

**Роскладка Андрій Анатолійович**

Доктор економічних наук, професор, завідувач кафедри цифрової економіки та системного аналізу
Державний торговельно-економічний університет, Київ, Україна

ORCID: 0000-0002-1297-377X

a.roskladka@knute.edu.ua

Кузін Олег Миколайович

Аспірант кафедри цифрової економіки та системного аналізу

Державний торговельно-економічний університет, Київ, Україна

ORCID: 0009-0009-3592-0345

o.kuzin@knute.edu.ua

МОДЕЛЮВАННЯ ВІДМОВОСТІЙКОЇ КОНФІГУРАЦІЇ ІНФОРМАЦІЙНОГО СЕРЕДОВИЩА БАНКУ

Анотація. Нормативні вимоги до операційної стійкості фінансового сектору визначають кількісні показники готовності критичних банківських сервісів, однак традиційна перевірка планів відновлення за принципом «успішно/неуспішно» не дає статистично обґрунтованої відповіді на питання, чи справді розгорнута конфігурація ці показники забезпечує. Коефіцієнт покриття відмов, тобто ймовірність того, що відмову буде виявлено й автоматично оброблено без переривання сервісу, у розрахунках готовності постулюється, але не вимірюється. У статті запропоновано метод експериментальної перевірки відмовостійкої конфігурації інформаційного середовища банку, що ґрунтується на контрольованому внесенні відмов у робоче середовище та інтервальному оцінюванні результатів. Показано, що програму випробувань доцільно формувати як проєкцію моделей аналізу ризиків – ранжування видів відмов за пріоритетним числом ризику та переліку захисних бар'єрів дерев відмов і подій, – завдяки чому кожна серія перевіряє окрему кількісну гіпотезу про конкретний механізм захисту, а її результат уточнює відповідний параметр моделі готовності. Формалізовано схему контрольованого експерименту, придатну для промислового банківського середовища: метрику усталеного стану, операційні означення моментів виявлення, локалізації та завершення перемикавання, обмеження радіуса впливу пілотним контуром і критерій автоматичної дострокової зупинки. Методику статистичного опрацювання побудовано на довірчих інтервалах Вілсона та зведених оцінках для однотипних механізмів. Кількісно визначено потрібні обсяги випробувань і показано, що підтвердження покриття на рівні 0,99 потребує щонайменше 381 бездефектного прогону, що обґрунтовує автоматизацію внесення відмов. Метод апробовано на пілотному георозподіленому середовищі діючого банку: вісім серій загальним обсягом 261 прогін дали інтервальні оцінки покриття всіх ключових бар'єрів, виявили два приховані дефекти конфігурації, які не виводяться з аналітичних моделей, і показали, що ручне перемикавання на резервний майданчик з медіаною 42 хв не відповідає нормативу часу відновлення найкритичнішого класу сервісів.

Ключові слова: відмовостійкість; внесення відмов; довірчий інтервал Вілсона; інформаційне середовище банку; коефіцієнт покриття; контрольований експеримент; моделювання; тестування.

ВСТУП

Постановка проблеми. Регуляторні вимоги до операційної стійкості фінансового сектору – від регламенту DORA [1] до стандартів готовності інформаційно-комунікаційних технологій до безперервності діяльності [2] – установлюють кількісні цілі відновлення критичних сервісів і прямо вимагають регулярного тестування засобів стійкості. В умовах воєнного стану до компонентних відмов додалися майданчикові сценарії – знеструмлення, фізичні ураження, втрата центру опрацювання даних [3]. У відповідь банки розгортають резервні, дедалі частіше георозподілені конфігурації. Проте сам факт розгортання резерву не гарантує виконання нормативів. Поведінка складних резервних конфігурацій у



момент відмови систематично відрізняється від задокументованої, а суттєва частка простоїв спричиняється недосконалістю автоматики перемикання та прихованими дефектами конфігурації [4], [14].

Традиційна практика перевірки у формі щорічних навчань за планами відновлення дає відповідь лише у форматі «успішно/неуспішно» і не породжує статистично значущої кількості спостережень. Через це коефіцієнт покриття відмов, тобто ймовірність того, що відмову буде виявлено й автоматично оброблено без переривання сервісу, у розрахунках постулюється, але не вимірюється. Аналітичні моделі готовності оперують параметрами, для яких у банківській практиці немає процедури експериментального оцінювання з контрольованою статистичною достовірністю.

