**ТЕМА 7. УПРАВЛІННЯ БАНКІВСЬКИМИ РИЗИКАМИ**

**Поняття управління ризиками та його значення**

*Управління банківськими ризиками –* це системний процес ідентифікації, оцінки та пом’якшення всіх видів ризиків, з якими стикається банк у своїй діяльності. До традиційних банківських ризиків належать кредитний ризик, ринковий ризик, ризик ліквідності, операційний та комплаєнс-ризик. Головна мета управління ризиками – захист фінансової стійкості банку, акціонерної вартості та довіри клієнтів, а також забезпечення дотримання регуляторних вимог.

У сучасному фінансовому середовищі значення ризик-менеджменту лише зросло. Складні глобальні зв’язки, цифровізація та нові загрози роблять банки більш вразливими, тож ефективне управління ризиками перетворилося на конкурентну перевагу банку, а не лише на засіб захисту. Нещодавні резонансні інциденти (наприклад, серія крахів банків у 2023 році) продемонстрували, що нехтування принципами управління ризиками може призвести до швидкої втрати ліквідності та довіри, ставлячи під загрозу саму життєздатність банку. Як відзначає експерт Sudhir Pai, у фінансовому секторі ризик-менеджмент відтепер є ядром кожного процесу – без належної уваги до ризиків та інвестицій у дані й інфраструктуру жодна банківська операція не може вважатися стійкою.

**Класифікація банківських ризиків у сучасних умовах**

Банки традиційно класифікують ризики на кілька ключових категорій:

* *Кредитний ризик* – небезпека невиконання позичальниками своїх зобов’язань.
* *Ринковий ризик* – можливі збитки від змін ринкових цін (процентних ставок, валютних курсів, вартості цінних паперів).
* *Ризик ліквідності* – небезпека нестачі коштів для виконання своїх зобов’язань у строк.
* *Операційний ризик* – втрати через збої внутрішніх процесів, людські помилки чи шахрайство, а також зовнішні події.
* *Ризик невідповідності* – ризик втрат від штрафів та збитків репутації через недотримання законів і нормативів.

Новітні тенденції привели до виокремлення нових видів ризиків, які раніше не отримували достатньої уваги. Зокрема, сьогодні банки приділяють значну увагу:

*Кіберризику та ІТ-ризику.* Стрімка діджиталізація породила ризики кібербезпеки та втрати даних. Кіберризик нині розглядається окремо (як підвид операційного ризику) – це загроза атак на інформаційні системи банку, витоку конфіденційних даних чи порушення безперервності цифрових сервісів. Наприклад, НБУ у 2023 році офіційно виокремив ризики інформаційно-комунікаційних технологій та кібербезпеки в структурі операційного ризику, що підкреслює актуальність цієї загрози. Одночасно впроваджено чіткі вимоги до управління цими ризиками згідно із законами про кібербезпеку.

*Кліматичним та ESG-ризикам.* Зростають екологічні й соціальні ризики, що впливають на банки. Кліматичний ризик включає фізичні ризики (прямі втрати від екстремальних погодних явищ, стихійних лих) та ризики переходу (фінансові втрати через перехід до низьковуглецевої економіки, наприклад знецінення активів у вугільній промисловості). Регулятори вимагають враховувати ці аспекти: належне управління ESG-ризиками визнається передумовою сталості банківського сектора. В Європі банки інтегрують кліматичні фактори у свої кредитні моделі та стрес-тести, хоча опитування показують, що ~60% банків ще розвивають відповідні методики. ESG-ризики також охоплюють соціальні та управлінські фактори – наприклад, ризик репутаційних втрат через недотримання прав людини або невідповідність корпоративного управління найкращим практикам.

*Ризику моделей.* Використання складних математичних моделей та алгоритмів (особливо на основі штучного інтелекту) породжує ризик помилок моделей. Неправильна модель оцінки кредитоспроможності або VaR може призвести до недооцінки ризиків і значних збитків. Тому зараз банки впроваджують суворі процедури валідації моделей та контролю їх якості. Наприклад, під час кризи 2008 року стало очевидно, що ненадійні моделі оцінки іпотечних паперів сприяли катастрофічним наслідкам – це урок, який закріплено в сучасних регуляціях щодо управління ризиком моделей.

