

Кондратов Дмитрий Александрович

Магистрант

Направление: Информатика и вычислительная техника

Магистерская программа: Информационные системы

Комплексная оценка и повышение функциональной живучести распределенных автоматизированных систем на основе информационной избыточности и упреждающей реконфигурации

Аннотация. Рассматривается задача повышения надежности распределенных автоматизированных систем (РАС), для которых бинарная модель состояний неприменима из-за частичной деградации функций при отказе отдельных узлов. Предложен согласованный комплекс моделей: сохранности данных с учетом групповых отказов домена размещения, мультиверсионного программного модуля с явным параметром корреляции ошибок версий.

Ключевые слова: распределенные автоматизированные системы, надежность, функциональная живучесть, информационная избыточность, помехоустойчивое кодирование, мультиверсионное проектирование, реконфигурация, предиктивный мониторинг, коэффициент готовности.

Системы управления производством, энергетикой и транспортом переходят к распределенной архитектуре, при которой функциональные компоненты разнесены между множеством узлов, а управляющая логика децентрализована. Микросервисные решения, контейнерная оркестрация и периферийные вычисления многократно увеличили число компонентов и потенциальных точек отказа, тогда как значительная часть таких систем отнесена к объектам критической информационной инфраструктуры.

Особенность распределенных систем состоит в неприменимости бинарной модели состояний «работоспособно – неработоспособно»: отказ узла переводит систему в состояние частичной деградации. Стандарты определяют надежность как свойство объекта сохранять во времени способность выполнять требуемые функции [1], однако коэффициент готовности отдельного узла не характеризует готовность системы в целом из-за зависимостей, порождающих каскадные отказы.

Известны развитые частные механизмы отказоустойчивости: репликация и помехоустойчивое кодирование данных [2; 3], мультиверсионное проектирование, самовосстановление в средах оркестрации [7], обнаружение аномалий по данным трассировки [5], проверка устойчивости методами chaos engineering [4] и прогнозирование состояния оборудования на основе цифровых двойников [6]. Однако единый аппарат, согласованно учитывающий информационную избыточность, программную надежность, реконфигурацию и прогнозное состояние узлов, отсутствует. Цель работы — разработка взаимосвязанного комплекса моделей и методики оценки функциональной живучести для обоснованного выбора средств избыточности и реконфигурации при заданных ресурсных ограничениях.

Постановка задачи

Интегральным показателем принят коэффициент функциональной живучести — математическое ожидание сохраняемой доли целевого назначения системы:

$$K_{фж}(x) = \sum_j P_j(x) \cdot [\sum_i w_i \cdot \delta_{ij}] / \sum_i w_i, \quad (1)$$

где P_j — вероятность пребывания системы в состоянии S_j ; w_i — вес важности функции f_i ; δ_{ij} — индикатор работоспособности f_i в состоянии S_j . Вектор проектных переменных включает параметры схемы кодирования (n, k), кратность репликации m , число версий V , время восстановления T_v и порог принятия решения Θ , а задача ставится как условная оптимизация

$$K_{фж}(x) \rightarrow \max \text{ при } C(x) \leq C_0, \tau_p(x) \leq \tau_0, K_{г}(x) \geq K_{г \text{ доп}}, \quad (2)$$

где $C(x)$ — суммарные затраты на средства избыточности, восстановления и мониторинга.

Информационная избыточность при децентрализованном хранении

Вероятность сохранности объекта, разделенного на n фрагментов с порогом восстановления k , при независимых отказах узлов с готовностью p описывается биномиальной суммой

$$P_{\text{сохр}}(n, k) = \sum_{i=k..n} C(n, i) \cdot p^i \cdot (1 - p)^{(n-i)}, \quad (3)$$

а избыточность хранения составляет $\eta_{\text{изб}} = n/k$. Однако узлы группируются по доменам отказа (стойка, коммутатор, энерговод), и отказ домена выводит из строя сразу $d = n/g$ фрагментов. Для учета этого предложено выражение

$$P_{\text{сохр}}^{\text{дер}} = (1 - \pi) \cdot P_{\text{сохр}}(n, k) + \pi \cdot P_{\text{сохр}}(n - d, k), \quad (4)$$

где π — вероятность группового отказа домена размещения, d — число теряемых в нем фрагментов. Отсюда следует требование к размещению $g \geq n/(n - k)$ при $d = \lfloor n/g \rfloor \leq n - k$, без соблюдения которого формально высокая сохранность кода не реализуется (таблица 1).