Аналіз останніх досліджень і публікацій. Термінологію відмов, помилок і відмовостійкості вжито в сенсі усталеної таксономії гарантоздатних обчислень [15]. Аналітичні моделі готовності систем із структурним резервуванням компонентів, зокрема марковські моделі з неідеальним покриттям відмов, викладено у [11] та розвинуто в українській науковій школі надійності. Технологію моделювання алгоритмів поведінки інформаційних систем, яка дає змогу будувати марковські моделі поведінки, запропоновано Б. Волочієм у [5], а засади оцінювання функціональної безпечності систем відповідального призначення – у дисертації Л. Озірковського [6]. Сучасні стратегії оцінювання готовності хмарних і розподілених середовищ, запропоновані В. Харченком, Ю. Поночовним, О. Іванченком та іншими [7], прямо передбачають збирання експлуатаційних даних про відмови для уточнення параметрів моделі. Проте значення коефіцієнта покриття відмов у таких моделях приймають як заздалегідь відоме, тому процедури його експериментального оцінювання в інформаційному середовищі банку досі не визначено.

Другий напрям – експериментальне оцінювання. Внесення відмов як інженерну практику систематизували К. Розенталь і Н. Джонс [4], [13], які унормували експерименти на робочих системах через гіпотезу усталеного стану (steady state), обмеження радіуса впливу та автоматичну зупинку. Утім, ці практики сформувалися в середовищі великих інтернет-сервісів, де допустимі експерименти на реальному трафіку, тому для банківського середовища з регуляторними обмеженнями їхнє безпосереднє перенесення неможливе, а опрацювання результатів у відповідних публікаціях здебільшого обмежується якісними висновками.

Третя складова – статистичний апарат оцінювання ймовірностей за обмеженими вибірками. Довірчий інтервал Вілсона дає коректні межі навіть за малих обсягів вимірювань і граничних результатів, коли всі прогони серії успішні; порівняльний аналіз інтервалів для біноміальної частки наведено у [12], а властивості інтервалу Вілсона докладно дослідив Б. О'Ніл [8]. У попередніх роботах авторів проаналізовано групи еквівалентності методів резервного копіювання [9] та побудовано систему моніторингу банківської інфраструктури [10], метрики якої використано як вимірювач усталеного стану.

Метою статті є розроблення та апробація методу експериментальної перевірки відмовостійкої конфігурації інформаційного середовища банку, який дає статистично обґрунтовані інтервальні оцінки коефіцієнта покриття відмов за реалістичних обсягів випробувань. Завданнями дослідження є такі: сформулювати принципи формування програми випробувань за результатами аналізу ризиків; формалізувати схему контрольованого експерименту, придатну для промислового банківського середовища; визначити методику вимірювань та інтервального оцінювання коефіцієнтів покриття; апробувати запропонований метод на пілотному середовищі діючого банку.

МЕТОДИКА ДОСЛІДЖЕННЯ

1. Формування програми випробувань за результатами аналізу ризиків

Вихідним положенням методу експериментальної перевірки відмовостійкої конфігурації інформаційного середовища банку є вимога, щоб програма випробувань була проєкцією моделей аналізу ризиків. Перше джерело – ранжування видів відмов за пріоритетним числом ризику з аналізу видів і наслідків відмов (FMEA). При цьому до програми включають ті види відмов, які мають найбільші значення ризику і для яких передбачені автоматичні механізми захисту. Друге джерело – перелік захисних бар'єрів дерев відмов і подій. Кожному бар'єру, ймовірність спрацювання якого входить до моделі готовності, має відповідати щонайменше одна серія випробувань. Так кожна серія перевіряє окрему кількісну гіпотезу, а її результат уточнює відповідний параметр моделі.

Кожній серії ставить у відповідність четвертка «вид відмови – спосіб внесення – перевірюваний бар'єр – обсяг серії». Принциповим є поділ серій за режимом виконання. Відмови компонентів вносяться у планових віках обслуговування на пілотному контурі із синтетичним навантаженням, а сценарії втрати майданчика відпрацьовуються у форматі планових навчань. Такий поділ зберігає ключову ідею хаос-інженерії – експеримент над реальною конфігурацією, а не над її моделлю [4].

2. Схема контрольованого експерименту

Кожен прогін організовано за схемою контрольованого експерименту з п'яти елементів.