*Ризику третьої сторони.* Широке використання аутсорсингу, фінтех-партнерів та хмарних сервісів створило ризик залежності від сторонніх провайдерів. Збої або неплатоспроможність критично важливого постачальника ІТ-послуг можуть прямо вплинути на банк. Тому банки запроваджують моніторинг ризиків контрагентів та плани безперервності бізнесу на випадок проблем у партнерів. Зокрема, європейське регулювання DORA (див. нижче) вимагає посилити оцінку ризиків постачальників технологій.

*Геополітичним та макроекономічним ризикам.* Сучасні банки враховують загрозу геополітичної нестабільності (санкції, військові конфлікти) і різких змін макроекономічних умов. Події на кшталт Brexit чи війни можуть спричинити одночасно і кредитні втрати (через спад економіки), і ринкові збитки, і ризик ліквідності. Наприклад, звіт PwC відзначає, що банки нині мусять маневрувати в умовах і кіберзагроз, і екологічних ризиків, і геополітичної невизначеності, які накладаються одночасно. Це вимагає гнучкішої та всеосяжної системи класифікації та моніторингу ризиків.

Таким чином, сучасна класифікація ризиків є багатовимірною. Вона поєднує класичні фінансові ризики з акцентом на новітні загрози (кібер, клімат, ESG, модельні, тощо). Банки переглядають внутрішні політики, щоб чітко визначити відповідальних за кожен новий сегмент ризику, та інтегрують ці фактори у загальну стратегію ризик-менеджменту.

**Сучасні методи оцінювання ризиків**

Аналіз та вимірювання ризиків суттєво еволюціонували завдяки новим технологіям і накопиченню даних. Нижче розглянуто сучасні підходи, які банки використовують для більш точного оцінювання своїх ризикових позицій.

*Big Data та аналітика даних.* Великі масиви даних (транзакції, поведінкові дані клієнтів, макроекономічні показники) дозволяють банкам отримати глибше розуміння ризиків. За допомогою технологій Big Data можна виявляти приховані закономірності та ранні ознаки проблем. Приміром, аналіз мільйонів транзакцій у реальному часі допомагає виявляти підозрілі операції та шахрайство ще до того, як вони призведуть до втрат. Об’єднуючи внутрішні дані банку з зовнішніми (ринковими, соціально-економічними), фінансові установи будують більш прогнозні моделі ризику. Це підвищує точність оцінки, дозволяючи проактивно управляти портфелями (напр., своєчасно знижувати позиції в сегментах, де зростає ризик).

*Машинне навчання у кредитному скорингу.* Штучний інтелект (AI) та машинне навчання наразі активно впроваджуються для оцінки кредитоспроможності позичальників. Традиційні скорингові моделі враховували обмежений набір фінансових показників, тоді як сучасні ML-алгоритми можуть опрацювати сотні змінних – від платіжної історії до поведінки в соцмережах. Це дає можливість точніше передбачати ймовірність дефолту. За даними експертів, провідні банки вже використовують штучний інтелект для аналізу великих обсягів клієнтських даних, виявлення патернів та більш точного оцінювання ризику. Практичний приклад – Banco Santander: банк запровадив AI-системи для прогнозування проблемних кредитів на ранній стадії, що дозволяє завчасно реагувати (наприклад, коригувати ліміти або умови позики). Деякі фінустанови (Standard Chartered, S-Bank Фінляндії) перейшли до автоматизованого ухвалення кредитних рішень на основі ML-моделей, що прискорює процес і мінімізує людський фактор. В результаті застосування AI в скорингу підвищує фінансову інклюзію – банки можуть оцінити позичальників без кредитної історії, використовуючи альтернативні дані, і запропонувати їм продукти. Водночас необхідно належним чином управляти ризиком моделі: забезпечувати прозорість алгоритмів, перевіряти їх на упередженість та оновлювати при зміні економічних умов.

