оцінки ризиків, пов'язаних з діяльністю конкретного клієнта, аналітики можуть використовувати його фінансову звітність, кредитну історію, інформацію з відкритих джерел, аналіз галузі.

4. За результатами розрахунків інтегральний показник економічної безпеки АТ «УНІВЕРСАЛ БАНК» становить 0,85, що відповідає високому рівню безпеки. Це свідчить про ефективне функціонування системи управління ризиками, стабільний фінансовий стан та здатність банку адаптуватися до зовнішніх загроз.

5. Система інформаційної безпеки АТ «УНІВЕРСАЛ БАНК» будується на принципах комплексності, багаторівневості та відповідності міжнародним стандартам (ISO/IEC 27001, ISO/IEC 22301) та вимогам НБУ. В результаті дослідження встановлено, що структура Департаменту інформаційної безпеки АТ «УНІВЕРСАЛ БАНК» побудована за принципом

функціонального розподілу повноважень і відповідності між окремими управліннями. До складу департаменту входять шість ключових управлінь, кожне з яких відповідає за певний напрям діяльності в межах загальної системи безпеки банку.

6. Для оцінки рівня ефективності інформаційного забезпечення було використано комплексний підхід. Що включає технічний, організаційний та навчальний компоненти. При цьому інтегральний показник ефективності 4 з 5, що свідчить про стабільну та ефективну систему, яка потребує вдосконалення в навчанні персоналу та автоматизації процесів.

РОЗДІЛ 3. УДОСКОНАЛЕННЯ ІНФОРМАЦІЙНОГО ЗАБЕЗПЕЧЕННЯ СИСТЕМИ ЕКОНОМІЧНОЇ БЕЗПЕКИ БАНКІВСЬКИХ УСТАНОВ

3.1. Напрями вдосконалення інформаційного забезпечення системи економічної безпеки банку

В умовах сучасного розвитку фінансового банківські установи стикаються з безпрецедентними викликами, що пов’язані з динамікою економічної кон’юнктури, глобалізацією фінансових потоків, зростанням обсягів клієнтських операцій та активним впровадження цифрових технологій. Ефективне управління ризиками стає ключовим елементом забезпечення економічної безпеки банку та гарантією стабільності його діяльності. Традиційні підходи до оцінки та контролю ризиків, що базуються переважно на періодичній звітності та експертних оцінках, вже не здатні забезпечити необхідну швидкість реакції та гнучкість у прийнятті рішень. У цьому контексті аналітичні платформи моніторингу ризиків виступають інтегрованим інструментом, який дозволяє здійснювати комплексний збір, обробку, аналіз та візуалізацію даних про ризики, а також прогнозування потенційних загроз.

Аналітична платформа моніторингу ризиків є багаторівневою системою, яка включає модулі збору даних, інтеграції та зберігання інформації, аналітики та прогнозування, візуалізації, а також контролю та оповіщення про критичні ризики.

Модуль збору даних забезпечує автоматизований доступ до інформації з внутрішніх джерел, таких як операційні системи банку, CRM-системи, бухгалтерський облік та кредитний портфель, а також із зовнішніх джерел – статистичних даних регуляторів, аналітичних звітів, фінансових новин і медіа-простору. Для забезпечення якості та узгодженості даних

застосовуються сучасні технології ETL (Extract, Transform, Load), що дозволяють виконувати вилучення даних, їх трансформацію та завантаження у єдине сховище даних, забезпечуючи тим самим надійність подальшого аналізу.

Інтеграційний модуль платформи дозволяє об’єднувати дані з різних джерел у єдину інформаційну модель [1]. Використання хмарних сховищ та технологій типу Data Warehouse або Data Lake забезпечує масштабованість, швидкий доступ до інформації та можливість обробки великих обсягів даних у режимі реального часу. Для підвищення точності прогнозування ризиків важливо впровадити механізми нормалізації та контролю якості даних, що дозволяє мінімізувати ймовірність помилкових сигналів та підвищити достовірність результатів аналітики.

Аналітичний модуль платформи реалізує оцінку ризиків за допомогою поєднання кількісних і якісних методів. Кількісні методи включають статистичний аналіз, кореляційний та регресійні моделі, моделі кредитного скорингу, оцінку Value at Risk (VaR) та Conditional Value at Risk (CVaR), а також стрес-тестування портфеля активів і кредитів. Якісні методи реалізуються через експертні оцінки, сценарний аналіз, моделювання наслідків кризових ситуацій та оцінку репутаційних ризиків на основі соціальних медіа тощо. Значну увагу варто приділити застосуванню алгоритмів штучного інтелекту та машинного навчання, зокрема методам класифікації клієнтів за рівнем ризику, прогнозуванню дефолтів, виявленню аномалій у фінансових операціях, прогнозуванню макроекономічних ризиків та тенденцій ринку.

Візуалізація даних здійснюється за допомогою інтерактивних дашбордів, графіків, карт ризиків та звітів, що дозволяють керівництву банку отримувати швидкий та наочний огляд стану портфеля ризиків, оцінювати динаміку показників і своєчасно виявляти критичні проблемні зони [31]. Модуль контролю та оповіщення забезпечує автоматичне повідомлення відповідальних співробітників про перевищення встановлених критичних

порогів ризиків, що дозволяє оперативно реагувати на загрози та мінімізувати їх негативні наслідки. Використання сценаріїв «що якщо» та правил бізнес-логіки дозволяє моделювати ефекти управлінських рішень і прогнозувати вплив різних дій на загальний стан портфеля ризиків.

Впровадження аналітичної платформи дозволяє суттєво підвищити ефективність управління ризиками у банку. Очікуваними результатами є систематизація процесів збору та аналізу даних про ризики, скорочення часу виявлення критичних загроз, підвищення точності прогнозів фінансових і операційних ризиків, оптимізація процесу прийняття управлінських рішень та загальне підвищення рівня економічної безпеки установи (табл.3.2).

Таблиця 3.1

Порівняльна оцінка ефективності управління ризиками до та після впровадження аналітичної платформи моніторингу ризиків

Показник	До впровадження	Після впровадження	Зміни, %
Час виявлення критичного ризику	48 годин	2 години	-95
Точність прогнозів дефолту	75%	92%	+17
Кількість несанкціонованих операцій	12/міс	3/міс	-75
Оцінка задоволеності керівництва	3,2/5	4,7/5	+46

Джерело: сформовано автором

Для більш детальної оцінки ефективності платформи доцільно застосовувати розподіл ризиків за категоріями та аналізу частоти їх виникнення. Розроблена карта ризиків для АТ «УНІВЕРСАЛ БАНК» (додаток В). Це дозволяє керівництву банку сконцентрувати ресурси на критично важливих загрозах та оптимізувати процеси управління.

