УДК 004.052.3

АНАЛІЗ СУЧАСНИХ МЕТОДІВ ЗАБЕЗПЕЧЕННЯ ВІДМОВОСТІЙКОСТІ ІНФОРМАЦІЙНИХ СИСТЕМ НА РІЗНИХ РІВНЯХ АРХІТЕКТУРИ

Фролов Д.Є.
Харківський національний університет радіоелектроніки
Україна, Харків
dmytro.frolov@nure.ua, ORCID: 0009-0009-3291-3561

***Анотація**. У роботі проаналізовано сучасні методи забезпечення відмовостійкості інформаційних систем на різних архітектурних рівнях та запропоновано п'ять класифікаційних підходів. За результатами аналізу зроблено припущення про застосовність тих чи інших методів в залежності від стану інформаційної системи та комплексу вимог до її функційної здатності у розрізі обраного класу.*

***Ключові слова**: інформаційна система; відмовостійкість; багаторівневість; метод; архітектура.*

Вступна частина. Сучасний стан розвитку інформаційних технологій характеризується стрімким зростанням обсягів даних, активним поширенням цифрових сервісів та критичною залежністю бізнес-процесів від безперебійного функціонування інформаційних систем (ІС) [1]. Збої у роботі зазначених систем можуть призводити до негативних рівнорівневих наслідків, зокрема, зниження довіри до державних електронних послуг, зриву банківських операцій, порушення стабільності критичних систем тощо [2]. Відтак, задача забезпечення відмовостійкості ІС є досить важливою для сучасної інформаційної безпеки та системного проєктування. Однак царина сучасних підходів до забезпечення відмовостійкості ІС є недостатньо систематизованим та потребує узагальнення структурованої класифікації [3-6].

Метою роботи є проведення комплексного аналізу сучасних методів забезпечення відмовостійкості ІС на різних рівнях архітектури з урахуванням їхніх слабких та сильних сторін в тих чи інших умовах, дослідження закономірностей їх застосовності.

Основна частина. Аналіз сучасних наукових досліджень у сфері відмовостійкості ІС [3-6] показує, що спочатку необхідно вирішити задачу класифікації для виявлення спільних ознак тих чи інших методів, а потім проводити їх порівняльний аналіз або експериментальні дослідження.

Обґрунтування вибору критеріїв класифікації. У даній роботі пропонуються різні підходи до класифікації методів забезпечення відмовостійкості ІС. Ці підходи будуються на: функціональних особливостях методів, ознаках їх темпоральності, взаємоузгодженості, поведінкових траєкторіях, ступені їх інноваційності. Окремим способом класифікації є синтез інших класифікацій з огляду на власні критерії (коли специфіка включає елементи тих підходів у класифікації методів відмовостійкості, що дозволяють вивести на єдину площину ознаки за певними якісними критеріями). Причому логіка віднесення конкретного методу не обмежується одним класом в межах однієї системи класифікації, що показано нижче. Це означає, що один і той же метод може бути як інноваційним в системі класифікації за ступенем інноваційності, але і відноситися до певного класу методів за своєю функціональною здатністю в системі класифікації за функціональними ознаками. Отже, розглянемо наступні підходи до класифікації методів забезпечення відмовостійкості ІС, враховуючи [3-6]:

1. Класифікація методів забезпечення відмовостійкості ІС за ступенем інноваційності.

1.1 Клас класичних методів:

- резервування, що передбачає дублювання компонентів із можливістю автоматичного перемикання. Типовими прикладами є використання кластерів та відмовостійких серверів;

- надмірність, що реалізується через багатократне дублювання елементів інформаційної системи, зокрема дублюванні процесів, що забезпечують їх взаємодію;

- реплікація даних і сервісів, що може здійснюватися у синхронному чи асинхронному режимах;

- фіксація поточного стану системи та її відновлення, що ґрунтується на створенні періодичних знімків її стану та відновленні функційної здатності у випадку збоїв;

- ізоляція відмов, яка передбачає локалізацію збоїв у межах елементів системи, що запобігає поширенню відмови на інші елементи (каскадна відмова);

- детектори відмов елементів ІС у формі: таймаут-детекторів, що маркують вузол як підозрілий у разі відсутності відповіді протягом заданого інтервалу; heartbeat-механізмів, де елементи ІС регулярно надсилають контрольні повідомлення; накопичувальних детекторів, які оцінюють ступінь підозри відмов на основі статистики часових міток.