*Сучасні підходи до stress-testing.* Стрес-тестування перетворилося на невід’ємний елемент оцінки ризиків банку. Після кризи 2008 року провідні центробанки запровадили регулярні стрес-тести, що перевіряють достатність капіталу банків за несприятливих сценаріїв (рецесія, обвал ринку нерухомості тощо). Сьогодні ці методики удосконалюються: банки використовують динамічні стрес-тести, моделюючи еволюцію балансу в часі, та часті стрес-тести для оперативного моніторингу. Новітня тенденція – включення кліматичних сценаріїв в stress-testing. Регулятори хочуть знати, як портфель банку витримає, скажімо, сценарій різкого підвищення цін на вуглецеві викиди або серію природних катаклізмів. Наприклад, ФРС США у 2023 році провела пілотний кліматичний сценарій для найбільших банків, де змоделювала наслідки урагану на Східному узбережжі. У 2022 році Банк Англії опублікував перші результати кліматичного стрес-тесту, оцінивши потенційні збитки банків за тривалих кліматичних змін. Такі аналізи допомагають виявити вразливі місця і заздалегідь скоригувати стратегію (наприклад, зменшити кредитування галузей з високим вуглецевим слідом чи збільшити резерви). Окрім кліматичних, розвиваються й інші нестандартні стрес-тести: кіберстрес-тести (моделювання широкомасштабної кібератаки), стрес-тести ліквідності з урахуванням масового відтоку депозитів (актуально після подій 2023 року) тощо. Сучасні технології дозволяють проганяти тисячі сценаріїв (використовуючи монте-карло симуляції) і отримувати розподіл можливих збитків, а не лише окремі точки. Це дає більш повну картину tail-risk – малоймовірних, але дуже руйнівних подій.

*Моніторинг ризиків у режимі реального часу.* Завдяки цифровим технологіям банки переходять від періодичних оцінок ризику (раз на квартал) до безперервного моніторингу. Автоматизовані інформаційні панелі збирають ключові метрики ризику щоденно чи щогодинно (VaR, ліквідність, показники ринкової волатильності). Це дозволяє менеджменту миттєво реагувати на стресові події – наприклад, якщо індикатори ліквідності падають нижче порогових значень, негайно скликати ризик-комітет і вжити заходів (продати ліквідні активи, залучити фінансування). Для цього банки впроваджують єдині сховища даних про ризики та аналітичні модулі, часто побудовані на хмарних технологіях, що агрегують інформацію з усього банку (трейдингу, кредитного підрозділу, ІТ-безпеки тощо) в реальному часі. Такий підхід підсилює проактивність ризик-менеджменту: замість реагувати постфактум на збитки, банк намагається передбачити та запобігти їм до того, як вони стануть критичними.

Отже, поєднання великого масиву даних, штучного інтелекту та удосконалених стрес-тестів дозволяє отримати більш повну і точну картину ризиків. Сучасний банк озброєний інструментами, що дають змогу не лише швидко виявити назріваючі проблеми, а й кількісно оцінити найгірші сценарії. Це надзвичайно важливо для прийняття обґрунтованих управлінських рішень у непевному фінансовому середовищі.

**Інструменти мінімізації ризиків та інноваційні рішення**

В арсеналі банків є численні методи мінімізації та хеджування ризиків: від диверсифікації портфеля і встановлення лімітів до використання страхування та деривативів (наприклад, свопів для хеджування процентного ризику чи кредитних деривативів для перенесення кредитного ризику). Сьогодні ці традиційні інструменти доповнюються новітніми технологічними рішеннями, що підсилюють ефективність ризик-менеджменту:

*Смарт-контракти* – це програми в середовищі блокчейну, які автоматично виконують умови договору при настанні визначених подій. У контексті управління ризиками, смарт-контракти можуть автоматизувати контроль за дотриманням умов і миттєво вживати захисні дії. Приміром, для ринкового ризику: смарт-контракт для деривативу може бути запрограмований автоматично закривати позицію або вимагати додаткове забезпечення, якщо ціна базового активу впаде до певного рівня. Це мінімізує людський фактор і швидко обмежує втрати (те, що у традиційному процесі могло б зайняти години і залежало б від уваги трейдера). Досвід DeFi (децентралізованих фінансів) демонструє дієвість такого підходу: на децентралізованих платформах позик смарт-контракти цілодобово слідкують за забезпеченням кредитів і ліквідують позиції, як тільки застави стає недостатньо, тим самим захищаючи протокол від збитків. Банки вивчають ці механізми, щоб запозичити їх для традиційних ринків. Приклад застосування: біржі та клірингові центри можуть перейти на смарт-контракти для виконання угод з цінними паперами – тоді одночасно з передачею цінних паперів буде автоматично переведена оплата, що виключає ризик розрахунку. Смарт-контракт може також автоматично нарахувати неустойку чи відсотки, якщо контрагент затримує платіж, без необхідності ручного втручання. Отже, smart contracts здатні знизити операційні ризики і прискорити процеси, хоча потребують пильного нагляду (помилка в коді сама по собі є новим джерелом ризику). Зауважимо, що регулятори поки обережно ставляться до повної автоматизації фінансових контрактів, але поступово виробляються стандарти їх безпечного використання.