- *Метрика усталеного стану* відображає працездатність цільового сервісу з погляду клієнта. В апробації використано частку успішних синтетичних транзакцій дистанційного банківського обслуговування за вікно 60 с з допустимим значенням не нижче 97 %.
- *Кількісна гіпотеза*: після внесення відмови метрика не виходить за межі допустимого інтервалу довше, ніж на нормативний час відновлення відповідного класу сервісів.
- *Обмеження радіуса впливу*: експеримент виконується на пілотному контурі, ізольованому від промислових операцій.
- *Критерій дострокової зупинки*: падіння метрики нижче 90 % понад 120 с автоматично скасовує ін'єкцію.
- *Повна фіксація конфігурації* забезпечує відтворюваність прогонів.

Хронограму прогону подано на рис. 1. Моменти подій означено операційно: момент внесення відмови t_0 – мітка часу ін'єкції; момент виявлення t_d – перша невдала активна перевірка або тривога відповідного рівня; момент завершення локалізації t_l – ідентифікація відмовного елемента засобами моніторингу; момент завершення перемикавання t_k – повернення метрики до допустимого інтервалу. Різниці цих моментів утворюють вимірювані складові часу відновлення T_d , T_l та $T_{пер}$, які фіксують журнали моніторингу з роздільністю 1 с за синхронізованими годинниками.

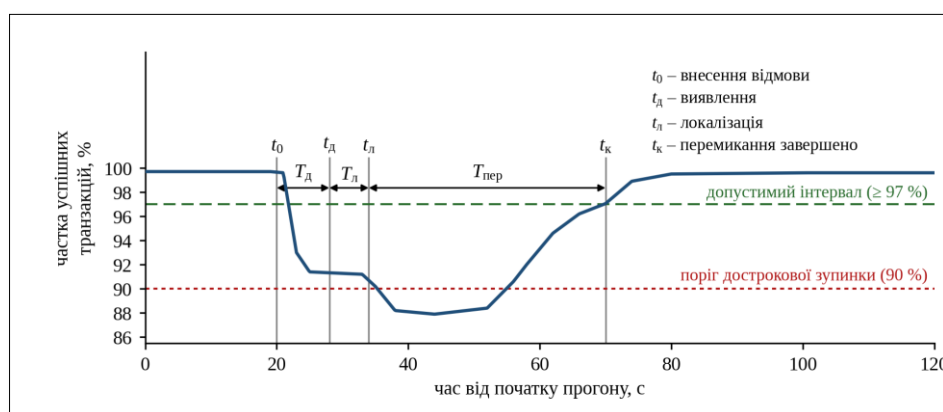


Рис. 1. Хронограма контрольованого експерименту у вигляді метрики усталеного стану та вимірюваних складових часу відновлення
Джерело: побудовано авторами

3. Методика статистичного оцінювання результатів

Результатом прогону є бінарний наслідок (автоматика або обробила відмову в межах гіпотези, або ні) та вектор вимірюваних тривалостей. Для серії з n прогонів, з яких k успішні, точкова оцінка коефіцієнта покриття відмов становить

$$\hat{c} = \frac{k}{n}, \quad (1)$$

однак за реалістичних обсягів серій точкова оцінка малоінформативна, і головним результатом слугує 95-відсотковий довірчий інтервал Вілсона [8]:

$$c_{1,2} = \frac{\hat{c} + \frac{z^2}{2n} \pm z \sqrt{\frac{\hat{c}(1-\hat{c})}{n} + \frac{z^2}{4n^2}}}{1 + \frac{z^2}{n}}, \quad (2)$$

де z – квантиль стандартного нормального розподілу рівня $1 - \alpha/2$ (для 95 % інтервалу $z = 1,96$). На відміну від нормального наближення, інтервал (2) зберігає коректність за малих n та граничних результатів $k = n$, типових для випробувань справної автоматики. Для видів відмов, що перевіряють один механізм на різних компонентах, обчислюється зведена оцінка

$$\hat{c}_{звед} = \frac{\sum_j k_j}{\sum_j n_j}, \quad (3)$$

де k_j та n_j – кількість успішних і загальна кількість прогонів у j -й серії.