У підсумку ефективне функціонування аналітичної платформи, створює передумови для підвищення фінансової стабільності, своєчасного реагування на загрози та забезпечення стійкого розвитку банківської установи в умовах сучасної економічної нестабільності.

Одним із ключових напрямів удосконалення інформаційного забезпечення є впровадження багаторівневого контролю доступу до інформаційних систем банку, що включає диференційовані права доступу

залежно від ролі співробітника, а також сегментацію систем для обмеження поширення потенційних загроз [4]. Крім того, шифрування даних як у стані зберігання (data at rest), так і під час передачі (data in transit) дозволяє забезпечити конфіденційність та захист від несанкціонованого доступу. Важливим елементом є моніторинг загроз у реально часі, що здійснюється за допомогою систем Security Information and Event Management (SIEM), які аналізують логи, виявляють аномалії та автоматично формують сповіщення для відповідальних співробітників.

Багаторівневий контроль доступу забезпечує принцип найменших привілеїв, коли співробітник має лише ті права, які необхідні для виконання його службових обов'язків [45]. Це дозволяє зменшити ймовірність внутрішніх порушень безпеки та знизити ризик витоку конфіденційної інформації. Шифрування даних, зокрема використання алгоритмів AES, RSA та TLS, забезпечує захист інформації у разі компрометації фізичних носіїв або мережевого трафіку. Моніторинг загроз у реальному часі дозволяє ідентифікувати спроби несанкціонованого доступу, атаки типу Brute Force, DDoS, шкідливе ПЗ та інші інциденти на ранніх стадіях, що дає можливість оперативно реагувати на загрози (табл.3.2).

Таблиця 3.2

Практичні заходи багаторівневого контролю доступу та шифрування даних

Захід	Опис	Очікуваний ефект	Пріоритет
Розмежування доступу	Диференціація прав користувачів за ролями	Зниження внутрішніх ризиків	Високий
Шифрування даних	Використання AES, RSA, TLS для зберігання та передачі інформації	Захист конфіденційності даних	Високий
Моніторинг подій у реальному часі	Використання SIEM для виявлення аномалій	Своєчасне виявлення та реагування на атаки	Високий
Багатофакторна аутентифікація	Паролі + SMS/Email/Token	Підвищення безпеки облікових записів	Середній

Джерело: сформовано автором

Наступним ключовим напрямом є розробка та впровадження

протоколів реагування та кіберінциденти. Це передбачає створення чітких процедур для виявлення, класифікації та усунення кіберзагроз, включаючи інструкції для оперативного відновлення систем після атак та заходи щодо зменшення негативних наслідків. Важливим компонентом є навчання персоналу – регулярні тренінги та симуляції інцидентів дозволяють співробітникам швидко орієнтуватися в кризових ситуаціях і правильно діяти у разі виникнення загроз, визначення правил безпечного користування корпоративними системами та способи ідентифікації фішингових атак.

В табл.3.3 наведено протоколи реагування на кіберінциденти, які включають:

Таблиця 3.3

Протоколи реагування на кіберінциденти та навчання персоналу

Компонент протоколу	Опис	Очікуваний ефект	Пріоритет
Виявлення та класифікація	Оцінка типу та критичності інциденту	Зменшення часу на реагування	Високий
Оповіщення відповідальних осіб	Автоматичні сповіщення керівництва та IT-підрозділу	Оперативність реакції	Високий
Ізоляція уражених систем	Відключення частини мережі або серверів для локалізації інциденту	Мінімізація поширення загрози	Високий
Відновлення та аналіз	Відновлення даних, систем та аналіз причин	Зниження повторних інцидентів	Середній
Навчання персоналу	Тренінги, симуляції інцидентів, тестування знань	Формування культури кібербезпеки	Високий

Джерело: власна розробка

Відмітимо, що інтеграція аналітичної платформи банку з системами виявлення шахрайських операцій та захисту від DDoS-атак. Аналітична платформа дозволяє збирати дані про транзакції в реальному часі, виявляти аномалії, прогнозувати можливі шахрайські дії та формувати автоматичні сповіщення для відповідальних співробітників. Інтеграція з DDoS-системами дозволяє контролювати мережевий трафік, виявляти аномальні навантаження на сервіси банку та автоматично застосовувати механізми обмеження або перенаправлення трафіку.

Переваги інтеграції аналітичної платформи: швидке виявлення потенційних загроз у транзакціях; можливість комбінованого аналізу даних з різних систем; зменшення ризику фінансових втрат та репутаційних втрат банку; оперативне реагування на атаки без втрати доступності сервісів для клієнтів.

Одним із ключових рішень є впровадження системи інтегрованого моніторингу ризиків, яка дозволяє об’єднати всі критичні показники ризиків у єдину аналітичну платформу. Така система забезпечує своєчасне отримання даних про кредитні, операційні, ринкові ризики, ризики ліквідності та репутаційні загрози, що значно підвищує ефективність процесів прийняття управлінських рішень.

Основою інтегрованого моніторингу є створення модуля «єдиного вікна» для керівництва, де візуально об’єднані всі ключову показники ризиків [12]. Завдяки цьому керівництво отримують можливість спостерігати за станом ризиків у режимі реального часу, аналізувати взаємозв’язки між ними та приймати своєчасні рішення щодо нейтралізації негативних наслідків (додаток Д). Використання карти ризиків (додаток В) дозволяє пріоритезувати реагування на найбільш критичні загрози і ризики та концентрувати ресурси на їх своєчасному усуненні. Такий підхід забезпечує перехід від реактивного управління, коли дії здійснюються після виникнення проблем, до проактивного, що передбачає прогнозування потенційних ризиків та їх мінімізацію до того, як вони вплинуть на діяльність установи.

Концепцію «єдиного вікна» інтегрованого моніторингу відображає всі основні категорії ризиків та їхнє оновлення в режимі реального часу для оперативного управління.

3.2. Інтелектуальні технології як інструмент удосконалення інформаційного забезпечення системи економічної безпеки банківських установ

У сучасних умовах цифровізації фінансового сектору забезпечення

економічної безпеки банківських установ потребує застосування інноваційних підходів до інформаційного забезпечення. Одним із перспективних напрямів є інтеграція інструментів штучного інтелекту (ШІ) у системи управління ризиками та моніторингу діяльності банку. Штучний інтелект дозволяє автоматизувати обробку великих обсягів даних, підвищити точність прогнозування ризиків та ефективність прийняття управлінських рішень.