*Open Banking (відкритий банкінг):* Ініціативи відкритого банкінгу (як-от PSD2 в ЄС) зобов’язують банки ділитися фінансовими даними клієнтів із сторонніми фінтех-компаніями через API за згодою клієнта. Хоч на перший погляд це створює більше ризиків (наприклад, ризик витоку даних при передачі третім сторонам), правильно реалізований open banking підвищує загальну стійкість та прозорість фінансової екосистеми. По-перше, відкритий обмін даними стимулює банки вдосконалювати кібербезпеку та протоколи захисту інформації. Нові стандарти API передбачають сильне шифрування та багато-факторну автентифікацію, що зменшує ризик несанкціонованого доступу. Фактично, open banking примушує банки посилити відповідність найкращим практикам безпеки, тим самим знижуючи ризик витоку даних. По-друге, завдяки open banking банки отримують ширший доступ до даних про клієнтів, зокрема про їхні рахунки в інших установах. Це дає повнішу картину фінансового становища позичальника і дозволяє точніше оцінити його кредитний ризик. Наприклад, якщо малий бізнес дає згоду на передачу даних з усіх своїх банків, кредитор побачить сумарні обороти і зможе виявити ризикові сигнали (спад виручки, збільшення позик в іншому банку) раніше. Відповідно, банк може завчасно відкоригувати ліміти чи вимоги до забезпечення, запобігаючи дефолту. По-третє, open banking відкрив простір для інноваційних сервісів ризик-менеджменту. Фінтех-стартапи пропонують банкам аналітичні платформи, що в режимі реального часу агрегують дані різних банків та попереджають про аномалії (корисно для відстеження операційного та шахрайського ризику). Самі ж споживачі, отримавши доступ до своїх даних, можуть краще керувати фінансами, знижуючи ймовірність прострочень (наприклад, за допомогою мобільних додатків з управління бюджетом, які через API знають про всі зобов’язання клієнта і нагадують про платежі). Таким чином, відкритий банкінг при належному управлінні ризиками сприяє більшій прозорості, конкуренції та стійкості фінансової системи. Звісно, це вимагає суворого дотримання стандартів безпеки та конфіденційності: банки впроваджують програми управління ризиками третьої сторони, щоб моніторити, як фінтех-компанії використовують надані дані, і запобігати зловживанням.

*Інноваційні рішення для комплаєнсу (RegTech):* Зростання регуляторних вимог спонукало появу окремого класу технологій – RegTech (Regulatory Technology) для автоматизації дотримання нормативів. Наприклад, системи моніторингу транзакцій у реальному часі з алгоритмами AI дозволяють миттєво виявляти підозрілу активність згідно з вимогами фінансового моніторингу і заморожувати кошти до з’ясування обставин. Це мінімізує ризик штрафів і репутаційних втрат за недотримання правил протидії відмиванню коштів. Такі рішення беруть на себе рутинну роботу перевірки клієнтів (KYC), санкційних списків, звітності для регулятора – знижуючи операційний ризик людських помилок і одночасно роблячи систему більш надійною та прозорою. Інший напрям – SupTech (Supervisory Tech), де й самі регулятори використовують інновації (аналітику даних, AI) для нагляду за банками. В Україні, до речі, НБУ впроваджує СупТех та РегТех ініціативи, що в перспективі спростить банкам виконання вимог і дозволить регулятору ранніше виявляти ознаки дестабілізації окремих установ.

В цілому, інноваційні інструменти не замінюють класичні методи, але значно підсилюють можливості банків у передбаченні та стримуванні ризиків. Водночас банки мусять пам’ятати, що нові технології приносять і нові виклики.