Класичні методи формують базовий набір інструментів відмовостійкості, проте їх аналіз ефективності у сучасних ІС показує обмеженість у масштабованості та/або гнучкістю.

1.2 Клас інноваційних методів. До сучасних інноваційних методів належать рішення, що стали можливими завдяки розвитку віртуалізації, контейнеризації та інтелектуальних технологій. Такими методами є:

- контейнеризація та оркестрація, наприклад, використання Docker compose, Kubernetes;

- віртуалізація та відновлення на основі знімків, що дозволяють швидке відновлення з образів віртуальних машин та контейнерів;

- методи машинного навчання, задачею яких є прогнозування відмов на основі даних стану елементів ІС;

- самовідновлення, що робить можливим автоматичне відновлення ресурсів;

- гібридні методи, що поєднують прикордонну реплікацію з резервуванням у хмарі, забезпечуючи баланс між продуктивністю, доступністю та стійкістю до відмов у розподілених середовищах.

2. Класифікація методів забезпечення відмовостійкості ІС за ознаками темпоральності.

За характером дій відносно настання відмови ІС методи групуються за такими класами:

- реактивні, що застосовуються після виникнення відмови;

- проактивні - спрямовані на прогнозування та запобігання відмовам.

Реактивні методи орієнтовані на мінімізацію наслідків відмов (у тому числі у ІС, що функціонують у динамічних умовах), тоді як проактивні дозволяють підвищити загальний рівень надійності завдяки прогнозуванню (але з більш ресурсоємними затратами).

3. Класифікація методів забезпечення відмовостійкості ІС за ознакою взаємоузгодженості.

Цей підхід до класифікації методів покликаний вирішити задачі узгодження станів між елементами ІС, на відміну від точкових підходів до відновлення окремо взятих елементів. Групування методів можливо за такими класами:

- клас методів консенсусу, що забезпечують узгодженість за наявності збоїв і асинхронності у поданні елементів ІС;

- клас методів кворумної реплікації, що гарантують цілісність операцій завдяки вимогам кворуму для читання / запису та дозволяють функціонувати за умов точкових відмов.

Методи консенсусу та кворумної реплікації є основою для побудови надійних розподілених ІС, забезпечуючи глобальну узгодженість станів її елементів.

4. Класифікація методів забезпечення відмовостійкості ІС за поведінковими траєкторіями.

Архітектурні патерни задають структурні та поведінкові принципи взаємодії між елементами ІС з метою підвищення їх стійкості до збоїв. Групування патернів можливе за такими класами:

- патерни локалізації та ізоляції відмов, що спрямовані на запобігання каскадів збоїв та обмеження їх впливу на всю ІС;

- патерни повторного виконання та компенсації, які реалізують підхід до повторюваності операцій або їх відкату до попереднього узгодженого стану ІС або її елементів;

- патерни відновлення стану ІС, що забезпечують відтворення її коректного стану на основі сукупності раніше збережених даних.

Зазначені методи дозволяють інтегрувати відмовостійкість на рівні самої архітектури ІС, поєднуючи алгоритмічні та інфраструктурні рішення у якості механізму відновлення.

5. Гібридний спосіб класифікації методів забезпечення відмовостійкості ІС.

