**ТЕМА 8. МОНІТОРИНГ ТА АУДИТ БАНКІВСЬКОЇ ДІЯЛЬНОСТІ**

**Моніторинг банківських ризиків**

Систематичний моніторинг ризиків є основою стабільної роботи банку. Він включає постійне спостереження за ключовими фінансовими показниками (достатність капіталу, ліквідність, якість кредитного портфеля тощо) та виконанням нормативів. Сучасні банки впроваджують автоматизовані системи контролю, що в реальному часі відстежують ці показники і сигналізують про відхилення. Такі системи дозволяють менеджменту оперативно реагувати на зміни та запобігати розвитку кризових ситуацій.

Нові підходи до моніторингу акцентують увагу на ранньому виявленні проблемних трендів. Замість реактивного реагування, банки використовують проактивні індикатори ризику та сценарний аналіз. Наприклад, моделі раннього попередження можуть виявити зростання прострочень по кредитах чи відтік депозитів ще до того, як ці тенденції призведуть до серйозних проблем. Стрес-тестування регулярно застосовується для прогнозування впливу несприятливих сценаріїв (економічний спад, зміна відсоткових ставок) на фінансовий стан банку. Отримані результати дозволяють завчасно вжити заходів для зміцнення стійкості балансу.

Особливу роль у сучасному моніторингу відіграють великі дані та штучний інтелект. Банки аналізують масиви транзакційних та поведінкових даних клієнтів з метою виявлення аномалій і ризикових моделей. Штучний інтелект здатний обробляти величезні обсяги інформації на високій швидкості, що робить його ефективним інструментом для моніторингу підозрілих операцій, виявлення випадків шахрайства та контролю за дотриманням регуляторних вимог. Наприклад, алгоритми машинного навчання можуть відстежувати нетипову активність на рахунках і таким чином своєчасно сигналізувати про можливе відмивання коштів чи інші незаконні дії. Застосування AI-технологій у ризик-менеджменті також дає змогу будувати прогностичні моделі, що попереджають про виникнення фінансових ризиків до того, як вони реалізуються.

**Внутрішній аудит і система контролю**

*Внутрішній аудит* – це незалежна оцінювальна функція всередині банку, яка контролює ефективність процесів управління та системи внутрішнього контролю. Сучасний підхід до внутрішнього аудиту є ризик-орієнтованим: ресурси аудиту спрямовуються першочергово на ті напрямки діяльності, які несуть найбільші ризики (кредитні операції, ринки капіталу, інформаційна безпека тощо). Внутрішні аудитори перевіряють відповідність операцій внутрішнім політикам і процедурам, оцінюють надійність систем контролю та надають рекомендації щодо їх вдосконалення. Таким чином, внутрішній аудит виступає однією з «ліній захисту» банку, допомагаючи своєчасно виявити недоліки до того, як ними скористаються зловмисники або вони призведуть до втрат.

Сьогодні внутрішній аудит активно інтегрується з цифровими рішеннями. Банки впроваджують програмні комплекси для автоматизації аудиторських перевірок і збору даних (Audit Management Software, системи бізнес-аналітики). Використання таких інструментів дозволяє проводити безперервний аудит: ключові показники контролюються у режимі реального часу, а відхилення автоматично фіксуються для подальшого аналізу. Наприклад, цифрові платформи аудиту можуть аналізувати всі транзакції (а не вибіркові вибірки, як у традиційному аудиті) і негайно виявляти аномалії або порушення. Завдяки машинному навчанню та AI, такі системи мінімізують людський фактор і підвищують точність перевірок. Це не лише прискорює аудиторські процедури, але й підсилює спроможність банку попереджувати операційні ризики та шахрайство.

Ефективна система внутрішнього контролю, яку оцінює аудит, є ключовою для запобігання шахрайству. Принцип розподілу обов’язків (separation of duties), багаторівневі дозволи на проведення операцій, регулярні звірки та інвентаризації – все це елементи внутрішнього контролю, що знижують ймовірність зловживань. Внутрішній аудит перевіряє виконання цих контрольних процедур і може виявити ознаки потенційного шахрайства (наприклад, маніпуляції з бухгалтерськими записами чи аномальні операції співробітників). Своєчасні аудиторські перевірки допомагають попередити значні втрати, підвищуючи операційну надійність банку.

**Зовнішній аудит та регуляторні вимоги**

Зовнішній аудит банку здійснюється незалежними аудиторськими компаніями з метою підтвердження достовірності фінансової звітності. Аудитори перевіряють, чи правильно банк відображає свої активи, зобов’язання, прибутки і ризики згідно з міжнародними стандартами фінансової звітності (наприклад, IFRS 9 для фінансових інструментів). Впровадження стандарту IFRS 9 стало викликом для аудиту, оскільки цей стандарт запровадив нову модель очікуваних кредитних збитків замість попередньої моделі понесених збитків. Тепер банки зобов’язані постійно оцінювати можливі втрати за кредитами, враховуючи історичні дані, поточні умови та прогнози, і завчасно формувати резерви під такі втрати. Зовнішні аудитори мають перевірити, що ці оцінки є обґрунтованими і відповідно відображені у звітності. Таким чином, сучасний зовнішній аудит фокусується не лише на перевірці минулих операцій, але й на адекватності резервів та оцінок майбутніх ризиків.