Формула (2) дає й відповідь на питання про необхідні обсяги випробувань. За бездефектної серії ($k = n$) дисперсійний доданок у (2) дорівнює нулю, і вираз спрощується до $c_1 = n/(n + z^2)$, тому умова $c_1 \geq c$ набуває вигляду $n \geq z^2 c / (1 - c)$. Для $c = 0,99$ і $z = 1,96$ це дає $n \geq 380,3$, тобто щонайменше 381 бездефектний прогін. Розраховані за цим співвідношенням нижні межі інтервалу наведено в табл. 1. Звідси випливають



два висновки. Ручні навчання принципово не можуть обґрунтувати високі значення покриття, тому внесення відмов має бути автоматизованим, а до накопичення достатньої статистики моделі готовності мають використовувати інтервальні оцінки.

Таблиця 1

Нижня межа 95 % довірчого інтервалу Вілсона залежно від обсягу серії

Обсяг серії n	25	50	100	200	381
Нижня межа за $k = n$	0,867	0,929	0,963	0,981	0,990
Нижня межа за $k = n - 1$	0,805	0,895	0,946	0,972	0,985

Джерело: розраховано авторами за формулою (2)

РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

4. Апробація методу на пілотному середовищі

Метод апробовано на пілотному георозподіленому середовищі діючого банку. Воно охоплює два майданчики з незалежним живленням і подвійними каналами зв'язку, дубльовані контури віртуалізації та балансування, кластер СУБД із синхронною реплікацією і резервне копіювання з ізольованим доменом керування. Метрика синтетичних транзакцій моніторингу [10] водночас слугує вимірювачем усталеного стану. Програму склали вісім серій E1–E8 обсягом 261 прогін (табл. 2). E1–E7 виконувались у планових вікнах на пілотному контурі із навантаженням близько 70 % пікового, E8 – у форматі щоквартальних навчань. Механізм відновлення з резервної копії, перевірюваний у E7, належить до групи еквівалентності, визначеної в [9].

Таблиця 2

Вибірка та інтервальні оцінки коефіцієнта покриття за серіями E1–E8

Серія	Внесена відмова або подія	n	k	$\hat{c}$ за (1)	95 % ДІ Вілсона за (2)
E1	Відмова активного вузла СУБД	25	24	0,960	[0,805; 0,993]
E2	Відмова вузла віртуалізації	30	29	0,967	[0,833; 0,994]
E3	Відмова зовнішнього каналу	40	40	1,000	[0,912; 1,000]
E4	Відмова балансувальника	40	39	0,975	[0,871; 0,996]
E5	Відмова шляху до сховища	20	19	0,950	[0,764; 0,991]
E6	Відмова сервера застосунків	50	48	0,960	[0,865; 0,989]
E7	Верифікація придатності резервної копії	52	51	0,981	[0,899; 0,997]
E8	Знеструмлення основного майданчика	4	4	1,000	[0,510; 1,000]
Разом	Уся вибірка	261	254	0,973	[0,946; 0,987]

Джерело: складено авторами за результатами випробувань

Приклад розрахунку. На серії E1 з $n = 25$ прогонів успішними були $k = 24$, тобто $\hat{c} = 0,960$. Підстановка у (2) за $z = 1,96$ дає

$$c_{1,2} = \frac{0,960 + 0,0768 \pm 1,96 \cdot \sqrt{0,00154 + 0,00154}}{1,1537} = [0,805; 0,993]$$

за ширини інтервалу 0,188. Нормальне наближення дало б [0,883; 1,037] – з верхньою межею поза областю визначення ймовірності, що й пояснює вибір інтервалу Вілсона. Решту рядків табл. 2 обчислено за такою самою схемою.

Зведення однотипних серій. Серії E3 і E4 перевіряють один бар'єр – автоматичне виведення несправного елемента з активного шляху обслуговування, – тому їх зведено за (3). Для цієї пари $k = 79$ із $n = 80$, звідки $\hat{c}_{\text{звед}} = 0,988$ і, за (2), інтервал [0,933; 0,998]. Зведення підняло нижню межу з 0,912 (E3) і 0,871 (E4) до 0,933, тобто дало точність, недосяжну для кожної серії окремо за того самого сукупного обсягу випробувань.

Точкові оцінки коефіцієнтів покриття та довірчі інтервали (2) подано в табл. 2, а графічно – на рис. 2. Вони лежать у діапазоні 0,95–1,00, проте в жодній серії нижня межа не досягає значення 0,99, яке типово закладають в апіорні моделі систем із резервуванням. Для E1 вона становить 0,805, а для E8 – 0,510. Це не свідчить про низьку якість автоматики, а є об'єктивною ціною реалістичних обсягів серій.