Сучасна практика забезпечення відмовостійкості дедалі частіше ґрунтується на гібридних стратегіях, що поєднують реактивні та проактивні підходи. У таких рішеннях класичні механізми резервування і реплікації інтегруються з інноваційними підходами контейнеризації та оркестрації, методами прогнозування відмов на основі машинного навчання тощо. Такі комбінації дозволяють мінімізувати наслідки збоїв та упереджувати їх виникнення. Виділення гібридних стратегій в окремий клас зумовлене їх інтегративним характером: вони не можуть бути повністю віднесені ані до традиційних реактивних, ані до інноваційних проактивних методів, оскільки поєднують всю плеяду властивостей та створюють нові підходи у забезпеченні стійкості ІС. Саме ця здатність до синтезу різнорівневих підходів робить гібридні стратегії окремим напрямом, який поступово уніфікується у хмарних і розподілених ІС, наприклад як у [6].

Висновки. За результатами проведеного аналізу встановлено, що розглянуті методи забезпечення відмовостійкості характеризуються за наступними ознаками: надмірність як базовий засіб підвищення відмовостійкості, компромісність як спосіб балансування між надійністю, продуктивністю та ресурсоємністю, еволюційність як траєкторний підхід від простих реактивних рішень до складних гібридних, у тому числі самовідновлюваних ІС.

Загальним недоліком проаналізованих методів є те, що забезпечення відмовостійкості завжди пов’язане з додатковими витратами ресурсів і складністю, що призводить до аномальних перекосів у розподілі ресурсних можливостей ІС для досяжності відповідного рівня вимог відмовостійкості. Зокрема, високий рівень надмірності підвищує ресурсну вартість ІС; механізми консенсусу та реплікації при тонких налаштуваннях можуть призводити до падіння рівня продуктивності елементів ІС, що призводить до погіршення роботи всієї ІС; інноваційні проактивні підходи через складність застосовних алгоритмів та обмеженість часу на їх виконання можуть давати квазіоптимальні стратегії прогнозування.

Результати проведеного аналізу можуть бути використані при розробці планів застосування довгострокових стратегій забезпечення відмовостійкості ІС в апостеріорній

невизначеності або інших умовах, які вимагають швидкого аналізу наявних підходів у зазначеній сфері. Відповідно, результати роботи можуть бути розширені шляхом додавання у зазначені класифікаційні форми інших класів або методів, що робить зазначений підхід універсальним з точки зору подання його структури та наповненості.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

[1] Tkachov, V., & Mikhnov, Y. (2024). Analysis of fault tolerance algorithms in multisegment networks.

[2] Kharchenko, V., Ponochovnyi, Y., Vdovichenko, O., & Mahmudov, K. (2025, May). Models for Assessing the Dependability of Programmable Devices with Controlled Multi-Level Degradation. In *International Conference on Dependability and Complex Systems* (pp. 85-95). Cham: Springer Nature Switzerland.

[3] Shahid, M. A., Islam, N., Alam, M. M., Mazliham, M. S., & Musa, S. (2021). Towards Resilient Method: An exhaustive survey of fault tolerance methods in the cloud computing environment. *Computer Science Review*, *40*, 100398.

[4] de Souza, K. E., Ferrari, F. C., de Camargo, V. V., Ribeiro, M., & Offutt, J. (2025). A systematic review of fault tolerance techniques for smart city applications. *Journal of Systems and Software*, *219*, 112249.

[5] Miranda, F. D. S., dos Santos, D. S., Vilela, R. F., Assunção, W. K. G., dos Santos, R. C., & Pinto, V. H. S. C. (2024, November). A proposed catalog of development patterns for fault-tolerant microservices. In *Proceedings of the XXIII Brazilian Symposium on Software Quality* (pp. 406-416).

[6] Shahid, M. A., Alam, M. M., & Su'ud, M. M. (2023). Achieving reliability in cloud computing by a novel hybrid approach. *Sensors*, *23*(4), 1965.

Frolov D.Ye.

Analysis of modern methods of ensuring failure tolerance of information systems at different levels of architecture

Abstract*. The study analyzes modern methods of ensuring the fault tolerance of information systems at various architectural levels and proposes five classification approaches. Based on the analysis results, assumptions were made regarding the applicability of certain methods depending on the state of the information system and the set of requirements for its functional capability within the chosen class.*

Keywords*: information system; fault tolerance; multilevel structure; method; architecture.*