Таблица 1.

Сопоставление схем информационной избыточности

Схема размещения	$\eta_{\text{изб}}$	Десятки сохранности	Трафик восстановления
Репликация $\times 2$	2,0	3,96	$1 \cdot S$
Репликация $\times 3$	3,0	5,98	$1 \cdot S$
RS(9, 6), $g = 3$	1,50	4,12	$6 \cdot S$
RS(12, 8), $g = 4$	1,50	5,78	$8 \cdot S$

Всей системе ограничений удовлетворяет код RS(12, 8) с разнесением по четырем доменам отказа: он дает уровень сохранности, сопоставимый с трехкратной репликацией, при экономии около 50% дискового пространства; платой является рост трафика восстановления в k раз.

Программная надежность мультиверсионного модуля

Классические модели мультиверсионного программирования предполагают независимость ошибок версий, что на практике не выполняется: реализации по общей спецификации наследуют общие дефекты требований. Введем долю связанных ошибок

γ , разделив вероятность отказа версии q на $q_{сс} = \gamma q$ и $q_{нез} = (1 - \gamma)q$; тогда для мажоритарного голосования по V версиям

$$Q(V, \gamma) = q_{сс} + (1 - q_{сс}) \cdot \sum_{i=\text{maj}..V} C(V, i) \cdot q_{нез}^i \cdot (1 - q_{нез})^{(V-i)}, \quad (6)$$

где $\text{maj} = \lfloor V/2 \rfloor + 1$. Предельный переход дает $\lim Q(V, \gamma) = \gamma q$ при $V \rightarrow \infty$, т. е. надежность модуля ограничена снизу независимо от числа версий. При $q = 0,05$ и $\gamma = 0,10$ переход от одной версии ($Q = 4,98 \cdot 10^{-2}$) к трем ($Q = 1,09 \cdot 10^{-2}$) снижает вероятность отказа в 4,6 раза, а дальнейший рост V дает выигрыш, несопоставимый с ростом затрат, поэтому обосновано решение $V = 3$ с адаптивным взвешенным голосованием.

Реконфигурация кластера и упреждающий мониторинг

Время реконфигурации представлено суммой $t_r = t_{обн} + t_{пр} + t_{пер} + t_{стаб}$. Введение состояния реконфигурации в граф состояний трехузлового кластера с критерием «2 из 3» дает

$$U(t_r) = 3\lambda t_r + 3\rho^2 + \rho^3, \quad K_r = 1 - U(t_r), \quad \rho = \lambda/\mu. \quad (7)$$

Расчет при наработке на отказ 10 000 ч показывает, что более 99 % неготовности кластера обусловлено временем реконфигурации, а не отказами оборудования. Поэтому основным резервом служит упреждающая реконфигурация, при которой миграция нагрузки выполняется до отказа по прогнозу состояния узла: $t_r^{\text{эф}} = \text{TPR} \cdot t_{\text{пред}} + (1 - \text{TPR}) \cdot t_r$. Порог Θ целесообразно выбирать не по F-мере, а по экономическому критерию

$$E_{\text{мон}}(\Theta) = \text{TPR} \cdot \text{потк} \cdot (\text{сав} - \text{смигр}) - \text{FPR} \cdot \text{Нокон} \cdot \text{смигр} \rightarrow \max, \quad (8)$$

максимум которого достигается при $\Theta^* = 0,50$ и соответствует рабочей точке $\text{TPR} = 0,85$, $\text{FPR} = 0,05$. В этой точке эффективное время восстановления управления сокращается с 60,00 до 15,80 с, коэффициент готовности возрастает с 0,999994970 до 0,999998653, а издержки от ложных срабатываний не превышают 27,4 тыс. руб./год. Контур мониторинга использует 12 диагностических признаков с окном агрегирования 15 мин [5; 6; 7].

