

СТРЕС-ТЕСТУВАННЯ ЯК ІНСТРУМЕНТ КОРПОРАТИВНОГО УПРАВЛІННЯ У ВОЄННИЙ ПЕРІОД

У воєнний період стрес-тестування банківської діяльності набуває критичного значення, оскільки традиційні підходи до оцінювання стійкості часто не встигають за швидкістю зміни загроз і поведінки клієнтів [1-3]. Основна проблема полягає в тому, що стрес-тестування часто відбувається як формалізований розрахунок показників або разова «перевірки на відповідність», тоді як воєнне середовище вимагає управлінського інструмента, здатного оперативно перетворювати сигнали ризику на конкретні рішення.

За таких умов стрес-тестування в банківській установі доцільно трактувати не як формальну «процедуру перевірки», а як механізм корпоративного управління, що переводить невизначеність у відбір рішень на рівні Наглядової ради та Правління. В результаті банк отримує не «опис ризиків», а параметризований простір дій: які напрями фінансування доцільно підтримувати, які – тимчасово обмежувати, які ліміти коригувати, які процеси резервувати, а які – переводити у спрощений режим під пікові навантаження.

У системі корпоративного управління ключовим є управлінський фокус стрес-тестування, що полягає у необхідності ухвалювати рішення, закріплені у відповідальності, строках виконання та контрольних метриках.

Початковою ланкою цієї логіки виступає конструювання сценаріїв. У воєнних умовах банківська установа повинна мати сценарії конкретних управлінських ситуацій з чіткими межами прийнятності та визначеним набором важелів реагування. До таких ситуацій належать: локальний дефіцит ліквідності через хвилеподібну міграцію коштів між регіонами; раптова деградація якості портфеля у сегментах, пов'язаних із релокацією підприємств і розривом ланцюгів постачання; стрибок транзакційного навантаження на цифрові канали разом із інцидентом доступності; зміна умов операційної роботи через безпекові обмеження або перебої інфраструктури. Окремо слід виділяти «суто воєнні» сценарії, які прямо впливають на доступність сервісів і довіру клієнтів, зокрема кібератаки та DDoS-атаки. У таких сценаріях об'єктом управлінського рішення є не лише фінансові параметри, а й забезпечення безперервності критичних функцій: платежів, доступу до рахунків, підтверджень операцій, а також здатність банку швидко стабілізувати канали взаємодії з клієнтами.

Другим рівнем у корпоративному управлінні є визначення частоти проведення стрес-тестів. У воєнний період календарний підхід «раз на рік» є малоефективним, оскільки ризикові події мають високу динаміку та нерідко запускаються раптовими тригерами. Доцільною є двоконтурна частотність. Перший контур – регулярний (наприклад, квартальний), який обслуговує показники капіталу, ліквідності, якості портфеля та чутливості до зміни ставок і валютних параметрів. Другий – тригерний, що запускається поза графіком при появі операційних або поведінкових сигналів: нестандартні відтоки коштів, локальні збої платіжної інфраструктури, хвилі шахрайства, аномальне зростання запитів у мобільному застосунку, різка зміна структури транзакцій. Для воєнного середовища важливо, що тригерний контур має включати окремі «пускові умови» для кібератак і DDoS-атак (наприклад, нетипові патерни трафіку). Саме тригерний контур формує управлінську «нервову систему», оскільки змушує менеджмент переходити від констатації до дій у межах годин і діб: які ліміти активуються, які операції отримують пріоритет, які сервіси переводяться у спрощені режими, як і коли надається інформація клієнтам.

Третьою ланкою є визначення управлінського виходу стрес-тестування. Якщо результатом залишаються лише «індикатори стійкості», банк фактично втрачає сенс інструмента, оскільки не отримує рішення, придатні до виконання. Натомість управлінський вихід має бути оформлений як пакет рішень щодо операційної стійкості – резервування, дублювання, зміни SLA з провайдерами, розширення моніторингу інцидентів та контроль часу відновлення. Такий пакет доцільно затверджувати як дорожню карту, яка містить відповідальних, строки, контрольні точки та показники підтвердження виконання.

