Система моніторингу банківської інфраструктури

Олег Кузін[1]

[1]Державний торговельно-економічний університет
Україна, 02156, м. Київ, вул. Кіото, 19
[1]o.kuzin@knute.edu.ua, orcid.org/0009-0009-3592-0345

Received 17.09.2024, accepted 30.10.2024
https://doi.org/10.32347/uwt.2024.15.1801

Анотація. У сучасних умовах цифрової трансформації фінансового сектору стабільність і безперебійна робота банківської інфраструктури є запорукою успіху. Відмовостійкість комп'ютерних систем є одним із ключових факторів успішної роботи сучасних організацій, особливо в таких критичних галузях, як банківська сфера. Забезпечення постійної доступності банківських сервісів є вкрай важливим для безперебійної роботи платіжних систем, обробки транзакцій і доступу до рахунків клієнтів. Одним з основних інструментів для підтримки відмовостійкості є моніторинг показників систем, який дозволяє виявляти проблеми до того, як вони стають критичними, та вживати заходи для запобігання збоям.

У цій роботі розглянуто систему моніторингу інформаційного середовища банку, проведено аналіз ключових показників забезпечення відмовостійкої роботи системи. Окремо розглянуто такі особливості як критичність досліджуваних параметрів, частота опитування підсистем, часова чутливість та порогові значення.

В рамках дослідження виділено стабільні і аномальні значення параметрів об'єктів моніторингу і на їх основі сформовані шаблони поведінки системи. Як результат, визначені рівні ескалації, методи сповіщень та застосування додаткових автоматизацій для стабілізації роботи підсистем.

Ключові слова: Відмовостійкість, інформаційне середовище, система моніторингу, моделювання.

Олег Кузін
аспірант кафедри цифрової економіки та системного аналізу

МЕТА ТА МЕТОДИ ДОСЛІДЖЕННЯ

Метою цього дослідження є моніторинг банківської системи щодо покращення працездатності інфраструктури в умовах потенційних загроз під час військової агресії.

Під час дослідження використовувалися методи системного аналізу та комплексного аналізу.

ВСТУП

Умови роботи банківської системи України суттєво змінилися з початком повномасштабного вторгнення російської федерації, коли критичні інфраструктури опинилися під постійною загрозою фізичних пошкоджень, кібератак та регулярних збоїв в енергопостачанні [3]. Відключення електроенергії, перебої з інтернет-зв'язком і атаки на цифрові ресурси стали постійними викликами для банківської інфраструктури, яка відіграє важливу роль у фінансовій стабільності країни [4]. У таких умовах надзвичайно важливим стає безперервний контроль за станом IT-систем банків, де навіть короткочасний збій може призвести до великих втрат та порушення роботи критичних сервісів, таких як платежі, банкомати, обслуговування рахунків [5]. Саме системи моніторингу відіграють ключову роль у забезпеченні стабільної роботи інфраструктури банків під час кризових ситуацій, дозволяючи вчасно виявляти загрози та запобігати відмовам. Ефективний моніторинг не тільки допомагає швидко реагувати на несправності, а й прогнозувати потенційні ризики, що особливо

важливо в умовах, коли від стабільної роботи банків залежить економічна та соціальна стабільність країни.

Відмовостійкість — це здатність системи функціонувати навіть у випадку відмови одного або кількох компонентів. У банківських системах це означає безперервну роботу банкоматів, інтернет-банкінгу, процесингу карткових платежів та інших важливих операцій навіть під час технічних проблем. Для цього необхідно впровадити механізми резервування, автоматичної заміни несправних компонентів і ефективного моніторингу.

РЕЗУЛЬТАТИ ДОСЛІДЖЕНЬ

Моніторинг показників систем допомагає вчасно виявляти потенційні проблеми і попереджати збої. Системи моніторингу, дозволяють збирати дані про стан серверів, мереж, баз даних та інших компонентів IT-інфраструктури, а також забезпечують інструменти для аналізу та побудови прогнозів.

Основні функції моніторингу:

- **Виявлення проблем на ранніх стадіях.** Моніторинг дозволяє виявляти проблеми до того, як вони перетворяться на критичні збої, що впливають на роботу системи.
- **Прогнозування відмов.** На основі історичних даних можна побудувати прогнози і визначити, коли певний компонент системи може вийти з ладу.
- **Автоматизація процесів реагування**. За допомогою тригерів можна налаштувати автоматичне сповіщення або навіть автоматичне переключення на резервне обладнання у випадку виявлення критичних проблем.