Впровадження штучного інтелекту у систему економічної безпеки банківської установи охоплює кілька ключових напрямів: аналітичну підтримку прийняття рішень, прогнозування фінансових та операційних ризиків, виявлення шахрайських операцій, оцінку кредитоспроможності клієнтів, моніторинг ліквідності та ринкових показників [46]. Використання алгоритмів машинного навчання та нейронових мереж дозволяє моделювати складні взаємозв'язки між фінансовими показниками та зовнішніми ризиками, забезпечуючи більш комплексну оцінку стану економічної безпеки (табл. 3.4).

Таблиця 3.4

Основні інструменти штучного інтелекту та їх функціональне застосування в банківській системі економічної безпеки

Інструмент ШІ	Функціональне призначення	Переваги застосування	Приклади використання
Машинне навчання	Прогнозування ризиків неплатоспроможності клієнтів	Підвищення точності кредитних рейтингів, зменшення кількості дефолтів	Моделювання кредитного скорингу, прогнозування дефолтів
Нейронні мережі	Аналіз складних фінансових залежностей	Виявлення аномалій та потенційних загроз	Моніторинг операційних потоків, виявлення шахрайства
Обробка природної мови	Аналіз текстових даних (контракти, новини)	Швидке виявлення ризиків та негативних тенденцій	Виявлення негативної інформації про контрагентів, аналіз медіа
Роботизація процесів	Автоматизація рутинних аналітичних операцій	Скорочення часу на обробку даних, зниження помилок	Автоматичне формування звітності, контроль транзакцій
Аналітичні платформи	Комплексний моніторинг показників ризиків	Інтеграція даних з різних джерел	Єдине інформаційне вікно для керівництва банку

Джерело: сформовано автором

Важливим аспектом впровадження ШІ у систему інформаційного забезпечення економічної безпеки є їх здатність до самонавчання та адаптації до нових умов [34]. Це дозволяє банкам швидко реагувати на зміну ринкових, кредитних, операційних та репутаційних ризиків, забезпечуючи динамічний контроль за фінансовою стабільністю установи.

Крім того, інтеграція ШІ з існуючими інформаційними системами банку дозволяє створювати системи раннього попередження загроз, де аналітичні алгоритми оцінюють ймовірність настання кризових ситуацій на основі комплексного аналізу внутрішніх та зовнішніх даних. Це особливо актуально для банків, що працюють у висококонкурентному та динамічному фінансовому середовищі.

Ще одним інструментом удосконалення інформаційного забезпечення системи економічної безпеки банківських установ в контексті інтелектуальних технологій є розробка та впровадження банківського корпоративного ШІ-асистента (БКША), який працює виключно у закритому, контрольованому середовищі банку (on-premise або Private Cloud).

БКША – це система підтримки рішень для фахівців з інформаційної безпеки та комплаєнсу.

На відміну від публічних ШІ (ChatGPT, Gemini), внутрішній ШІ-Асистент навчається більшою мірою на внутрішній базі знань (документах та інших матеріалах банку). При цьому всі обговорення, скинуті матеріали в чати залишаються всередині і під контролем банку.

БКША зосереджений на трьох критичних напрямках (рис.3.1):

1. Регуляторний комплаєнс [32]:

- прискорений структурний аналіз нових постанов НБУ, виявлення ключових вимог, дедлайнів та відповідальних підрозділів;

- автоматичне зіставлення нових зовнішніх вимог з внутрішніми документами, ідентифікація прогалин та документів, що потребують змін.

2. Управління ризиками інформаційної безпеки:

- аналіз нової загрози чи вразливості та пропозиція попередньої оцінки ризику (високий/середній/низький) на основі внутрішнього досвіду та галузевих стандартів;

- генерація конкретних, адаптованих до інфраструктури банку, заходів для зниження ідентифікованих ризиків.

3. Генеративна підтримка:

- формулювання чернеток внутрішніх нормативних документів, інструкцій, службових листів та звітів щодо інформаційної безпеки, забезпечуючи високу якість та відповідність банківській термінології.