**Актуальні вимоги регуляторів**

Регуляторне середовище у сфері банківських ризиків динамічно розвивається після фінансових криз, під впливом нових викликів (як-то кліматичних) та технологічних змін. Основні актуальні тренди та вимоги такі:

*Базельські стандарти (Базель III та IV).* Після кризи 2008 р. Базельський комітет з банківського нагляду запровадив Базель III – пакет правил щодо капіталу, ліквідності та важелів, аби посилити стійкість банків. У 2017 р. було погоджено фінальне доопрацювання цих реформ, неофіційно відоме як “Базель IV”, імплементація якого почнеться з 2025 року. Базель IV привносить кілька важливих змін у розрахунок ризиків і капіталу банків:

* По-перше, обмежено використання внутрішніх моделей банків для оцінки кредитного ризику великих корпоративних позичальників. Банки більше не зможуть вільно застосовувати власні моделі для великих корпорацій (з виручкою понад €500 млн) – це зроблено, щоб вирівняти підхід і унеможливити занадто оптимістичні оцінки ризику великих експозицій.
* По-друге, запроваджено “output floor” – мінімальне обмеження на вигоду від внутрішніх моделей. Якщо банк раніше розраховував свої ризик-зважені активи по внутрішніх моделях значно нижче, ніж за стандартним регуляторним підходом, тепер вводиться нижня планка: оцінка ризику не може бути меншою ніж 72,5% від стандартного підходу. Іншими словами, внутрішні моделі не повинні давати занадто великої економії капіталу.
* Додатково уточнено методики для розрахунку операційного ризику (новий єдиний підхід замість безлічі варіантів) та ринкового ризику (реформа FRTB – фундаментальний перегляд торговельної книги).
* Загальна мета Базеля IV – підвищити порівнюваність і надійність капітальних вимог, не стільки збільшуючи обсяг капіталу глобально, скільки вирівнюючи правила гри між банками різних юрисдикцій. Для багатьох європейських банків нові вимоги означатимуть збільшення ризик-зважених активів і, відповідно, потребу наростити капітал, особливо для тих, хто активно використовував власні моделі. Очікується, що це може дещо підвищити вартість кредитування для позичальників в ЄС (~на 0,25–0,5 в.п. за оцінками досліджень). Впровадження відбудеться поступово до кінця десятиліття, щоб пом’якшити вплив на банківське кредитування.

Нові вимоги ЄС до стійкості банківської системи. Євросоюз, імплементуючи Базельські стандарти, паралельно запроваджує власні ініціативи для підвищення стійкості банків:

* По-перше, триває робота над CRR3/CRD6 – новими редакціями Регламенту та Директиви про капітальні вимоги, які впроваджують елементи Базеля IV в ЄС з 2025 року. Вони включають вищезгаданий output floor, жорсткіші вимоги до розрахунку ризиків, а також заходи для малих та середніх банків (пропорційне регулювання).
* По-друге, ЄС приділяє дуже велику увагу операційній та ІТ-стійкості фінансового сектора. Зокрема, ухвалено Цифровий акт про операційну стійкість (DORA), який набуде чинності з січня 2025 р. Він зобов’язує усі фінансові установи в ЄС впровадити комплексну систему управління ІТ-ризиками та кіберризиками, проводити регулярні тестування на стійкість (penetration tests, сценарії відмов систем) і контролювати ризики від третіх сторін. DORA встановлює високі вимоги до безперервності бізнесу, планів реагування на інциденти та резервних систем. Фактично, кожен банк повинен мати план дій на випадок кіберкризи і демонструвати регулятору здатність швидко відновити критичні послуги. Також DORA вводить нагляд за постачальниками ІТ-послуг (хмарні сервіси, процесінгові центри) – найбільших із них ЄС визначатиме як “критичних” і буде здійснювати прямий нагляд, аби зменшити системний ризик від аутсорсингу ІТ.
* По-третє, ESG-регулювання: Європейська банківська влада (EBA) видала рекомендації щодо інтеграції ESG-факторів у управління ризиками банків. Вимоги поступово стають обов’язковими: банки у ЄС мають розкривати показники сталого розвитку (Taxonomy Regulation, SFDR), оцінювати кліматичні ризики в ICAAP (процесі оцінки адекватності капіталу) і готуватися до кліматичних стрес-тестів. Планується включити кліматичні буфери чи підвищені ваги ризику для “коричневих” активів, якщо банки не скоротять концентрацію в високо вуглецевих галузях. Усе це – частина нових вимог до стійкості банківської системи в умовах переходу до зеленої економіки.
* Регулювання відкритого банкінгу та даних. PSD2 у ЄС вже кілька років як діє, але на підході PSD3/PSR (Payment Services Regulation), які ще більше розширять сферу відкритого банкінгу та посилять вимоги кібербезпеки. Крім того, прийнято Регламент про управління даними (Data Governance Act), що впливає і на банки у частині роботи з персональними даними клієнтів.