Окрім фінансової звітності, банки повинні дотримуватися багатьох регуляторних вимог, що перевіряються як зовнішніми аудиторами, так і наглядовими органами. Новітні міжнародні регуляції, такі як Базель IV, вимагають від банків підвищеної уваги до ризик-менеджменту та звітності. Базель IV запроваджує більш жорсткі підходи до розрахунку ризикованих активів і капіталу, а також нові вимоги до оперативного моніторингу ризиків. Зокрема, банки повинні забезпечити збір детальних даних по позиціях, розрахунок ризикових показників у реальному часі та наявність розширених аудит-трейлів для перевірки операцій. Ці зміни фактично змушують банки інвестувати значні кошти в сучасні технології, системи управління ризиками та операційну стійкість.

В Європейському Союзі набуває чинності новий регламент DORA (Digital Operational Resilience Act – Акт про цифрову операційну стійкість), який висуває окремі вимоги до ІТ-стійкості банків. Відповідно до DORA, фінансові установи зобов’язані дотримуватися суворих правил захисту від інцидентів, пов’язаних з інформаційно-комунікаційними технологіями (ІКТ). Це охоплює заходи з захисту, виявлення, локалізації та відновлення після кіберінцидентів, регулярне тестування оперативної стійкості та посилений контроль ризиків, пов’язаних з третіми сторонами (постачальниками ІТ-послуг). DORA закриває прогалину в регулюванні, наголошуючи, що операційна стійкість – це не лише питання капітальних буферів, а й здатність банку протистояти та швидко відновлюватися після ІТ-збоїв чи кібератак.

Ефективний зовнішній аудит і відповідність регуляторним стандартам безпосередньо впливають на довіру інвесторів та стейкхолдерів до банку. Аудит фінансової звітності за міжнародними стандартами підвищує впевненість користувачів у достовірності звітності та якості оприлюдненої інформації. Регулятори та інвестори розглядають позитивний аудиторський висновок як підтвердження фінансового здоров’я установи та належного управління ризиками. Водночас тісна співпраця зовнішніх аудиторів з наглядовими органами (центральними банками, комісіями) сприяє кращому розумінню банком очікувань регулятора і своєчасному усуненню виявлених недоліків.

**Методи оцінки якості активів та резервування**

Якість активів банку (передусім його кредитного портфеля) прямо впливає на фінансову стійкість. Тому оцінка якості активів та створення резервів під можливі збитки є одним з ключових елементів аудиту і нагляду. Банки класифікують свої кредити за ступенем ризику – від стандартних (без ознак проблеми) до непрацюючих (non-performing loans, NPL) – і відповідно оцінюють, скільки резервів потрібно відкласти на покриття потенційних втрат. Традиційно резервування базувалося на моделі понесених збитків: резерв формувався лише після того, як позичальник починав прострочувати платежі. Проте такий підхід часто призводив до запізнілого визнання проблем, особливо під час криз.

Сучасні стандарти вимагають більш прогностичного підходу. Впровадження IFRS 9 з 2018 року докорінно змінило методологію резервування, запровадивши концепцію очікуваних кредитних збитків (Expected Credit Loss, ECL). Тепер банки повинні оцінювати й визнавати кредитні втрати на випередження – ще до фактичного дефолту позичальника. Згідно з IFRS 9, якщо кредит тільки виданий і не має ознак значного погіршення, банк резервує суму очікуваних збитків на горизонті 12 місяців (Stage 1). Якщо ж кредитний ризик істотно зріс, резерв збільшується до суми очікуваних втрат за весь строк дії кредиту (Lifetime ECL, Stage 2). Коли актив уже вважається знеціненим (дефолтним), банк визнає повні втрати та формує резерв у розмірі різниці між балансовою вартістю і очікуваним відшкодуванням (Stage 3). Така трирівнева модель дозволяє раніше відображати проблеми з активами та створювати фінансові буфери до того, як збитки реалізуються.

Оцінка якості активів також спирається на систему внутрішніх рейтингів позичальників, аналіз фінансового стану клієнтів та вартості застав. Внутрішні моделі ризику (показники PD, LGD тощо) використовуються для кількісної оцінки ймовірності дефолту та рівня втрат у разі дефолту, що потім враховується в розрахунку резервів. Регулятори висувають жорсткі вимоги до адекватності таких моделей і припущень, закладених у них, щоб запобігти заниженню резервів. Нові норми (включаючи стандарти на кшталт IFRS 9 та настанови регуляторів) підвищили прозорість усього процесу: банки мають регулярно розкривати інформацію про якість своїх активів та сформовані резерви, обґрунтовувати моделі оцінки. Це сприяє ранньому виявленню накопичення проблемних боргів та формуванню достатніх резервів для покриття потенційних втрат.