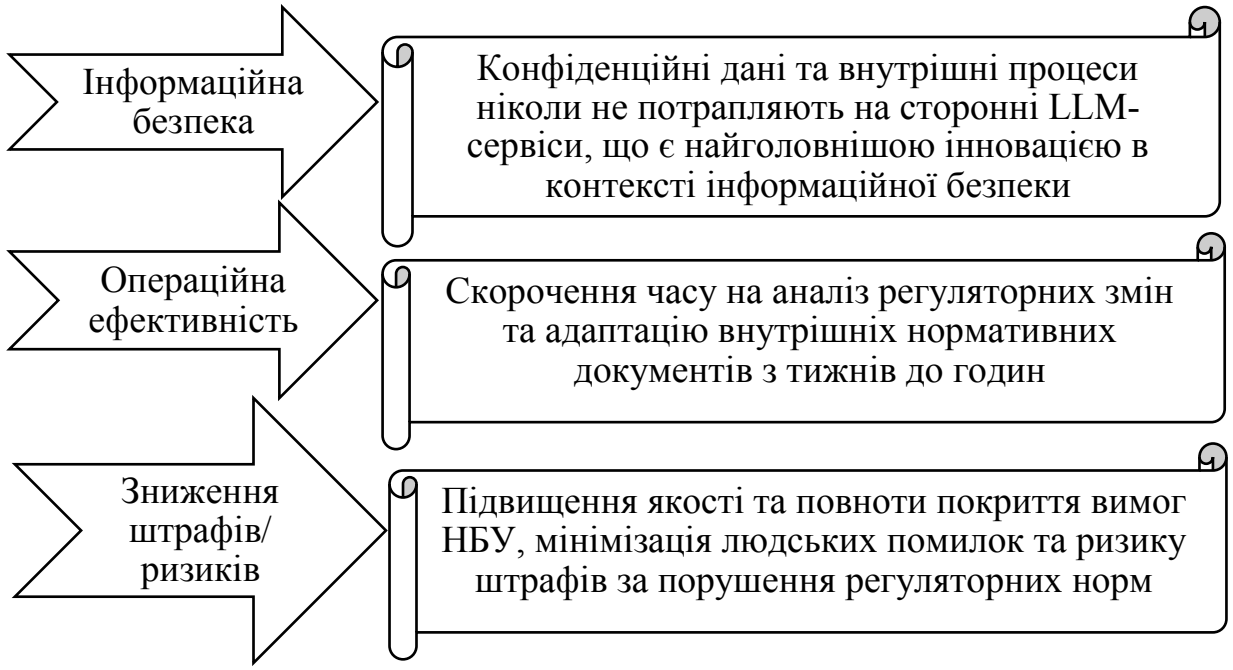

Рис. 3.1. Переваги від впровадження банківського корпоративного ШІ-асистента

Джерело: сформовано автором

Таким чином, застосування ШІ у системі інформаційного забезпечення економічної безпеки банківських установ є стратегічно важливим кроком для підвищення їх стійкості та ефективності управління ризиками. Удосконалення системи за допомогою інтелектуальних технологій дозволяє не лише автоматизувати рутинні процеси, а й забезпечити комплексний, динамічний та превентивний підхід до захисту фінансової стабільності банку.

Особливу увагу слід приділяти поєднанню ШІ з існуючими процесами внутрішнього контролю, управління ліквідністю та аналітичними системами.

У результатів інтеграції з’являється можливість формування адаптивних моделей ризик-менеджменту, які здатні не тільки оцінювати поточну ситуацію, а й прогнозувати потенційні загрози в умовах мінливої економічної кон’юнктури.

3.3. Оцінювання ефективності інформаційно-аналітичної системи банку за допомогою економіко-математичних методів

Інформаційно-аналітична система (ІАС) банківських установ є ключовим елементом забезпечення економічної безпеки та ефективного управління фінансовими потоками банку. Основне завдання системи полягає у своєчасній обробці даних, формуванні аналітичних звітів та наданні керівництву повної та достовірної інформації для прийняття стратегічних та оперативних рішень. Ефективність ІАС визначається такими критеріями, як швидкість обробки даних, точність інформації, рівень інтеграції модулів і здатність забезпечувати мінімізацію ризиків. Для кількісної оцінки застосовуються економіко-математичні методи, що дозволяють розраховувати інтегральний показник ефективності, провести сценарне моделювання та визначити оптимальні шляхи розподілу ресурсів.

Структура ІАС банку складається з чотирьох основних модулів: фінансового, ризикового, клієнтського та звітного. Фінансовий модуль відповідає за обробку операційних даних, аналіз доходів, витрат та прибутку банку, моніторинг ліквідності та платоспроможності. Ризиковий модуль здійснює облік кредитних, ринкових та операційних ризиків, прогнозування негативних сценаріїв і визначення резервів. Клієнтський модуль забезпечує ведення бази даних клієнтів, моніторинг їх фінансового стану та кредитної історії. Звітний модуль формує аналітичні звіти для внутрішніх і зовнішніх користувачів та інтегрується з фінансовими і ризиковими модулями.

Для оцінювання ефективності ІАС пропонуємо застосовувати інтегральний показник E_{IAC}, який розраховується за формулою:

$$E_{IAC} = \sum_{i=1}^{n} \omega_i \times Q_i$$

де,

ω_i – питома вага модуля у загальній системі;

Q_i – оцінка ефективності модуля за критеріями точності, повноти та актуальності даних (0-1);

n – кількість модулів.

Для АТ «УНІВЕРСАЛ БАНК» оцінки модулів виглядають так (табл.3.5):

Таблиця 3.5

Оцінка модулів АТ «УНІВЕРСАЛ БАНК»

Модуль	Питома вага ω_i	Показник ефективності Q_i
Фінансовий	0,35	0,95
Ризиковий	0,25	0,90
Клієнтський	0,20	0,85
Звітний	0,20	0,80

Таким чином, інтегральний показник ефективності ІАС дорівнює:

E_{IAC} = 0,35*0,95+0,25*0,90+0,20*0,85+0,20*0,80 = 0,8875

Результат E_{IAC} = 0,89 свідчить про високий рівень ефективності ІАС банку, що забезпечує своєчасне та достовірне інформаційне забезпечення управлінських рішень. Для більш детальної оцінки було проведено щомісячний моніторинг ефективності модулів протягом 2024 року (табл.3.6).

Таблиця 3.6

Щомісячний моніторинг ефективності модулів, 2024 р.

Місяць	Фінансовий Q_1	Ризиковий Q_2	Клієнтський Q_3	Звітний Q_4	Інтегральний E_{IAC}
Січень	0.94	0.89	0.85	0.80	0.884
Лютий	0.95	0.90	0.85	0.80	0.888
Березень	0.95	0.91	0.86	0.81	0.895
Квітень	0.96	0.90	0.86	0.82	0.899
Травень	0.96	0.92	0.87	0.82	0.908

Червень	0.97	0.91	0.87	0.83	0.912
Липень	0.97	0.90	0.88	0.83	0.911
Серпень	0.96	0.91	0.88	0.84	0.913
Вересень	0.96	0.92	0.88	0.84	0.918
Жовтень	0.97	0.92	0.89	0.85	0.924
Листопад	0.97	0.91	0.89	0.85	0.922
Грудень	0.98	0.92	0.90	0.86	0.932

Джерело: сформовано автором

Дані свідчать про стабільну та високу ефективності системи протягом року, з помірним зростанням у другій половині 2024 р. після проведення оптимізації модулів.

Сценарне моделювання показує вплив зміни ефективності окремих модулів на інтегральний показник. Наприклад, у разі зниження ефективності ризикового модуля на 50% через технічні збої інтегральний показник розраховується:

$$E_{IAC,\text{сцен}} = 0{,}35*0{,}95+0{,}25*0{,}90*0{,}5+0{,}20*0{,}85+0{,}20*0{,}80 = 0{,}8175$$

Зниження ефективності на $\sim$ 7% демонструє чутливість системи до якості ризикового модулю та необхідності заходів щодо його стабілізації.

Для оптимізації використовується задача максимізації інтегрального показника при обмеженому бюджеті на модернізацію модулів. При наявності бюджету 1000000 грн на рік ресурс розподіляється наступним чином: фінансовий модуль – 400 тис.грн, ризиковий – 300 тис.грн, клієнтський – 150 тис.грн, звітний – 150 тис. грн. після оптимізації показники ефективності модулів збільшується:

Таблиця 3.7

Оптимізовані модулі АТ «УНІВЕРСАЛ БАНК»

Модуль	Оптимальний Q_i^*
Фінансовий	0,98
Ризиковий	0,92
Клієнтський	0,90
Звітний	0,85

Таким чином, інтегральний показник оптимізації дорівнює:

$$E^{*}_{IAE}$$ = 0,35*0,98+0,25*0,92+0,20*0,90+0,20*0,85 = 0,92

Підвищення інтегрального показника на 3% відображає ефект раціонального розподілу і модернізації ключових модулів системи.