Український центробанк також активно оновлює регуляції у сфері ризик-менеджменту, часто гармонізуючи їх з європейськими нормами:

* *У 2018 році НБУ запровадив Положення про організацію системи управління ризиками в банках*, що зобов’язує всі банки мати розгорнуту систему ризик-менеджменту, ризик-апетит, політики і процедури за кожним видом ризику, а також незалежний підрозділ з управління ризиками на чолі з CRO (Chief Risk Officer). Це положення (постанова Правління НБУ №64 від 11.06.2018) встановило мінімальні стандарти: наявність комітету з ризиків у наглядовій раді, регулярну оцінку внутрішнього капіталу під ризики (ICAAP) і внутрішньої ліквідності (ILAAP) тощо.
* *Останні зміни 2023 року.* НБУ у квітні 2023 актуалізував згадане Положення, врахувавши нові виклики. Зміни (постанова Правління НБУ №40 від 30.03.2023) передбачають: виокремлення в структурі операційного ризику ІТ-ризиків та кіберризику (з чіткими дефініціями цих понять); уточнення вимог до управління інформаційною безпекою згідно з законом про кібербезпеку; удосконалення вимог до ринкового ризику – зокрема, впровадження концепції торгового портфеля (“трейдинг-дески”) та нових критеріїв розмежування торгової і банківської книги). Також банки зобов’язані розкривати в управлінській звітності інформацію про судові провадження, що є додатковим заходом для обліку юридичного та репутаційного ризику. НБУ дав банкам час до жовтня 2023 для внесення змін у внутрішні документи з управління ризиками відповідно до нових вимог. Паралельно регулятор встановив графік впровадження нового порядку розрахунку ринкового ризику (імовірно, наближеного до стандартів Basel’s FRTB): тестові розрахунки наприкінці 2023, повноцінне запровадження з 2024 року.
* *Нагляд на основі ризиків.* Важливо, що НБУ перейшов до ризик-орієнтованого нагляду, що відповідає принципам Basel Core Principles. Це означає, що інспекції та дистанційний нагляд фокусуються на найбільш ризикових сферах діяльності банку. Реалізована система SREP (Supervisory Review and Evaluation Process) – комплексна оцінка профілю ризиків банку, якості ризик-менеджменту і достатності капіталу для покриття ризиків. За підсумками SREP НБУ може встановлювати додаткові буфери капіталу для конкретного банку або вимагати зменшити ризикові активи.
* *Вимоги до капіталу та ліквідності.* Україна вже запровадила основні нормативи Базель III: коефіцієнт покриття ліквідності LCR (з 2018 р.), норматив чистого стабільного фінансування NSFR (з 2021 р.), контрциклічний буфер (введено, але поки 0%), буфер системної важливості для найбільших банків. Мінімальні вимоги до капіталу приведені до європейських (10% адекватність основного капіталу, 7% – Tier1). У 2020-21 рр. НБУ тимчасово послаблював вимоги через COVID-19, дозволяючи використовувати буфери, але зараз курс на їх відновлення.
* *Окремі ризики.* НБУ вимагає від банків наявності політик управління окремими специфічними ризиками, як-от ризик процентної ставки в банківській книзі (IRRBB) – він став актуальним після різких змін ставок у 2022-23 рр. Банки мають оцінювати, як зміна процентних ставок вплине на їх чистий процентний дохід та економічну вартість капіталу, і тримати цей ризик у встановлених межах. Так само приділяється увага концентраціям кредитного ризику – існують ліміти на великі кредити та інсайдерські кредити, щоб обмежити концентраційний ризик.
* *Адаптація до воєнних ризиків.* Після початку війни в 2022 р. НБУ запровадив мораторій на деякі вимоги (стрес-тестування банків було відкладене), однак водночас банки мусили оперативно впроваджувати плани реагування на екстремальні операційні ризики (резервні копії даних, релокація ІТ-систем, відновлення роботи відділень). Вимога мати план безперервності бізнесу стала не просто формальністю, а реально перевіряється на практиці. Регулятор у Звітах про фінансову стабільність відзначає, що українські банки змогли зберегти операційну стійкість та продовжити роботу навіть в умовах війни, значною мірою завдяки налагодженим процедурам управління ризиками та запасам капіталу.