Результаты и технико-экономическая оценка

Частные решения сведены в единый критерий, связывающий аппаратную, программную и организационную составляющие надежности: $K_{фж} = [P_{\text{норм}} +$

$d_{рек} \cdot P_{рек}] \cdot [1 - w_{по} \cdot Q(V, \gamma)]$. Для модельного объекта из шести функций и пяти состояний получены $d_{рек} = 0,50$ и $w_{по} = 0,50$ (таблица 2).

Таблица 2.

Показатели надежности до и после внедрения решений

Показатель	Базовая конфигурация	Предлагаемая конфигурация
Схема хранения данных	Репликация $\times 3$	RS(12, 8), $g = 4$
Избыточность хранения $\eta_{изб}$	3,0	1,5
Число версий ПО V	1	3
Время реконфигурации, с	60,00	15,80
Коэффициент готовности K_g	0,999994970	0,999998653
Коэффициент живучести $K_{фж}$	0,97511	0,99457
Доля утрачиваемого назначения, %	2,489	0,543

Экспериментальная проверка выполнена методом управляемого внесения отказов [4] на пяти сценариях по 200 прогонов: для четырех сценариев отличие расчета от измерений не превысило 8%, а областью неконсервативности оказалась частичная сетевая изоляция узла (+37,3%).

Технико-экономический расчет дал: капитальные затраты 2780,0 тыс. руб., годовой эффект 4204,4 тыс. руб. (89,2% поступлений обеспечивает именно рост функциональной живучести), срок окупаемости 0,661 года (7,9 мес.), чистый дисконтированный доход за пять лет 10 368,0 тыс. руб. при норме дисконтирования 18%, внутреннюю норму доходности 149,7 % и индекс доходности 4,73.

Заключение

Предложенный комплекс моделей отличается от известных подходов совместным учетом коррелированных отказов при выборе схемы избыточности хранения, связанных ошибок версий при обосновании кратности мультиверсионного резервирования, времени реконфигурации при оценке готовности и стоимости ошибок прогноза при выборе порога принятия решения, а также согласуется с терминологией действующих

стандартов надежности [1]. Совместное применение решений повышает Кфж с 0,97511 до 0,99457, сокращая долю утрачиваемого целевого назначения в 4,58 раза.

Практическая значимость состоит в возможности обоснованного выбора параметров схемы кодирования, числа версий программного обеспечения, допустимого времени реконфигурации и порога принятия решения без проведения дорогостоящих натурных исследований. Перспективные направления – уточнение модели восстановления для режимов частичной сетевой изоляции и адаптивное изменение порога Θ .

Литература

1. ГОСТ Р 27.102-2021. Надежность в технике. Надежность объекта. Термины и определения. – М.: Стандартинформ, 2021. 24 с.
2. Shen Z., Cai Y., Cheng K., Lee P. P. C., Li X., Hu Y., Shu J. A Survey of the Past, Present, and Future of Erasure Coding for Storage Systems // ACM Transactions on Storage. 2025. Vol. 21, № 1. Art. 4. – DOI 10.1145/3708994.
3. Yin C., Xu Z., Li W., Li T., Yuan S., Liu Y. Erasure Codes for Cold Data in Distributed Storage Systems // Applied Sciences. 2023. Vol. 13, № 4. Art. 2170. – DOI 10.3390/app13042170.
4. Owotogbe J., Kumara I., van den Heuvel W.-J., Tamburri D. A. Chaos Engineering: A Multi-Vocal Literature Review. 2024. arXiv:2412.01416. – DOI 10.48550/arXiv.2412.01416.
5. Panahandeh M., Hamou-Lhadj A., Hamdaqa M., Miller J. ServiceAnomaly: An anomaly detection approach in microservices using distributed traces and profiling metrics // Journal of Systems and Software. 2024. Vol. 209. Art. 111917. – DOI 10.1016/j.jss.2023.111917.
6. Abdullahi I., Longo S., Samie M. Towards a Distributed Digital Twin Framework for Predictive Maintenance in Industrial Internet of Things (IIoT) // Sensors. 2024. Vol. 24, № 8. Art. 2663. – DOI 10.3390/s24082663.

7. Enhancing Kubernetes Resilience through Anomaly Detection and Prediction. 2025.
arXiv:2503.14114. – DOI 10.48550/arXiv.2503.14114.

@Бюллетень магистранта 2026 №5