Додатково проводяться допоміжні розрахунки для оцінки середнього часу формування звітів та обсягу оброблених транзакцій. Середній час формування операційного звіту – 15 хв, фінансового – 60 хв, ризикового – 120 хв, звітного – 45 хв. Кількість оброблених записів на місяць коливається від 50 000 до 500 000, а кількість помилок не перевищує 0,5 %.

Високі показники ефективності ІАС дозволяють банку знизити ризики фінансових втрат, підвищити оперативність прийняття рішень та забезпечити точне і своєчасне аналітичне супроводження діяльності [40]. Рекомендації щодо подальшого вдосконалення включають модернізацію ризикового і фінансового модулів, підвищення інтеграції інформаційних потоків, регулярне навчання персоналу та застосування сценарного моделювання для прогнозування можливих відхилень у роботі системи.

Економіко-математичне моделювання ефективності інформаційно-аналітичної системи АТ «УНІВЕРСАЛ БАНК» демонструє високу результативність системи та забезпечує основу для прийняття управлінських рішень щодо підтримки економічної безпеки банку. Інтегральний показник E_{IAC} як базовий 0,89 і після оптимізації 0,92 свідчить про стабільну та надійну роботу системи, що підтверджує її ключову роль у забезпеченні інформаційного супроводу фінансової діяльності та економічної безпеки банку.

Отже, ефективність інформаційно-аналітичної системи АТ «УНІВЕРСАЛ БАНК» має ключове значення для забезпечення економічної безпеки та стабільності фінансової діяльності установи, оскільки саме від точності, швидкодії та узгодженості її модулів залежить якість управлінських рішень і здатність банку своєчасно реагувати на ризики. Це доводить, що сучасна інформаційно-аналітична система є не лише технічним

інструментом, а стратегічним ресурсом банку, який формує основу його конкурентоспроможності й захищеності в умовах динамічних змін фінансового ринку.

Висновки до третього розділу

1. Визначено, що аналітична платформа моніторингу ризиків є багаторівневою системою, яка включає модулі збору даних, інтеграції та зберігання інформації, аналітики та прогнозування, візуалізації, а також контролю та оповіщення про критичні ризики. Інтеграційний модуль платформи дозволяє об’єднувати дані з різних джерел у єдину інформаційну модель. Використання хмарних сховищ та технологій типу Data Warehouse або Data Lake забезпечує масштабованість, швидкий доступ до інформації та можливість обробки великих обсягів даних у режимі реального часу.

2. Запропоновано впровадження багаторівневого контролю доступу до інформаційних систем банку, що включає диференційовані права доступу залежно від ролі співробітника, а також сегментацію систем для обмеження поширення потенційних загроз. Визначено практичні заходи багаторівневого контролю доступу та шифрування даних: розмежування доступу; шифрування даних; моніторинг подій у реальному часі; багатофакторна аутентифікація.

3. Встановлено, що ключовим напрямом є розробка та впровадження протоколів реагування та кіберінциденти, що передбачає створення чітких процедур для виявлення, класифікації та усунення кіберзагроз, включаючи інструкції для оперативного відновлення систем після атак та заходи щодо зменшення негативних наслідків. Наголошено, що важливим компонентом є навчання персоналу.

4. Одним із ключових рішень є впровадження системи інтегрованого моніторингу ризиків, яка дозволяє об’єднати всі критичні показники ризиків у єдину аналітичну платформу. Запропоновано концепцію «єдиного вікна» інтегрованого моніторингу, яка відображає всі основні категорії ризиків та

їхнє оновлення в режимі реального часу для оперативного управління.

5. Визначено основні інструменти штучного інтелекту та їх функціональне застосування в банківській системі економічної безпеки. Запропоновано до впровадження банківський корпоративний ШІ-асистент, який працює виключно у закритому, контрольованому середовищі банку (on-premise або Private Cloud). Наведено переваги від впровадження банківського корпоративного ШІ-асистента.

6. Проведене економіко-математичне моделювання ефективності інформаційно-аналітичної системи АТ «УНІВЕРСАЛ БАНК» показало, що система забезпечує високий рівень оперативності, точності та повноти обробки даних, що сприяє своєчасному прийняттю управлінських рішень та зниженню фінансових ризиків. Інтегральний показник E_{IAC} у базовому сценарії становив 0,89, а після оптимізації ресурсів модулів зростає до 0,92, що свідчить про можливість підвищення ефективності системи за рахунок модернізації ключових модулів та інтеграції інформаційних потоків.

ВИСНОВКИ

1. Констатовано, що у сфері банківського менеджменту інформаційне забезпечення економічної безпеки можна визначити як цілеспрямований процес створення, обробки, аналітичного використання та захисту інформаційних ресурсів, необхідних для підтримання стабільності фінансових потоків, збереження конфіденційності банківський даних і своєчасного реагування на ризики.

2. Досвід останніх років підтвердив, що порушення інформаційної безпеки мають не лише технічний, а й системний вплив - вони здатні викликати втрату ліквідності, масовий відтік депозитів і значні репутаційні втрати. Відповідно, кіберстійкість стала невід'ємною складовою фінансової стабільності, а інвестиції у кіберзахист - стратегічним пріоритетом банківського менеджменту. Український досвід, сформований у надзвичайно складних умовах воєнних дій, довів, що адаптивність, інтегровані ІТ-рішення та системний моніторинг загроз здатні забезпечити ефективну протидію навіть наймасштабнішим кібератакам.

3. АТ «УНІВЕРСАЛ БАНК» - це український комерційний банк, заснований у 1994 році. Він входить до групи ТАС і відомий як банкір-партнер мобільного додатку monobank, який працює на його базі. Банк є сучасним фінансовим інститутом, який надає широкий спектр банківських послуг як фізичним, так і юридичним особам. Комплексна оцінка фінансового стану АТ «УНІВЕРСАЛ БАНК» свідчить про стабільно високий рівень фінансової стійкості та ефективності діяльності. Інтегрований показник протягом аналізованого періоду перебуває у межах 7,48-7,84 балів, що відповідає рейтингу «А» - високий фінансовий стан.