Практика українських банків свідчить, що управлінська природа стрес-тестування може проявлятися не лише у «класичних» макросценаріях, а й у поведінково-транзакційних та технологічних шоках, що демонструють межі масштабування цифрових контурів. Показовим прикладом є кейс monobank (як цифрового бренду Universal Bank) [1], так звана «лимонна лихоманка», тобто гейміфікована активність у застосунку, яка спричинила стрибкоподібне навантаження, хвилю звернень і помітні проблеми доступності сервісів. Управлінська значущість цього кейсу полягає в тому, що він фактично відтворив структуру «польового» стрес-тесту, де навантаження зростає не поступово, а хвилюю, одночасно збільшуючи кількість транзакційних запитів, частоту повторних спроб і загальну кількість взаємодій у застосунку. У таких умовах будь-яка деградація доступності породжує ефект самопідсилення: клієнти повторюють дії, трафік збільшується, сервісні канали перевантажуються, а це додатково погіршує показники часу відповіді та рівень успішності операцій. З позиції менеджменту та адміністрування

принциповим є те, що «лимонна лихоманка» виявляє не лише технічну межу пропускнуї спроможності, а й організаційну межу: готовність підтримки, узгодженість між командами, швидкість стабілізації, якість кризової комунікації. Таким чином, «цифровий шок» оголює управлінську залежність між продуктово-комунікаційними рішеннями та операційною витривалістю: кожна хвилина недоступності може конвертуватися у репутаційні втрати, зростання навантаження на контакт-центр, падіння довіри та потенційні витрати на компенсації.

Воєнний контекст підсилює значущість такого кейсу, оскільки подібні пікові навантаження можуть накладатися на кібератаки та DDoS-атаки. У цьому випадку банк стикається з комбінованим шоком: одночасно зростає частка нелегітимного трафіку, виникає конкуренція за ресурси між реальними клієнтськими запитами та атакувальним потоком, підвищується ймовірність часткової недоступності окремих функцій. Управлінський сенс таких сценаріїв полягає у перевірці здатності банку зберегти «ядро сервісу» - критичні платежі, доступ до рахунків, ключові підтвердження і одночасно швидко стабілізувати комунікаційні контури так, щоб мінімізувати повторні звернення та «панічні» повторні дії користувачів, які збільшують навантаження. Важливо, щоб реакції на кіберінциденти були формалізовані управлінськими рішеннями, а не лише технічними регламентами IT-підрозділів, і підлягали контролю на рівні профільних комітетів Наглядової ради банку.

Щоб перетворити подібні події на керований інструмент, банк має формалізувати управлінський протокол «навмисного навантажувального експерименту», який доцільно інтегрувати у контур корпоративного управління цифровими ризиками. По-перше, необхідно встановити порogi навантаження, після яких автоматично запускаються деградаційні режими: пріоритизація критичних операцій (платежі, доступ до рахунків), спрощення «важких» запитів, тимчасове обмеження неключових функцій. По-друге, слід зафіксувати порядок публічних повідомлень: що саме і в якій послідовності повідомляється клієнтам при збої, хто є уповноваженим голосом, які формулювання мінімізують паніку й повторні звернення. По-третє, підсумки таких тестів доцільно виносити на порядок денний профільного комітету Наглядової ради банку (цифрові ризики/операційна стійкість) як підставу для інвестицій у масштабування, резервування, посилення захисту та навчання сервісних команд. У результаті стрес-тестування перестає бути разовою «подією» і стає циклом управління: виявлення меж → рішення про ресурси та правила → контроль виконання → повторне тестування.

Отже, стрес-тестування у воєнний період має бути інституціоналізоване як управлінський контур корпоративного управління, який забезпечує прийняття рішень на основі сценаріїв, тригерів і вимірюваних порогів, а

також дозволяє банку підтримувати безперервність критичних сервісів під впливом пікових навантажень, кібератак і DDoS-атак.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Касіян В. «Не очікували такого». Акція з лимонами збільшила навантаження на моноу вісім разів. Інформаційний портал Ліга-нет. URL: <https://finance.liga.net/ua/bank/novosti/ne-ochikuvaly-takoho-aktsiia-z-lymonamy-zbilshyla-navantazhennia-na-mono-u-visim-raziv?>
2. Стрес-тестування банків як інструмент банківського регулювання. Національний банк України. 2023. URL: https://bank.gov.ua/admin_uploads/article/Stres-testuvannya_bankiv_19-05-2023.pdf.com.
3. Kloba L., Kloba T. Cyber threats of the banking sector in the conditions of the war in Ukraine. *Financial and credit activity: problems of theory and practice*. 2022. Vol. 5 (46). URL: <https://fkd.net.ua/index.php/fkd/article/view/3883>.