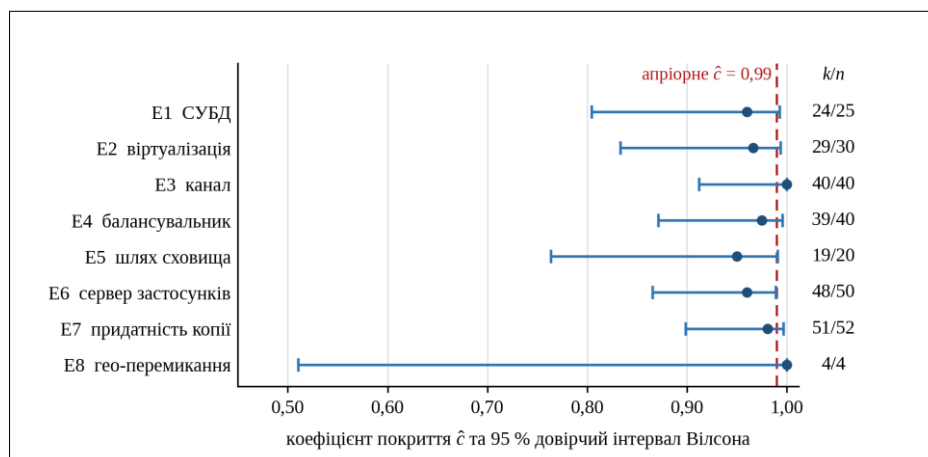


Рис. 2. Оцінки коефіцієнтів покриття за серіями E1–E8 з 95 % довірчими інтервалами Вілсона (праворуч – кількість успішних прогонів до загальної)

Джерело: побудовано авторами за даними табл. 2

Окрему цінність мають невдалі прогони. Єдиний невдалий прогін E1 стався за пікового навантаження, коли перемикавання не відбулось у відведений тайм-аут, і кластер завершив його лише після ручного підтвердження. При цьому аналіз виявив дефект конфігурації таймерів, який не проявлявся за штатних умов. Два невдалі прогони E6 виявили вичерпання черги з'єднань балансувальника в момент виведення вузла з пулу. Обидва дефекти належать до прихованих помилок конфігурації, які не виводяться з аналітичних моделей [4].

Серія E8 ілюструє межі ручних навчань, де за чотирьох успішних навчань інтервал [0,510; 1,000] практично неінформативний. Водночас вимірний медіанний час перемикавання на резервний майданчик у 42 хв сам собою є значущим результатом. Він більш ніж утричі перевищує цільовий час відновлення найкритичнішого класу сервісів за внутрішніми нормативами, тому автоматизацію цієї процедури визначено першочерговим напрямом розвитку.

ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

У статті розроблено метод експериментальної перевірки відмовостійкої конфігурації інформаційного середовища банку. Програма випробувань формується в ньому як проєкція моделей аналізу ризиків. Кожному захисному бар'єру, ймовірність спрацювання якого входить до моделі готовності, відповідає окрема серія контрольованих експериментів з кількісною гіпотезою, що усуває довільність вибору сценаріїв.

Формалізовано схему контрольованого експерименту, придатну для промислового банківського середовища. Вона охоплює метрику усталеного стану, операційні означення моментів виявлення, локалізації та завершення перемикавання, обмеження радіуса впливу пілотним контуром і критерій автоматичної зупинки. Методику статистичного опрацювання побудовано на інтервалах Вілсона – точковій оцінці (1), довірчому інтервалі (2) та зведеній оцінці (3). Показано, що підтвердження покриття на рівні 0,99 потребує щонайменше 381 бездефектного прогону, а зведення серій E3 і E4 підняло нижню межу інтервалу до 0,933 без додаткових випробувань.

Метод апробовано на пілотному георозподіленому середовищі діючого банку. Вісім серій обсягом 261 прогін дали інтервальні оцінки покриття всіх ключових бар'єрів з точковими оцінками 0,95–1,00 і нижніми межами 0,51–0,91. Випробування виявили два приховані дефекти конфігурації та показали, що ручне перемикавання на резервний майданчик з медіаною 42 хв не відповідає нормативу часу відновлення.

Перспективи подальших досліджень охоплюють автоматизацію внесення відмов з накопиченням вибірки між релізами, повторну серію перемикавання на резервний майданчик достатнього обсягу, застосування послідовних статистичних процедур та поширення методу на платіжний контур банку.



СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector (DORA). (2022). *Official Journal of the European Union*, L 333, 1–79.
2. International Organization for Standardization. (2025). *ISO/IEC 27031:2025. Information and communication technology readiness for business continuity* (2nd ed.).
3. Національний банк України. (б. д.). *Power Banking: спільна мережа банківських відділень, які працюють в умовах знееструмлення*. <https://power.bank.gov.ua>
4. Rosenthal, C., & Jones, N. (2020). *Chaos engineering: System resiliency in practice*. O'Reilly Media.
5. Волочій, Б. Ю. (2004). *Технологія моделювання алгоритмів поведінки інформаційних систем*. Вид-во Національного університету «Львівська політехніка».
6. Озірковський, Л. Д. (2020). *Розвиток теоретичних засад оцінювання показників функціональної безпечності радіоелектронних систем відповідального призначення* [Дисертація доктора технічних наук, Національний університет «Львівська політехніка»].
7. Kharchenko, V., Ponochovnyi, Y., Ivanchenko, O., Fesenko, H., & Illiashenko, O. (2022). Combining Markov and semi-Markov modelling for assessing availability and cybersecurity of cloud and IoT systems. *Cryptography*, 6(3), Article 44. <https://doi.org/10.3390/cryptography6030044>
8. O'Neill, B. (2021). *Mathematical properties and finite-population correction for the Wilson score interval*. arXiv. <https://doi.org/10.48550/arXiv.2109.12464>
9. Roskladka, A., & Kuzin, O. (2023). Analysis of equivalence groups in data backup methods of the banking information environment. In *Information Technologies and Innovations (IT&I-2023)* (pp. 254–256).
10. Кузін, О. М. (2024). Система моніторингу банківської інфраструктури. *Смарт технології: промислова та цивільна інженерія*, 2(15), 119–123.
11. Trivedi, K. S. (2002). *Probability and statistics with reliability, queuing, and computer science applications* (2nd ed.). John Wiley & Sons.
12. Brown, L. D., Cai, T. T., & DasGupta, A. (2001). Interval estimation for a binomial proportion. *Statistical Science*, 16(2), 101–133.
13. Basiri, A., Behnam, N., de Rooij, R., Hochstein, L., Kosewski, L., Reynolds, J., & Rosenthal, C. (2016). Chaos engineering. *IEEE Software*, 33(3), 35–41.
14. Oppenheimer, D., Ganapathi, A., & Patterson, D. A. (2003). Why do Internet services fail, and what can be done about it? In *Proceedings of the 4th USENIX Symposium on Internet Technologies and Systems*. USENIX Association.
15. Avizienis, A., Laprie, J.-C., Randell, B., & Landwehr, C. (2004). Basic concepts and taxonomy of dependable and secure computing. *IEEE Transactions on Dependable and Secure Computing*, 1(1), 11–33.

**Andrii Roskladka**

Doctor of Sciences in Economics, PhD in Applied Mathematics, Professor,
Head of the Digital Economy and System Analysis Department,
State University of Trade and Economics, Kyiv, Ukraine
ORCID: 0000-0002-1297-377X
a.roskladka@knute.edu.ua

Oleh Kuzin

PhD student of the Department of Digital Economy and System Analysis
State University of Trade and Economics, Kyiv, Ukraine
ORCID: 0009-0009-3592-0345
o.kuzin@knute.edu.ua

MODELLING A FAULT-TOLERANT CONFIGURATION OF A BANK INFORMATION ENVIRONMENT

Abstract. Regulatory requirements for the operational resilience of the financial sector define quantitative availability targets for critical banking services; however, the traditional pass/fail verification of disaster-recovery plans provides no statistically grounded answer to the question of whether a deployed configuration actually meets these targets. The failure coverage factor, that is, the probability that a failure is detected and handled automatically without interrupting the service, is postulated rather than measured in availability calculations. The paper proposes a method for experimental verification of a fault-tolerant configuration of a bank information environment, based on controlled fault injection into the production-grade environment combined with interval estimation of the results. It is shown that the test programme should be derived as a projection of the risk-analysis models, namely the ranking of failure modes by their risk priority numbers and the list of protective barriers of fault and event trees, so that every experiment series tests a separate quantitative hypothesis about a specific protection mechanism and its outcome refines the corresponding parameter of the availability model. A controlled-experiment scheme suitable for an industrial banking environment is formalized: a steady-state metric, operational definitions of the detection, localization and switchover completion instants, blast-radius confinement to a pilot circuit, and an automatic abort criterion. The statistical processing rests on Wilson confidence intervals and on pooled estimates for identical mechanisms tested on different components; the required sample sizes are quantified, showing that at least 381 defect-free runs are needed to confirm coverage of 0.99, which justifies the automation of fault injection. The method was validated on a pilot geo-distributed environment of an operating bank: eight series totalling 261 runs produced interval estimates of coverage for all key barriers, revealed two latent configuration defects that cannot be derived from analytical models, and demonstrated that manual switchover to the backup site, with a median of 42 minutes, violates the recovery-time objective of the most critical service class.