4. Встановлено, що структура системи економічної безпеки банку передбачає функціонування Департаменту економічної безпеки, Департаменту ризиків. А також низки спеціалізованих управлінь і відділів,

які взаємодіють між собою у процесі збору, аналізу та обробки інформації про фінансові, операційні та репутаційні загрози. Відмічено, що рівень організації системи економічної безпеки АТ «УНІВЕРСАЛ БАНК» досить високий. Виявлення загроз відбувається постійно, а аналіз є доволі глибоким. Використовуються різні методики складання аналітичних документів, наприклад, звітність про ризики будується на базі міжнародних стандартів, таких як Basel III для банків.

5. За результатами розрахунків інтегральний показник економічної безпеки АТ «УНІВЕРСАЛ БАНК» становить 0,85, що відповідає високому рівню безпеки. Це свідчить про ефективне функціонування системи управління ризиками, стабільний фінансовий стан та здатність банку адаптуватися до зовнішніх загроз.

6. Система інформаційної безпеки АТ «УНІВЕРСАЛ БАНК» будується на принципах комплексності, багаторівневості та відповідності міжнародним стандартам (ISO/IEC 27001, ISO/IEC 22301) та вимогам НБУ. В результаті дослідження встановлено, що структура Департаменту інформаційної безпеки АТ «УНІВЕРСАЛ БАНК» побудована за принципом функціонального розподілу повноважень і відповідності між окремими управліннями. До складу департаменту входять шість ключових управлінь, кожне з яких відповідає за певний напрям діяльності в межах загальної системи безпеки банку.

7. Для оцінки рівня ефективності інформаційного забезпечення було використано комплексний підхід. Що включає технічний, організаційний та навчальний компоненти. При цьому інтегральний показник ефективності 4 з 5, що свідчить про стабільну та ефективну систему, яка потребує вдосконалення в навчанні персоналу та автоматизації процесів.

8. Запропоновано інтеграційний модуль аналітичної платформи, який дозволяє об’єднувати дані з різних джерел у єдину інформаційну модель. Розроблено концепцію «єдиного вікна» інтегрованого моніторингу, яка відображає всі основні категорії ризиків та їхнє оновлення в режимі

реального часу для оперативного управління.

9. Запропоновано впровадження багаторівневого контролю доступу до інформаційних систем банку, що включає диференційовані права доступу залежно від ролі співробітника, а також сегментацію систем для обмеження поширення потенційних загроз. Визначено практичні заходи багаторівневого контролю доступу та шифрування даних: розмежування доступу; шифрування даних; моніторинг подій у реальному часі; багатофакторна аутентифікація.

10. Встановлено, що ключовим напрямом є розробка та впровадження протоколів реагування та кіберінциденти, що передбачає створення чітких процедур для виявлення, класифікації та усунення кіберзагроз, включаючи інструкції для оперативного відновлення систем після атак та заходи щодо зменшення негативних наслідків. Важливим компонентом є навчання персоналу.

11. Доведено, що одним із перспективних напрямів є інтеграція інструментів штучного інтелекту у системи управління ризиками та моніторингу діяльності банку. Запропоновано до впровадження банківський корпоративний ШІ-асистент, який працює виключно у закритому, контрольованому середовищі банку (on-premise або Private Cloud). Наведено переваги від впровадження банківського корпоративного ШІ-асистента.

12. Проведене економіко-математичне моделювання ефективності інформаційно-аналітичної системи АТ «УНІВЕРСАЛ БАНК» показало, що система забезпечує високий рівень оперативності, точності та повноти обробки даних, що сприяє своєчасному прийняттю управлінських рішень та зниженню фінансових ризиків. Інтегральний показник E_{IAC} у базовому сценарії становив 0,89, а після оптимізації ресурсів модулів зростає до 0,92, що свідчить про можливість підвищення ефективності системи за рахунок модернізації ключових модулів та інтеграції інформаційних потоків. Результати дослідження підтверджують, що інформаційно-аналітична система є надійним інструментом забезпечення економічної безпеки банку та

ефективного управління його фінансовими ресурсами.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Баланда А.Л. Проблеми забезпечення інформаційної безпеки банківських автоматизованих систем. *Інформаційний прості*. 2025. №6. С.23-29.

2. Бандурка О.М. Економічна безпека підприємства: стратегічне управління в умовах ризику. Харків: Право, 2021. 256 с.

3. Барановський О., Путінцева Т. Формування комплексної програми забезпечення фінансової безпеки комерційних банків. *Світ фінансів*. 2021. № 3 (68). С. 65–79

4. Бєлоусова К.І., Бєлоусов Я.І. Забезпечення інформаційної безпеки – реалізація стратегії банківської установи. *Науковий вісник ДУІКТ*. 2020. С.33-38. 5.

5. Бондаренко О. Інформаційно-аналітичне забезпечення управління фінансовими ресурсами суб'єктів господарювання. *Економіка та держава*. 2018. № 6. С. 21–24.

6. Бондарчук Л., Мазур Н., Цалко Т., Коваленко М., Заріцька Н., Пузирьова П. Інноваційний дизайн фінансово-управлінського обліку та впливу міграції населення на розвиток агропідприємств в умовах безпекових та інформаційних ризиків. *Фінансово-кредитна діяльність: проблеми теорії та практики*. 2023. Т. 5 (52). Р. 481-493.

7. Варналій З. С. Економічна та фінансова безпека України в умовах глобалізації: монографія. Київ: Знання України, 2020. 423 с.

8. Васильців Т. Г. Інноваційні підходи до формування системи економічної безпеки суб’єктів господарювання. Львів: ЛНУ ім. І. Франка, 2022. 298 с.

9. Волощук Л. Обліково-аналітичне забезпечення управління інноваційним розвитком підприємства. *Праці Одеського політехнічного університету*. 2021. № 2. С. 329-334.

10. Гаряга Л.О., Куліш Р.Р. Фінансова безпека банківської діяльності в умовах цифровізації. *Проблеми економіки*. 2019. № 4 (42). С. 163–171.

11. Гречка В., Островський В., Білий, М. Розвиток системи фінансової безпеки банківських установ в умовах цифровізації. *Науковий вісник Полісся*. 2025. №2. С 461–478.

12. Диба М.О., Зубок М.І., Яременко С.М. Інформаційні ризики в банківській діяльності. *Вісник НБУ*. 2017. С.28-35.

