РОЗДІЛ 2 РЕЗУЛЬТАТИ ГОСПОДАРСЬКОЇ ДІЯЛЬНОСТІ ПІДПРИЄМСТВА, ЕФЕКТИВНІСТЬ ВИРОБНИЦТВА ТА ЕКОНОМІЧНА БЕЗПЕКА

2.1. Інтегрована система управління ризиками як основа фінансової безпеки банківських установ

© Кравченко В. П.
канд. екон. наук, доцент,
Центральноукраїнський національний технічний університет,
м. Кропивницький, Україна

Фінансова безпека банківської системи є ключовою умовою стабільності всієї економіки, адже банки виконують роль основних посередників у перерозподілі фінансових ресурсів, забезпечують кредитування бізнесу та населення, а також підтримують функціонування платіжної інфраструктури.

Упродовж 2022 – 2024 рр. банківська система України демонструвала загальну стійкість, незважаючи на складні економічні та геополітичні умови. Основні фінансові показники – достатність капіталу, рівень ліквідності, прибутковість – свідчать про здатність банків адаптуватися до кризових викликів. Зокрема, коефіцієнт достатності капіталу перевищував 20 % у 2022 – 2023 рр. і досягнув приблизно 21 % у 2024 р. Короткострокова ліквідність (LCR) стабільно трималась вище 200 %, а у 2024 р. зросла до понад 210 %, що свідчить про високий рівень платоспроможності банків. Прибуток сектору у 2023 р. сягнув 67 млрд грн, а за підсумками 2024 р. – понад 72 млрд грн, що є рекордним показником за останні роки [1].

Попри позитивну динаміку ключових фінансових показників, банківська система України у 2022 – 2024 рр. залишалася вразливою до низки системних загроз, які не завжди проявляються у звітності, але мають потенціал дестабілізувати сектор у середньо- та довгостроковій перспективі.

Однією з найактуальніших проблем є збереження високої частки непрацюючих кредитів (NPL). Хоча показник поступово знижувався з 29 % у 2022 р. до 25 % у 2024 р. він все ще перевищував критичні межі, прийняті у міжнародній практиці. Це свідчить про тривалий вплив кредитних ризиків, зумовлений зниженням платоспроможності позичальників, втратами бізнесу та загальним економічним спадом [2].

Не менш загрозливою є кількість кіберінцидентів, які зросли з 600 у 2022 р. до 1200 у 2024 р. [3]. Це вказує на зростання атак на цифрову інфраструктуру банків, що потребує посилення систем захисту, впровадження сучасних технологій моніторингу та підвищення кваліфікації персоналу (табл. 1).

Таблиця 1

Порівняння фінансової безпеки банківської системи України, 2022 – 2024 рр.

Показники	2022 р.	2023 р.	2024 р.
Достатність капіталу (CAR), %	19	> 20	21
Короткострокова ліквідність (LCR)	180	> 200	210
Частка непрацюючих кредитів (NPL)	29	27	25
Прибуток банківського сектору, млрд грн	25	67	72
Кількість кіберінцидентів	понад 600	понад 1000	понад 1200
Частка державних банків в активах, %	50	52	53

Джерело: розраховано автором за даними [3].

Крім того, у низці банків виявлено недоліки в системах управління ризиками, що проявлялися у непрозорості операцій, слабкому контролі за ризиковими активами та неефективному комплаєнсі. У відповідь на ці виклики Національний банк України у 2024 р. оновив нормативну базу, посиливши вимоги до організації систем управління ризиками [4].

Таким чином, наявність системних загроз, виявлених у банківському секторі України у 2022 – 2024 рр., свідчить про те, що фінансова стійкість не є абсолютною величиною, а потребує постійного оновлення інструментів захисту, адаптації регуляторної політики та вдосконалення внутрішніх процесів банківських установ. У цьому контексті особливої актуальності набуває питання інтегрованого управління ризиками, яке вже представлено у кількох концептуальних підходах сучасної банківської практики. Кожен із них має свої переваги, сфери застосування та певні обмеження.

Найбільш поширеною є модель “трьох ліній захисту”, яка передбачає розподіл відповідальності між операційними підрозділами, функціями контролю та внутрішнім аудитом. Цей підхід забезпечує базову структурованість, однак часто не враховує взаємозв’язок між різними типами ризиків і не охоплює нові загрози, зокрема цифрові та репутаційні [5].