**Сучасні технології у моніторингу та аудиті**

Технологічний прогрес відкриває нові можливості для підвищення ефективності моніторингу та аудиту. Штучний інтелект (AI) і машинне навчання вже широко застосовуються банками для аналізу даних у сфері ризик-контролю. AI-моделі можуть миттєво виявляти нетипову поведінку клієнтів у різних каналах (онлайн-банкінг, мобільні додатки, банкомати) та сигналізувати про потенційно шахрайські операції в режимі реального часу. Подібні системи моніторингу транзакцій допомагають ефективніше боротися з відмиванням коштів, відстежуючи підозрілі шаблони операцій, що можуть вказувати на фінансові злочини. Окрім того, сучасні скорингові моделі ризику активно використовують AI для оцінки кредитоспроможності: враховуючи сотні параметрів про позичальника, алгоритми прогнозують ймовірність дефолту значно точніше за традиційні методики. Це дозволяє банку приймати більш обґрунтовані рішення щодо видачі кредитів і вимог до забезпечення.

У сфері аудиту також впроваджуються передові технології. Спеціалізовані програмні рішення автоматизують рутинні процедури перевірки, збирають та агрегують дані з різних систем банку для аналізу. Використання Big Data-аналітики дає внутрішнім аудиторам можливість швидко виявляти тенденції або відхилення, які раніше лишалися непоміченими при вибіркових перевірках.

Також набувають розвитку антифрод-системи та інші цифрові засоби контролю. Це програмні комплекси, що відстежують дії користувачів і співробітників, аби запобігти внутрішньому шахрайству або витоку інформації. Наприклад, системи виявлення аномалій можуть сповістити службу безпеки, якщо працівник виконує незвично велику кількість операцій поза межами своїх повноважень. Крім того, впровадження технологій розширює можливості комплаєнс-контролю: алгоритми автоматично перевіряють відповідність операцій встановленим лімітам ризику, внутрішнім політикам тощо і оперативно повідомляють про порушення. Усі ці цифрові інструменти в сукупності підсилюють систему моніторингу та аудиту, роблячи її більш прозорою, оперативною і всеосяжною.

**Практичні кейси та рекомендації**

Передові банки світу вже сьогодні демонструють ефективність впровадження згаданих підходів. Вони створюють єдині «дашборди» ризиків, що об’єднують дані з різних підрозділів, і використовують прогнозну аналітику для оцінки майбутніх загроз. Наприклад, JPMorgan Chase розробила систему COIN на базі штучного інтелекту для автоматичного аналізу юридичних документів, що зекономило сотні тисяч годин роботи і знизило кількість помилок при обробці кредитних угод. Інші великі банки інвестують в системи кібербезпеки та антифрод-моніторингу, щоб захистити клієнтів і свої активи від сучасних кібер-загроз. Такі інвестиції окуповуються через підвищення операційної ефективності та довіри клієнтів.

Уроки минулих фінансових криз підкреслюють важливість належного моніторингу та аудиту. Фінансова криза 2008 року виявила, що недостатній контроль за якістю складних фінансових інструментів та слабкий ризик-менеджмент можуть призвести до катастрофічних наслідків для системи. В результаті глобальні регулятори посилили вимоги до капіталу і ризиків, а банки переглянули внутрішні політики та процедури.

Більш свіжий приклад – крах Silicon Valley Bank у 2023 році – став наслідком фундаментальних прорахунків в управлінні ризиками, особливо відсутності належного контролю за процентним ризиком (невідповідність між короткостроковими депозитами і довгостроковими активами). Звіт Федерального резерву США показав, що керівництво та контролери SVB проігнорували низку попереджувальних сигналів, а культура банку недооцінювала роль контролю порівняно зі стратегією агресивного зростання. Це підкреслює, що навіть високотехнологічні установи потребують сильної культури ризик-менеджменту та постійного нагляду.

На основі розглянутих матеріалів можна сформулювати такі рекомендації для банків:

* *Проактивний моніторинг ризиків:* Запровадити системи раннього попередження та регулярно проводити стрес-тести, щоб виявляти потенційні проблеми до того, як вони стануть критичними.
* *Інвестиції в технології контролю:* Використовувати штучний інтелект, аналітику великих даних та автоматизовані інструменти для підсилення якості моніторингу і аудиту (зокрема для виявлення шахрайства та точнішої оцінки ризиків).
* *Посилення внутрішнього контролю і аудиту:* Забезпечити незалежність та належні ресурси внутрішнього аудиту, регулярно переглядати внутрішні політики, впроваджувати культуру, в якій контроль та відповідність є не менш пріоритетними, ніж бізнес-цілі.
* *Відповідність міжнародним стандартам:* Дотримуватися актуальних регуляторних вимог (IFRS, базельські нормативи, DORA тощо) і підтримувати відкриту взаємодію з зовнішніми аудиторами та наглядовими органами. Це підвищує довіру інвесторів і забезпечує стійкість банківської діяльності навіть в умовах турбулентності.

Таким чином, сучасний моніторинг і аудит банківської діяльності переходять на новий рівень, характеризуючись більшою деталізацією, використанням передових технологій та посиленою увагою до ризиків. Інтегруючи ці підходи, банки можуть своєчасно виявляти та мінімізувати загрози, забезпечуючи стабільність фінансової системи і захист інтересів своїх клієнтів.