Таким чином, регулятори сьогодні висувають до банків жорсткі вимоги в сфері ризик-менеджменту. Нові правила (Базель IV, європейські директиви, вимоги НБУ) охоплюють як фінансові ризики (капітал під кредитний/ринковий ризик), так і нефінансові аспекти стійкості – кібербезпеку, оперативну надійність, стійкість до кліматичних змін. Банки повинні постійно вдосконалювати свої системи, аби відповідати цим стандартам. Невиконання регуляторних вимог загрожує не лише штрафами, але й підвищеним ризиком для самого банку – адже вимоги сформовані на основі уроків минулих криз. У підсумку, регуляторний тиск стимулює банки бути далекогляднішими та більш дисциплінованими у менеджменті ризиків, що зміцнює всю фінансову систему.

**Реальні приклади з банківської практики останніх років**

Щоб краще зрозуміти наведені концепції, розглянемо кілька показових прикладів із нещодавньої практики банків, які ілюструють важливість належного управління ризиками та наслідки прорахунків:

*Крах Silicon Valley Bank (США, 2023)* – приклад провалу в управлінні процентним та ліквідним ризиком. SVB був середнього розміру банком, активним у технологічному секторі. У період низьких ставок він інвестував значні кошти в довгострокові облігації. Коли у 2022–2023 рр. ставки ФРС різко зросли, вартість цих облігацій впала, що спричинило величезні нереалізовані збитки у портфелі SVB. Одночасно велика частка депозитів банку була незастрахованою (понад 90%), і схвильовані новинами клієнти почали масово вилучати кошти. Завдяки соціальним мережам паніка поширилася блискавично – за лічені дні стався класичний bank run, і 10 березня 2023 банк збанкрутував. Цей випадок показав, наскільки важливо проводити стрес-тести ліквідності та процентного ризику і диверсифікувати депозитну базу. Уроки SVB вже враховуються: регулятори США планують посилити нагляд за середніми банками, вимагаючи від них кращого управління процентним ризиком в банківській книзі (IRRBB) та підтримання достатньої високоліквідної резервної бази.

*Crédit Suisse (Швейцарія, 2021–2023)* – приклад накопичення ризиків через поганий корпоративний контроль і репутаційні втрати. Один з найбільших банків Швейцарії зазнав серії скандалів і збитків: у 2021 році банк втратив понад $5 млрд через крах хедж-фонду Archegos (CS не встежив за концентрацією експортної позики) та заморозив ~$10 млрд фондів, пов’язаних з Greensill Capital. Ці події проявили слабкість внутрішніх політик ризик-менеджменту – банк дозволив клієнтам брати надмірні кредити під сумнівні забезпечення, не відстежував належно їхній ризиковий профіль. Внаслідок цього було зіпсовано репутацію і підірвано довіру інвесторів. Попри спроби реорганізації, в березні 2023, на фоні загальної нервозності після випадків SVB, Credit Suisse зіткнувся з відтоком коштів і падінням вартості акцій. Швейцарський центробанк був змушений організувати термінове поглинання CS банком UBS, щоб запобігти його неконтрольованому краху. Цей приклад підтверджує: ризик-менеджмент має бути невід’ємною частиною культури банку, а повторні збої в контролі ризиків і комплаєнсі (як у випадку CS) неминуче накопичують проблеми та можуть звалити навіть глобальний банк. Для топ-менеджменту це урок про персональну відповідальність: після Archegos керівників підрозділів ризику було звільнено, але репутаційна шкода вже була нанесена. Банки по всьому світу переглянули ліміти на контрагентів та практики margin-call після ситуації з Archegos.

*Використання AI для зниження кредитного ризику.* Позитивний приклад: широкомасштабне впровадження машинного навчання дозволило банкам покращити якість кредитного портфеля. Зокрема, в одному з кейсів впровадження AI-системи скорингу призвело до 15% зростання схвалення заявок при одночасному зниженні дефолтів на 10%. Це демонструє, як інновації в оцінці ризиків розширюють бізнес-можливості без погіршення його якості. Приклад Santander вже згадувався: банк завдяки predictive analytics скоротив частку “раптових” дефолтів, виявляючи проблемних позичальників заздалегідь. Інший приклад – Monobank та інші цифрові банки, які активно використовують нетрадиційні дані (поведінкові, дані смартфона) для оцінки позичальників. В результаті вони змогли вийти на сегменти, які раніше вважалися надто ризикованими (молодь без кредитної історії тощо), і утримати прийнятний рівень дефолтів. Ці випадки ілюструють потенціал Big Data та AI: краща оцінка ризику дозволяє і прибуток підвищити, і зробити фінансові послуги доступнішими, зберігаючи керованість ризиками. Водночас банки вчаться управляти і ризиком моделей – проводять незалежні перевірки алгоритмів, щоб уникнути ситуацій, коли модель збільшує ризики (наприклад, непередбачувано змінює критерії і починає схвалювати завідомо погані кредити).