Інша модель інтегрований ризик-менеджмент (IRM) яка передбачає централізовану платформу для збору, аналізу та моніторингу ризиків. Вона активно впроваджується в окремих українських банках у межах цифрової трансформації. Однак її застосування здебільшого обмежується технічними аспектами, без належної інтеграції в стратегічне управління [6].

Модель ризик-менеджменту на основі корпоративного управління акцентує увагу на включенні ризиків у процес прийняття стратегічних рішень. Вона передбачає активну участь наглядової ради та комітетів з ризиків, однак вимагає високої зрілості управлінських структур, що не завжди реалізовано на практиці [7].

Регуляторна модель, визначена Національним банком України, встановлює чіткі вимоги до організації системи управління ризиками, включаючи визначення ризик-апетиту, проведення стрес-тестування та формування звітності. Вона забезпечує відповідність нормативним вимогам, але часто орієнтована на формальні показники, не враховуючи специфіку окремих установ.

Узагальнюючи, можна стверджувати, що існуючі моделі управління ризиками мають значну теоретичну та практичну базу, проте залишаються фрагментарними, недостатньо адаптивними або не охоплюють нові типи ризиків, що актуалізує потребу в їх удосконаленні.

Водночас фінансова безпека банку не може розглядатися ізольовано від нефінансових ризиків. Зокрема, ризики комплаєнсу, кіберзахисту та внутрішнього ризик-менеджменту мають як прямий, так і опосередкований вплив на ключові фінансові показники, загальну стабільність функціонування банку та його репутацію. Ігнорування цих чинників здатне нівелювати навіть позитивні фінансові результати, що підкреслює необхідність інтегрованого підходу до управління ризиками.

Такий підхід базується на системному поєднанні трьох ключових компонентів:

1. Фінансові ризики – кредитний, ринковий, ризик ліквідності, процентний ризик. Їх оцінка та моніторинг є традиційною частиною банківського ризик-менеджменту.

2. Операційні та нефінансові ризики – комплаєнс, кібербезпека, внутрішній контроль, репутаційні ризики. Вони мають опосередкований, але критично важливий вплив на фінансові показники.

3. Стратегічні ризики – пов’язані з геополітичними процесами, регуляторними змінами, макроекономічними шоками, які формують зовнішнє середовище функціонування банку.

Інтегрований підхід передбачає створення єдиної системи управління ризиками, в межах якої всі типи ризиків аналізуються у взаємозв’язку, а управлінські рішення приймаються на основі консолідованої інформації. Це дозволяє:

– своєчасно виявляти приховані загрози, які можуть залишатися непоміченими під час ізольованого аналізу;

– забезпечувати проактивне реагування на зміни зовнішнього та внутрішнього середовища;

– підвищувати стійкість банку до комплексних кризових сценаріїв;

– оптимізувати розподіл ресурсів між напрямами управління ризиками;

– зміцнювати довіру з боку клієнтів, інвесторів і регуляторів завдяки прозорості та системності управлінських рішень;

– інтегрувати фінансові та нефінансові ризики у стратегічне планування банку.

Ураховуючи складність сучасного ризик-середовища та обмеженість традиційних підходів до управління ризиками, виникає об’єктивна потреба у створенні цілісної, адаптивної моделі, здатної забезпечити стійкість банківської установи в умовах багатовекторних викликів. Саме тому доцільним є розроблення інтегрованої системи управління ризиками, яка поєднує стратегічне бачення, операційну ефективність, аналітичну глибину та регуляторну відповідність.

Враховуючи потребу в системному, поетапному підході до управління ризиками, запропонована модель включає п’ять взаємопов’язаних рівнів, кожен з яких виконує окрему функцію в забезпеченні фінансової безпеки банку:

1. Стратегічний рівень. На стратегічному рівні управління ризиками здійснюється через діяльність Комітету з управління ризиками, який затверджує політику, визначає ризик-апетит банку та координує сценарне планування. Ризик-апетит формується у вигляді кількісних меж допустимих ризиків, наприклад: частка непрацюючих кредитів (NPL) не більше 10 %, коефіцієнт ліквідності (LCR) не нижче 150 %. Сценарне планування передбачає моделювання кризових ситуацій, таких як масова кібератака, дефолт контрагента чи валютна нестабільність, з подальшою оцінкою їх впливу на фінансову стійкість банку.