13. Дубницький В.І., Науменко Н. Ю., Овчаренко О.В. Теоретико-методологічні аспекти забезпечення економічноі та інформаційноі безпеки регіону в умовах цифрової трансформації. *Держава та регіони*. 2021. № 3. С. 78-87.

14. Жарій Я. В., Сидоренко І. В. Система фінансово-інформаційної безпеки банків України: проблеми та перспективи розвитку. Концептуальні засади формування фінансово-економічної безпеки: колективна монографія / за заг. ред. С. М. Шкарлета. Ніжин: ФОП Лук'яненко В. В.; ТПК «Орхідея», 2015. С. 240–256.

15. Жилін С.В. Теоретико-методичні засади державного регулювання діяльності банківських установ в контексті формування інформаційного суспільства. http://repositsc.nuczu.edu.ua/btream/123456789/25209/1/Zhylin.pdf

16. Засадна Х.О. Стандарти управління інформаційною безпекою. *Фінансовий простір*. 2021. №3. С.60-64.

17. Захаров О. Інформація в управлінні системою економічної безпеки підприємства. *Вчені записки Університету КРОК*. 2019. №19. С.177-186.

18. Зубок М.І. Безпека банківської діяльності. Навч. посібник. К.: КНЕУ, 2022. 190 с.

19. Кісільов О.І., Качков С.О. Сутність інтегрованого управління проєктними та операційними ризиками в організації. *Управління розвитком складних систем.* 2023. № 55. С. 46–54.

20. Клюско Л. А., Москаленко Н. В. Інновації у сфері банківського бізнесу. Збірник наукових праць *Університету державної фіскальної служби України*. 2019. № 2. С. 109–128.

21. Коваленко В. В. Фінансова безпека банків: реалії та перспективи забезпечення. *Економічний форум*. 2022. № 2. С. 141–151.

22. Козаченко І.П., Голубєв С.В. Загальні принципи захисту банківської комп'ютерної інформації. Центр дослідження проблем комп'ютерної злочинності. URL: http:// www.crime-research.ru/library/Koz_gol.htm.

23. Котик О.В., Стасюк Б.Б., Щур О.О. Діяльність національного банку України в умовах війни. *Вісник Національного університету водного господарства та природокористування*. 2024. Вип. 2. С. 69–77.

24. Крамаренко К., Вінниченко О. Інформаційно-аналітичне забезпечення управління фінансово-економічною безпекою суб'єктів господарювання. *Сталий розвиток економіки*. 2024. №3(50). С. 344-349.

25. Кульчицький І. І. Цифрова економіка та економічна безпека підприємства: стратегії управління. *Актуальні питання економічних наук*, 2024, №6. С. 115-123.

26. Лазаришина І. Джерела інформаційно-аналітичного забезпечення економічної безпеки підприємства. *Вісник економіки транспорту і промисловості*. 2023. №38. С. 62-65.

27. Лісняк А. Є. Чинники фінансової безпеки банків. *Вісник університету банківської справи*. 2023. № 3 (30). С. 77-82.

28. Лісняк А. Є. Формування стратегії забезпечення фінансової безпеки банку. *Науковий вісник Ужгородського національного університет*. 2018. № 22(2). С. 72–77.

29. Ліхоносова Г. С. Інструменти зміцнення економічної безпеки: цифровізація та усунення соціально-економічного відторгнення. *Інвестиції: практика та досвід*. 2023.№19. С. 16-21.

30. Ліхоносова Г. С. Фінансова безпека країни в умовах цифровізації

соціальноекономічних процесів. *Часопис економічних реформ*. 2023. № 2. С. 48-53.

31. Луньова М. Інформаційна безпека як основа фінансової стабільності: досвід українських банків. Фінансово-економічна безпека: теоретико-методичні засади та практичні інструменти управління: колективна монографія / за заг. ред. Губарик О.М., Васільєвої Л.М. ДДАЕУ, Дніпро: Журфонд, 2025. С. 182-192.

32. Луньова М. Підходи щодо вдосконалення інформаційного забезпечення системи економічної безпеки банківської установи. Облік, аудит, оподаткування та звітність у системі забезпечення економічної стійкості підприємств: тези доповідей IX Всеукраїнської науково-практичної Інтернет-конференції 8-9 травня 2025 р. ДДАЕУ, Дніпро, 2025. С. 147-149.

33. Марущак А.І. Інформаційна безпека банківської установи: структура та система забезпечення. Суми : ДВНЗ «УАБС НБУ», 2020. С.21-24.

34. Матвійчук Н. М., Теслюк С. А. Основні тенденції розвитку банківських інновацій в Україні. *Економічний часопис Волинського національного університету імені Лесі Українки.* 2021. № 1 (25). С. 79-87.

35. Мордань Є. Ю., Журавка О. С., Діденко К. В., Кравченко Я. І. Фінансова безпека банків: сутність та оцінка. *Бізнес-інформ*. 2021. С. 243-251.

36. Москаленко Н. Концептуальні аспекти фінансової безпеки банку. *Зб. наукових праць Державного податкового університету*. 2024.№1.С 53-58.

37. Онищенко С., Глушко А. Інформаційно-аналітичне забезпечення фінансової безпеки підприємств у сучасних умовах. *Науковий вісник Одеського національного економічного університету.* 2023. №. 7. С. 135–154.

38. Отенко І. П., Мішин О. Ю., Мішина С. В. Організація та управління фінансово-економічною безпекою банківських установ: навч. посібник. Х.: ХНЕУ ім. С. Кузнеця, 2015. 240 с.

39. Про хмарні послуги: Закон України від 17.02.2022 № 2075-IX URL: https://zakon.rada.gov.ua/laws/show/2075-20#Text

40. Решетов С. Вплив цифрової трансформації економіки на економічну безпеку. *Менеджмент та підприємництво: тренди розвитку*. 2022. Вип. 4. С. 8-16.

41. Ролдугіна Ю.В., Ковальова І.В. Особливості інформаційної безпеки банків. *Актуальні проблеми економічного і соціального розвитку регіону*. 2021. С.283-287.

42. Родченко С. Забезпечення системи безпеки комерційного банку за вартісно-орієнтованим підходом: інформаційно-аналітичний аспект. *Науковий вісник ЛДУ внутрішніх справ*. 2018. №2. С. 111–119.

43. Світлична В.Ю. Забезпечення інформаційної безпеки банківських установ. *Економіка.* 2024. №1. С.172-175.

44. Стечишин Ю. Сутність та складові інформаційно-аналітичного забезпечення системи економічної безпеки банківських установ. *Вчені записки Університету «КРОК».* 2025. №1. С 379-387.