Keywords: fault tolerance; fault injection; Wilson confidence interval; bank information environment; coverage factor; controlled experiment; modelling; testing.

REFERENCES (TRANSLATED AND TRANSLITERATED)

1. Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector (DORA). (2022). *Official Journal of the European Union*, L 333, 1–79.
2. International Organization for Standardization. (2025). *ISO/IEC 27031:2025. Information and communication technology readiness for business continuity* (2nd ed.).
3. National Bank of Ukraine. (n.d.). *Power Banking: Spilna mrezhka bankivskykh viddilen, yaki pratsiuiut v umovakh znestrumlennia* [Power Banking: A joint network of bank branches operating under power outages]. <https://power.bank.gov.ua> [in Ukrainian].
4. Rosenthal, C., & Jones, N. (2020). *Chaos engineering: System resiliency in practice*. O'Reilly Media.
5. Volochii, B. Yu. (2004). *Tekhnolohiia modeliuvannia alhorytmiv povedinky informatsiinykh system* [Technology of modelling the behaviour algorithms of information systems]. Lviv Polytechnic National University Publishing House [in Ukrainian].



6. Ozirkovskyi, L. D. (2020). *Rozvytok teoretychnykh zasad otsiniuvannia pokaznykiv funktsionalnoi bezpechnosti radioelektronnykh system vidpovidalnoho pryznachennia* [Development of the theoretical foundations for assessing functional safety indicators of mission-critical radio electronic systems] [Doctoral dissertation, Lviv Polytechnic National University] [in Ukrainian].
7. Kharchenko, V., Ponochovnyi, Y., Ivanchenko, O., Fesenko, H., & Illiashenko, O. (2022). Combining Markov and semi-Markov modelling for assessing availability and cybersecurity of cloud and IoT systems. *Cryptography*, 6(3), Article 44. <https://doi.org/10.3390/cryptography6030044>
8. O'Neill, B. (2021). *Mathematical properties and finite-population correction for the Wilson score interval*. arXiv. <https://doi.org/10.48550/arXiv.2109.12464>
9. Roskladka, A., & Kuzin, O. (2023). Analysis of equivalence groups in data backup methods of the banking information environment. In *Information Technologies and Innovations (IT&I-2023)* (pp. 254–256).
10. Kuzin, O. M. (2024). Systema monitorynhu bankivskoi infrastruktury [Monitoring system of the banking infrastructure]. *Smart Technologies: Industrial and Civil Engineering*, 2(15), 119–123 [in Ukrainian].
11. Trivedi, K. S. (2002). *Probability and statistics with reliability, queuing, and computer science applications* (2nd ed.). John Wiley & Sons.
12. Brown, L. D., Cai, T. T., & DasGupta, A. (2001). Interval estimation for a binomial proportion. *Statistical Science*, 16(2), 101–133.
13. Basiri, A., Behnam, N., de Rooij, R., Hochstein, L., Kosewski, L., Reynolds, J., & Rosenthal, C. (2016). Chaos engineering. *IEEE Software*, 33(3), 35–41.
14. Oppenheimer, D., Ganapathi, A., & Patterson, D. A. (2003). Why do Internet services fail, and what can be done about it? In *Proceedings of the 4th USENIX Symposium on Internet Technologies and Systems*. USENIX Association.
15. Avizienis, A., Laprie, J.-C., Randell, B., & Landwehr, C. (2004). Basic concepts and taxonomy of dependable and secure computing. *IEEE Transactions on Dependable and Secure Computing*, 1(1), 11–33.

Отримано редакцією журналу / Received: 30.06.26

Прорецензовано / Revised: 15.07.26

Схвалено до друку / Accepted: 26.10.26



This work is licensed under Creative Commons Attribution-noncommercial-sharealike 4.0 International License.