2. Операційний рівень. Операційний рівень охоплює щоденне управління ризиками через єдину платформу ризик-менеджменту, яка інтегрує всі типи ризиків – кредитний, ринковий, ліквідності, комплаєнс, кібербезпеку. Система раннього попередження дозволяє виявляти критичні відхилення за ключовими показниками, такими як падіння ліквідності чи зростання скарг клієнтів. Моніторинг нефінансових ризиків включає щоденний контроль транзакцій на предмет дотримання вимог AML, тестування IT-систем на вразливості, аудит внутрішніх процесів та реагування на операційні збої.

3. Аналітичний рівень. Аналітичний рівень забезпечує консолідацію даних з усіх підрозділів банку для формування повної картини ризиків. Стрес-тестування проводиться регулярно для оцінки впливу гіпотетичних кризових сценаріїв на капітал, ліквідність та прибутковість. Індикатори репутаційного ризику включають аналіз згадок у медіа, скарг клієнтів та соціальних мереж, що дозволяє оперативно реагувати на інформаційні загрози.

4. Регуляторна інтеграція. Система управління ризиками має бути узгоджена з вимогами Національного банку України. Це передбачає постійний моніторинг нормативів CAR, LCR, NPL, автоматичне формування звітності та адаптацію внутрішніх процедур до змін у нормативній базі. Важливим елементом є взаємодія з Центром кіберзахисту НБУ, що включає обмін інформацією про інциденти, участь у навчаннях та доступ до централізованих ресурсів безпеки.

5. Культурний компонент. Формування ризик-культури є основою ефективного управління. Це включає регулярне навчання персоналу, внутрішні комунікації щодо ризиків, мотивацію до дотримання процедур. Етичний кодекс банку регламентує поведінку співробітників, запобігає конфліктам інтересів та забезпечує захист прав клієнтів. Внутрішні механізми повідомлення про порушення сприяють прозорості та відповідальності.

Запропонована система являє собою комплексну модель, що забезпечує виявлення, оцінку, моніторинг та мінімізацію як фінансових, так і нефінансових ризиків (табл. 2).

Інтегрована система управління ризиками дозволяє банку не лише реагувати на загрози, а й проактивно керувати ними, забезпечуючи довгострокову фінансову стабільність, відповідність регуляторним вимогам та зміцнення довіри клієнтів.

Таблиця 2

Структура інтегрованої системи управління ризиками банку

Рівень	Компоненти
Стратегічний рівень	Комітет з управління ризиками: визначення ризик-апетиту; затвердження політики; сценарне планування
Операційний рівень	Єдина платформа ризик-менеджменту: кредитний ризик; ринковий ризик; ліквідність; комплаєнс; кібербезпека Система раннього попередження: індикатори NPL, LCR, CAR
Аналітичний рівень	Консолідована звітність: об'єднання даних з усіх підрозділів Стрес-тестування: моделювання кризових сценаріїв Індикатори репутаційного ризику: аналіз медіа, скарг
Регуляторна інтеграція	Відповідність вимогам НБУ: CAR, LCR, NPL Взаємодія з Центром кіберзахисту Підготовка до перевірок
Культурний компонент	Ризик-культура: навчання персоналу; внутрішні комунікації Етичний кодекс: запобігання конфліктам інтересів; захист прав клієнтів

Джерело: розроблено автором.

Таким чином, ефективне функціонування інтегрованої системи управління ризиками в банку потребує реалізації п'яти послідовних етапів керування, кожен з яких виконує окрему функцію в загальній архітектурі ризик-менеджменту. Це дозволить банківській установі не лише реагувати на ризики, а й проактивно керувати ними, забезпечуючи:

Системну стійкість до зовнішніх та внутрішніх загроз. Інтегрована система дозволяє банку не лише реагувати на окремі ризики, а й формувати цілісну картину загроз.

Завдяки взаємозв'язку між стратегічним, операційним, аналітичним і регуляторним рівнями, банк здатен витримувати вплив як внутрішніх збоїв (наприклад, порушення комплаєнсу), так і зовнішніх шоків (економічна нестабільність, кібератаки).