45. Сухонос В. В. Концептуальні організаційно-правові засади функціонування системи економічної безпеки банків. *Правовий вісник Української академії банківською справи*. 2021 № 1. С. 64–66.

46. Шелудько С. А. Цифровізація банківської діяльності в Україні як виклик і рушій у забезпеченні фінансової безпеки. *Проблеми сучасних трансформацій.* 2025. №18. https://doi.org/10.54929/2786-5738-2025-18-08-07

47. Хвальчик І., Волощук Л. Сутність інформаційно-аналітичного забезпечення управління. *Економіка: реалії часу*. 2020. № 1 (47). С. 84-90.7

48. Фурман В. М., Зачосова Н. В. Сучасні загрози економічній безпеці вітчизняних фінансових установ (на прикладі банківських установ і страхових компаній). *Інвестиції: практика та досвід*. 2025. № 16. С. 7–11.

49. Olshanska O. Financing innovative activities as a factor of ensuring financial and economic security of industrial enterprises in the conditions of continuous development. *Формування ринкових відносин в Україні*. 2021. № 11.

С. 42-50.

50. Tkachenko V., Tkachenko I., Puzyrova P., Klochko A.Organizational and economic mechanism of a business security as a guarantee of its sustainable development. *Virtual Economics*. 2019. Vol. 2. №. 4. P. 71-85.

ДОДАТКИ

Додаток А

Оцінка ліквідності, платоспроможності та оборотності оборотних активів АТ «УНІВЕРСАЛ БАНК», тис. грн.

№ з/п	Показник	Нормативне значення	2020 р.	2021 р.	2022 р.	2023 р.	2024 р.	2024 р. у %до 2020 р.
1. Оцінка ліквідності								
1.1	Високоліквідні активи (А1)	≥П1	665,000.0	718,000.0	802,000.0	52,000.0	60,000.0	9.02
1.2	Середньолікві дні активи (А2)	≥П2	81,200.0	96,430.0	6,770.0	12,015.0	17,260.0	21.26
1.3	Низьколіквідні активи (А3)	≥П3	160.0	195.0	220.0	245.0	280.0	175.00
1.4	Найбільш строкові зобов'язання (П1)	≤А1	730.0	870.0	1,010.0	1,150.0	1,290.0	176.71
1.5	Короткострокові зобов'язання (П2)	≤А2	671,150.0	726,400.0	811,650.0	891,900.0	52,450.0	7.81
1.6	Довгострокові зобов'язання (П3)	≤А3	6,650.0	7,930.0	9,210.0	10,490.0	11,770.0	176.99
2. Оцінка платоспроможності								
2.1	Коефіцієнт абсолютної ліквідності	≥0,2	96.34	98.99	98.96	5.87	6.06	6.29
2.2	Проміжний коефіцієнт покриття	≥0,7	108.03	112.20	99.09	6.01	6.19	5.73
2.3	Коефіцієнт покриття (загальної ліквідності)	≥2	108.07	112.25	112.71	113.22	113.25	104.79
2.4	Коефіцієнт загальної платоспроможності	Збільшення	109.63	113.80	114.74	115.65	115.93	105.74

Додаток Б

Комплексна оцінка фінансового стану АТ «УНІВЕРСАЛ БАНК»

№ з/п	Показники	2020 р.		2021 р.		2022 р.		2023 р.		2024 р.		Питома вага (Vi, %) в інтегровано-му показнику
		Значення	Рейтинг	Значення	Рейтинг	Значення	Рейтинг	Значення	Рейтинг	Значення	Рейтинг	
1	***Показники ліквідності***											
1.1	Коефіцієнт поточної ліквідності	1.08	7	1.12	7	1.13	7	1.13	7	1.13	7	8
1.2	Коефіцієнт швидкої ліквідності	1.08	10	1.12	10	0.99	10	0.06	1	0.06	1	8
2	***Показники ділової активності***											
2.1	Період оборотності дебіторської заборгованості, днів	193.0	0	105.8	0	287.0	0	54.8	10	77.3	9	9
2.2	Період оборотності оборотних запасів, днів	0.1	10	0.1	10	0.1	10	0.1	10	0.1	10	9
2.3	Період оборотності активів, днів	209.4	0	112.1	0	87.2	0	61.4	0	85.6	0	9
3	***Показники фінансової незалежності***											
3.1	Коефіцієнт фінансової незалежності	91.22	2	87.88	3	87.16	3	86.95	3	95.33	1	9
3.2	Частка оборотних активів, сформованих за рахунок власних коштів	10.15	6	10.91	6	11.82	7	12.18	7	12.14	7	9
Інтегрований показник фінансового стану		**7.48**		**7.57**		**7.66**		**7.84**		**7.57**		**100**
Рейтинг фінансового стану		**A**		**A**		**A**		**A**		**A**		

Додаток В
Карта ризиків АТ «УНІВЕРСАЛ БАНК»

Категорія ризику	Тип ризику	Ймовірність виникнення	Потенційний вплив	Пріоритет реагування	Заходи мінімізації
Кредитний ризик	Невиконання зобов’язань клієнтами	Висока	Високий	Високий	Кредитний скоринг, стрес-тестування портфеля, ліміти на позики
	Зростання простроченої заборгованості	Середня	Високий	Середній	Моніторинг платежів, автоматизовані нагадування, реструктуризація боргу
Операційний ризик	Помилки у внутрішніх процесах	Середня	Середній	Середній	Автоматизація процесів, внутрішній аудит, регламенти роботи
	Несанкціоновані операції	Низька	Високий	Високий	Системи контролю доступу, двофакторна аутентифікація, моніторинг аномалій
Ризик ліквідності	Нестача грошових коштів для виконання зобов’язань	Середня	Високий	Високий	Планування грошових потоків, резерви ліквідності, короткострокові кредити
Ринковий ризик	Коливання процентних ставок	Середня	Середній	Середній	Хеджування процентних ризиків, диверсифікація портфеля
	Коливання валютних курсів	Низька	Середній	Низький	Хеджування валютних позицій, валютна диверсифікація
Репутаційний ризик	Негативна інформація в ЗМІ	Низька	Високий	Середній	Моніторинг медіа, PR-стратегія, швидке реагування на скандали
	Невдоволення клієнтів	Середня	Середній	Середній	Система зворотного зв’язку, покращення обслуговування клієнтів

Додаток Д

Концепція «єдиного вікна» інтегрованого моніторингу та управління ризиками