Основні показники моніторингу

Щоб забезпечити відмовостійкість, важливо відстежувати ряд ключових показників системи. Основні з них включають:

- Завантаження процесора (CPU Load):

Високе завантаження процесора може призвести до перевантаження і збою у роботі серверів. Системи моніторингу дозволяють відслідковувати рівень завантаження і вчасно попереджати про критичні ситуації. Аналізуючи історичні дані, можна спрогнозувати сповільнення роботи підсистем внаслідок перевантаження і вчасно вжити заходів для підвищення продуктивності. Найбільше процесорне навантаження відбувається в робочі дні з 09:00 до 18:00 (Рис.1) і саме аналіз цих часових проміжків дозволяє робити висновки і прогнози завантаження і швидкодії бізнес-застосунків.

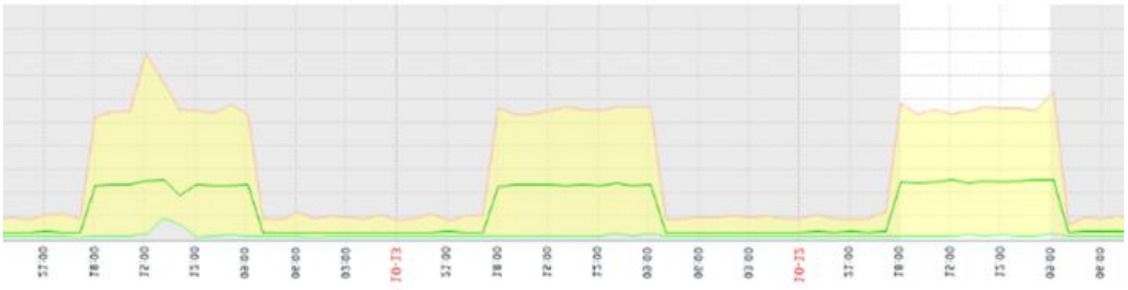

Рис. 1. Завантаження процесора в бізнес-час

Fig. 1. Processor load during business hours

Використання оперативної пам’яті (RAM Usage):

Надмірне використання оперативної пам’яті може призвести до уповільнення або відмови системи. Моніторинг використання пам’яті дозволяє оптимізувати ресурси і запобігати відмовам. Аналіз графіків використання оперативної пам’яті дозволяє виявити години навантаження серверних застосунків, виявити складні для обладнання часові рамки і виявити тенденції завантаження серверних застосунків, щоб уникнути перевантаження та витоків пам’яті.

- Вільне місце на диску (Disk Space Usage):

Моніторинг вільного місця на диску є одним із найважливіших елементів для забезпечення стабільної роботи IT-систем,

де зберігаються великі обсяги даних, зокрема бази даних, транзакційна інформація, журнали подій та інші критичні файли. Аналіз використання дискового простору кожної підсистеми дозволяє встановити порогові значення, при перевищенні яких потрібно вживати дій по очищенню дискового простору, або планувати покупку дискових накопичувачів, згідно тенденції використання, як зазначено на Рис.2. Окремої уваги потребує моніторинг вільного дискового простору в системних областях, при переповненні яких виникають проблеми не просто із застосунками, а і з операційною системою.

Рис. 2. Прогнозування покупки дискових накопичувачів згідно тенденції використання
Fig. 2. Forecasting disk drive purchases according to usage trends

- Мережеві показники:

Пропускна здатність (Network Bandwidth) і затримки (Latency) — ці параметри визначають ефективність передачі даних і швидкість доступу до системи [7]. Мережеві ресурси використовуються для обробки транзакцій, обміну даними між офісами, клієнтськими запитами до інтернет-банкінгу, підтримки систем електронної пошти та інтеграції з платіжними системами. Моніторинг пропускної здатності мережі допомагає вчасно виявляти потенційні проблеми, попереджувати їх і забезпечувати стабільну роботу мережевої інфраструктури. Аналіз історичних даних системи моніторингу мережі дозволяє визначити пікові періоди використання мережі протягом бізнес-часу та поза ним. Ці показники дають можливість спрогнозувати навантаження мережевої інфраструктури, виявити окремі «пляшкові горла» трафіку, на яких виникають затримки, виявити аномалії (Рис.3) і попередити витоки інформації [1]. Постійний моніторинг пропускної здатності мережі і її окремих вузлів допомагає у прийнятті рішень про масштабування підсистем і модернізацію мережі для досягнення необхідних швидкостей передачі даних.