Адаптивність до змінного економічного, технологічного та регуляторного середовища. Система забезпечує гнучке реагування на зміни в економіці, технологіях, законодавстві та геополітиці. Завдяки сценарному плануванню, стрес-тестуванню та постійному оновленню політик, банк може оперативно адаптувати свої стратегії до нових умов.

Прозорість управлінських рішень і відповідність вимогам Національного банку України. Автоматизоване формування звітності, моніторинг нормативних показників (CAR, LCR, NPL) та взаємодія з регулятором забезпечують відповідність чинним вимогам. Прозорість процесів управління ризиками підвищує довіру з боку регуляторних органів і знижує ризик санкцій.

Оптимізацію ресурсів між напрямами ризик-менеджменту. Єдина платформа дозволяє ефективно розподіляти людські, фінансові та технологічні ресурси між управлінням фінансовими, операційними, стратегічними та репутаційними ризиками. Це зменшує дублювання функцій і підвищує ефективність роботи.

Зміцнення довіри з боку клієнтів, інвесторів і регуляторів. Системний підхід до ризиків демонструє відповідальність банку, його готовність до кризових ситуацій і здатність захищати інтереси клієнтів. Це сприяє формуванню позитивної репутації, залученню інвестицій та розширенню клієнтської бази.

Інтеграцію ризиків у стратегічне планування та корпоративну культуру. Ризики розглядаються не як окремі загрози, а як елемент стратегічного управління. Вони враховуються при ухваленні рішень, розробці нових продуктів, зміні бізнес-моделі. Формування ризик-культури серед персоналу сприяє відповідальному ставленню до процедур і підвищує загальний рівень корпоративної етики.

Алгоритм керування інтегрованою системою ризиків запропановано на рис. 1.