*Кібератаки на банки та важливість кіберзахисту.* Останні роки відзначились кількома гучними інцидентами кібербезпеки у фінансовій сфері. Наприклад, у 2021 хакери зламали системи одного з великих банків Нової Зеландії, що спричинило багатогодинний простій онлайн-сервісів. У 2019 сталася масштабна крадіжка даних у Capital One (США) – компрометація персональних даних ~100 мільйонів клієнтів через помилку конфігурації хмарного серверу. Ці інциденти завдали значних репутаційних втрат і штрафів. Вони служать нагадуванням, що операційні та кіберризики реальні та потребують постійних інвестицій. Банки відповіли підсиленням кіберзахисту: збільшено бюджети на ІТ-безпеку, створено центри моніторингу кіберзагроз (SOC), проводяться регулярні навчання персоналу з кібергігієни. Українські банки під час війни 2022 також відбивали безпрецедентні кібератаки і навчились підтримувати роботу навіть під час блекаутів – фактично пройшли екстремальне випробування операційної стійкості. Досвід показав, що інвестувати в превентивні заходи дешевше, ніж потім ліквідовувати наслідки кібератаки, а відмова онлайн-банкінгу навіть на кілька годин серйозно б’є по довірі клієнтів. Тому кіберризик тепер на контролі не лише технічних фахівців, а й ради директорів банків.

Наведенні приклади підтверджують ключові тези: ефективне управління ризиками – це не теорія, а життєва необхідність для банку. Помилки або недбалість в цій сфері швидко приводять до реальних втрат, тоді як передові підходи дають конкурентну перевагу. Кожна криза чи інцидент стає уроком, який галузь враховує, вдосконалюючи практики ризик-менеджменту.

Загалом, сучасне управління банківськими ризиками являє собою комплексну, багатоаспектну систему, яка пронизує всі рівні діяльності банку – від фронт-офісу до ради директорів. Ми розглянули, як класичні поняття ризик-менеджменту еволюціонували під впливом нових трендів: з’явилися нові види ризиків (кібер, ESG, модельний), нові методи їх оцінки (Big Data, AI, кліматичні stress-test) та інноваційні інструменти мінімізації (блокчейн, open banking). Банки, що вчасно адаптуються до цих змін, отримують більш стійку бізнес-модель і довіру стейкхолдерів.

Важливо підкреслити, що ризики у банківській сфері взаємопов’язані. Наприклад, прорахунки в моделі кредитного скорингу (модельний ризик) можуть призвести до зростання неповернень (кредитний ризик), що викличе відтік депозитів (ліквідні ризики) і приверне увагу регулятора (комплаєнс-ризик). Тому підхід до управління ризиками має бути цілісним і проактивним: виявляти проблеми на стику різних сфер, формувати резерви під всі суттєві ризики, а головне – формувати культуру усвідомлення ризиків на кожному рівні. Культура ризик-менеджменту означає, що рішення про нові продукти, стратегії чи технології приймаються з огляду на їх ризик-профіль і способи контролю.

Сучасні регуляторні вимоги (Базель IV, вимоги ЄС, настанови НБУ) задають високу планку – фактично, регулятори очікують, що банки зможуть вижити в умовах серйозних потрясінь. Але виконання цих вимог – в інтересах самих банків. Зрештою, стабільність банківської установи напряму залежить від того, наскільки добре вона розуміє та контролює свої ризики. Події останніх років – від пандемії до війни, від банківських крахів до кібератак – лише підтвердили мудрість цієї максими.

Отже, оновлена та розширена система управління банківськими ризиками – це живий механізм, що постійно вдосконалюється. Банки інвестують у нові технології, наймають кваліфікованих ризик-менеджерів, перебудовують процеси, аби передбачати майбутні загрози. Принцип “Risk Management first” стає визначальним у корпоративній стратегії банків: зростання і прибутковість тепер досягаються не шляхом надмірного ризику, а навпаки – через грамотне управління ризиками, що дозволяє рухатися вперед без потрясінь. Лише та фінансова установа, яка по-справжньому опанувала науку управління ризиками, може вважатися стійкою та сучасною в нинішньому фінансовому ландшафті.