Рис. 3. Аномальне споживання трафіку системою при оновленні версії серверної компоненти
Fig. 3. Abnormal traffic consumption by the system when updating the version of the server component

- Температура обладнання:

Перегрів серверів, мережевого обладнання чи систем зберігання даних може призвести до серйозних збоїв, пошкодження компонентів або втрати інформації. Своєчасне виявлення підвищених температур дозволяє вжити заходів для охолодження або оптимізації навантаження, що знижує ризик відмов системи. Ефективний моніторинг допомагає підтримувати обладнання в межах рекомендованих температурних параметрів, продовжуючи його термін служби. Таким чином, аналізуючи графіки коливання температур обладнання, можна виявити несприятливі тенденції і вчасно вжити заходів з дотримання оптимальних температурних режимів серверної кімнати, створити автоматизації по увімкненню додаткових систем кондиціонування при

невеликому перевищенні температур, як показує графік на Рис.4, або прийняти рішення [2] по активації системи пожежогасіння при критичному перевищенні температури.

Рис. 4. Впровадження додаткової системи охолодження
Fig. 4. Implementation of an additional cooling system

ПРОГНОЗУВАННЯ ВІДМОВ

Окрім виявлення проблем у реальному часі, системи моніторингу допомагають у прогнозуванні можливих відмов. Наприклад, якщо система моніторингу збирає дані про зростання завантаження серверів протягом кількох місяців, це може свідчити про наближення критичного навантаження, і керівництво банку може ухвалити рішення про модернізацію обладнання або розширення ресурсів.

АВТОМАТИЗАЦІЇ ТА СПОВІЩЕННЯ

Сповіщення від системи моніторингу є критично важливими для своєчасного реагування на проблеми в банківській інфраструктурі, дозволяючи оперативно усувати збої до того, як вони стануть критичними [8]. Важливим критерієм є правильне налаштування порогових значень, коли система має генерувати сповіщення – це дозволяє уникнути як надмірної кількості "шуму", так і пропуску серйозних інцидентів. Система повинна враховувати не лише поточний стан компонентів, але й тривалість аномалій, щоб запобігти реакції на тимчасові сплески навантаження. Ескалація оповіщень залежно від рівня критичності дозволяє залучати потрібних фахівців у випадку серйозних відмов. Нарешті, важливою є інтеграція сповіщень з автоматизованими процесами реагування, щоб забезпечити мінімальний час простою в разі критичних подій.

Автоматизація є важливою частиною процесу забезпечення відмовостійкості [6]. Системи моніторингу можуть автоматично генерувати сповіщення, створювати резервні копії даних або ініціювати переключення на резервні сервери без участі людини, особливо в в умовах, коли час на реакцію обмежений, а швидкість відновлення роботи системи є критичним фактором.

Консолідація даних моніторингу.
Консолідована панель (Дашборд) є зручним інструментом для візуалізації основних показників моніторингу в реальному часі, що дозволяє швидко оцінювати стан всієї IT-інфраструктури. Вона об'єднує на одному екрані критичні метрики і надає можливість оперативно відстежувати потенційні проблеми (Рис.5). Графіки та індикатори допомагають легко виявляти відхилення від нормальних значень і прогнозувати можливі збої. Дашборд також дозволяє налаштовувати рівні попереджень і сповіщень для кожного з показників, забезпечуючи швидкий доступ до критичної інформації для своєчасного реагування і підтримки відмовостійкості та ефективного управління IT-інфраструктурою.

Рис. 5 Приклад консолідованої панелі моніторингу ключових показників
Fig. 5. Example of a consolidated key performance indicator dashboard

ВИСНОВОК

Система моніторингу банківської інфраструктури відіграє ключову роль у забезпеченні її стабільної та відмовостійкої роботи, особливо в умовах воєнного стану та постійних технічних викликів.