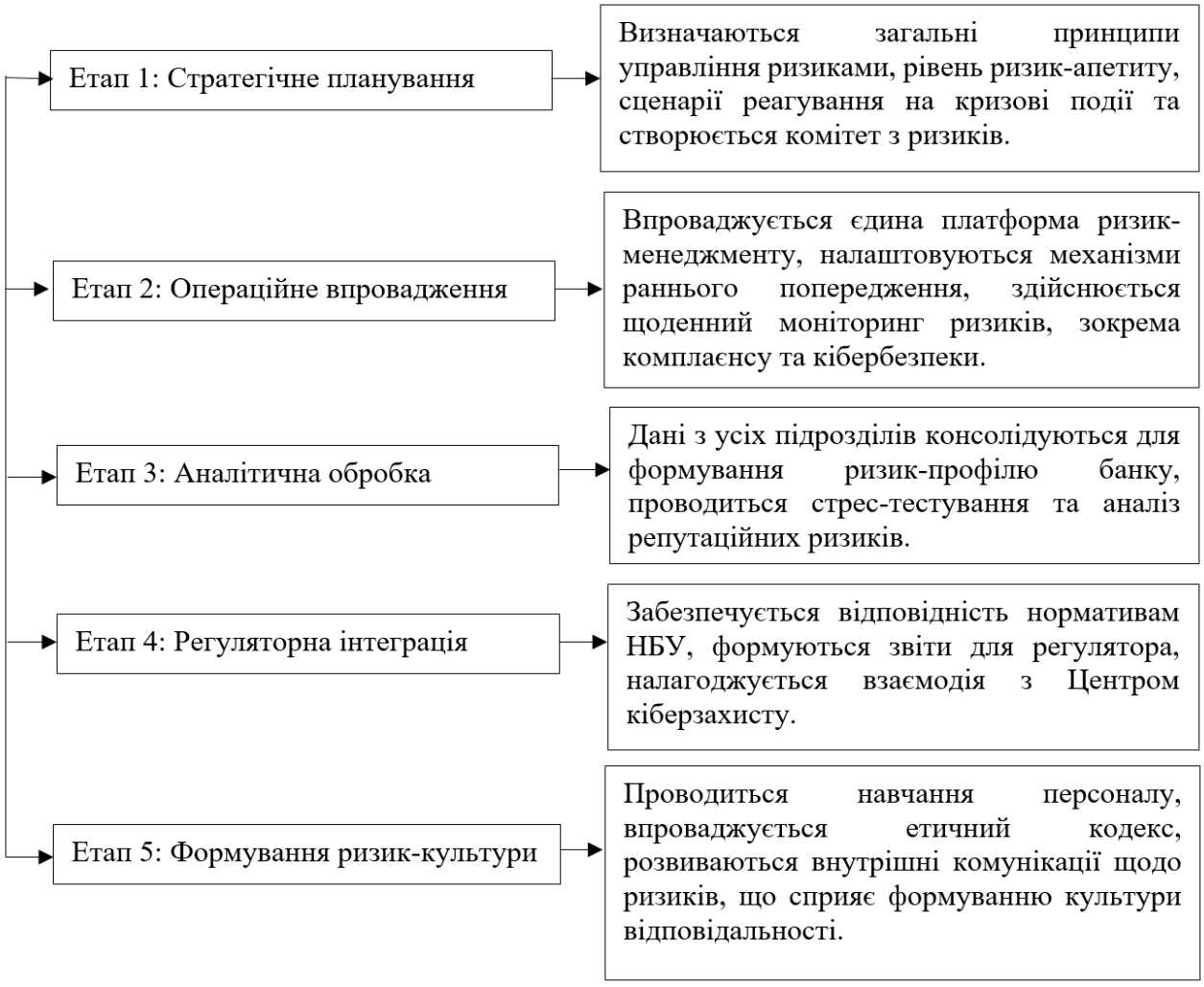

Рис. 1. Алгоритм керування інтегрованою системою ризиків

Джерело: розроблено автором.

Поетапне керування інтегрованою системою ризиків формує основу для довгострокової фінансової стабільності банку, підвищення його конкурентоспроможності та стійкості до кризових сценаріїв. Такий підхід дозволяє не лише систематизувати управління ризиками, а й забезпечити його гнучкість, адаптивність і стратегічну узгодженість.

У межах проведеного дослідження було здійснено комплексний аналіз сучасних підходів до управління ризиками в банківських установах України, з особливим акцентом на інтегровану модель ризик-менеджменту як стратегічний інструмент трансформації системи фінансової безпеки.

Фінансова безпека банківських установ в умовах зростаючих ризиків та цифрової трансформації потребує переходу від фрагментарного контролю до системного управління ризиками. Такий підхід охоплює стратегічний, операційний та технічний рівні, забезпечуючи узгодженість управлінських рішень і контрольних функцій.

Інтегрований ризик-менеджмент є ключовим компонентом сучасної банківської стратегії. Його застосування дозволить ефективно реагувати на багатовекторні виклики: фінансові, операційні, репутаційні та формувати адаптивну модель управління, здатну до швидкої трансформації в умовах нестабільності.

Розроблена в межах дослідження інтегрована система управління ризиками забезпечує: централізовану обробку та аналіз ризик-даних; проактивне виявлення загроз і сценарне моделювання; автоматизацію процесів контролю, звітності та внутрішнього аудиту; інтеграцію ризик-менеджменту в стратегічне планування; підвищення прозорості та ефективності управлінських рішень.

До переваг інтегрованої моделі можна віднести: зменшення дублювання функцій та витрат на контроль; посиленні міжфункціональної взаємодії між підрозділами; підвищенні довіри з боку регуляторів, інвесторів і клієнтів; гнучкості в умовах кризових змін та здатності до швидкої адаптації.

Таким чином, інтегрована система управління ризиками є не лише технологічним рішенням, а й стратегічною основою модернізації банківського сектору України. Її впровадження сприятиме підвищенню фінансової стійкості, конкурентоспроможності та довіри до національної банківської системи в умовах глобальних викликів.

2.2. Економічна безпека в системі безпеки підприємства

© Сонюк О. В.
канд. юрид. наук, доцент,
доцент кафедри правового забезпечення безпеки бізнесу,
Державно-торговельний економічний університет,
м. Київ, Україна

Еволюція підходів до захисту підприємництва, в т.ч. в умовах воєнних та політичних викликів, повоєнного відновлення України та її інтеграції до європейського простору орієнтує на розроблення цілісного комплексу заходів забезпечення безпеки бізнесу. Дослідження у цій сфері пройшли шлях від аналізу безпеки підприємництва на мікрорівні національної економіки до впровадження систем інтегрованого ризик-менеджменту в корпоративне управління відповідно до міжнародних стандартів.

Ретроспектива та врегулювання питання управління, розвиту і забезпечення безпеки вітчизняного підприємництва датується серединою XX – початком XXI ст. Дослідники історії розвитку сутності економічної безпеки підприємства