Використання інструментів моніторингу дозволяє не тільки виявляти проблеми на ранніх етапах, але й прогнозувати потенційні загрози для всіх критичних компонентів системи. Завдяки постійному контролю за ключовими показниками, такими як завантаження процесора, використання оперативної пам'яті, стан мережевих ресурсів та температура обладнання, можна запобігти серйозним збоям і забезпечити безперебійну роботу банківських сервісів. Крім того, впровадження автоматизацій та оповіщень значно підвищує ефективність управління інфраструктурою, дозволяючи швидко реагувати на зміни та забезпечувати її надійність. Таким чином, системи моніторингу є невід'ємним інструментом для підтримки безпеки і стабільності банківської інфраструктури в умовах сучасних викликів.

REFERENCES

1. **Khlaponin, Y., Kozubtsova, L., Kozubtsov, I., & Shtonda, R.** (2022). Funktsiyi systemy zakhystu informatsiyi i kiberbezpeky krytychnoyi informatsiynoyi infrastruktury. *Elektronne fakhove nau-kove vydannya «Kiberbezpeka: osvita, nauka, tekhnika»*, 3(15), 124–134. https://doi.org/10.28925/2663-4023.2022.15.1241341
2. **Humennyy, D., Kuzin, O., & Shabala, YE.** (2024). Radarnyy zakhyst ta aktyvne perekhoplennya droniv-kamikadze. Pidvodni Tehnologii, 1(14), 98–106. https://doi.org/10.32347/uwt.2024.14.1301.
3. **Nastasyak, R. V., and O. O. Perepolkina.** Funktsionuvannya bankivs′koyi systemy ukrayiny v umovakh voyennoho stanu. Or-hanizatsiynyy komitet konferentsiyi: 234.
4. Postanova Pravlinnya Natsional′noho banku Ukrayiny «Pro robotu bankivs′koyi systemy v period zaprovadzhennya voyennoho stanu» vid 24.02.2022 № 18. URL: https://zakon.rada.gov.ua/laws/show/v0018500-22#Text.
5. Metodychni vkazivky z inspektuvannya bankiv « Systema otsinky ryzykiv » [Elektronnyy resurs] // NBU. Rezhym dostupu do resursu: https://bank.gov.ua/admin_uploads/article/Organizacijna_struktura_sistemi_upravlinnya_rizikami_2018-09-18_19_pr.pdf?v=6
6. **Kasovska I. V., Shapovalenko O. D., Lutsenko I. M.** (2021). Prohramni kompleksy merezhevoho monito-rynhu dlya pidvyshchennya efektyvnosti zakhy-stu merezh. *Suchasnyy zakhyst informatsiyi*, №1(45), 47–52.
7. **Kuznyuk K. V., Kovalenko O. Ye.** Doslidzhennya tekhnolohiy ta rozroblennya zasobiv rozshyrennya funktsional′nosti system monitorynhu komp'yuternykh merezh. *Informatsiyni tekhnolohiyi: ekonomika, tekh-nika, osvita: Zb. materialiv KHIII mizhnar. nauk.-prakt. Konf*
8. **Koskinen Marko.** (2024). Integrating open-source computer and network monitoring software to an automation supervision system.
9. https://www.zabbix.com/features, [Accessed 10.10.2024].

Banking infrastructure monitoring system

Oleg Kuzin

Annotation. In today's conditions of digital transformation of the financial sector, the stability and uninterrupted operation of the banking infrastructure is the key to success. The fault tolerance of computer systems is one of the key factors in the successful operation of modern organizations, especially in such critical industries as banking. Ensuring the constant availability of banking services is extremely important for the uninterrupted operation of payment systems, transaction processing and access to customer accounts. One of the main tools for maintaining fault tolerance is the monitoring of system indicators, which allows you to detect problems before they become critical and take measures to prevent failures.

This work examines the monitoring system of the bank's information environment, analyzes the key indicators of ensuring the system's fault-tolerant operation. Such features as the criticality of the studied parameters, the frequency of polling subsystems, time sensitivity and threshold values are separately considered.

Within the framework of the study, stable and abnormal values of the parameters of the monitoring objects were selected, and based on them, patterns of system behavior were formed. As a result, escalation levels, notification methods and application of additional automations to stabilize subsystems are defined.

Keywords: Fault tolerance, information environment, monitoring system, modeling.