Оригинальная статья
https://doi.org/10.21683/1729-2646-2022-22-1-4-12

Анализ влияния использования информационной избыточности на показатели надежности распределенных информационных систем

Владимир В. Кульба[1], Сергей К. Сомов[1]*, Алексей Б. Шелков[1]
[1]Федеральное государственное бюджетное учреждение науки Институт проблем управления им. В.А. Трапезникова Российской академии наук, Москва, Российская Федерация
**ssomov2016@ipu.ru*


Владимир В. Кульба


Сергей К. Сомов


Алексей Б. Шелков

Резюме. Цель. *В работе анализируется влияние информационной избыточности на показатели надежности функционирования распределенных автоматизированных информационных систем. Рассмотрена информационная избыточность в виде оперативного резерва и архивов магнитных носителей, размещенных в узлах системы.* **Методы.** *Использованы понятия теории вероятностей и Марковских процессов.* **Результаты.** *Проанализированы показатели надежности функционирования распределенных информационных систем и влияние на эти показатели оперативного и восстановительного резервирования массивов данных. Выполнен анализ эффективности использования трех стратегий оперативного резервирования в распределенных системах.* **Выводы**. *Использование информационной избыточности значительно увеличивает надежность и эффективность работы распределенных систем. В то же время данный вид избыточности требует некоторого увеличения эксплуатационных затрат.*
Ключевые слова: *распределенные информационные системы, резервирование и восстановление данных, отказы, сбои, показатели надежности информационных систем.*

Для цитирования: *Кульба В.В., Сомов С.К., Шелков А.Б. Анализ влияния использования информационной избыточности на показатели надежности распределенных информационных систем // Надежность. 2022. №1. С. 4-12. https://doi.org/10.21683/1729-2646-2022-22-1-4-12*

Поступила *06.10.2021 г.* / **После доработки** *07.02.2022 г.* / **К печати** *18.03.2022 г.*

Введение

В настоящее время информационные технологии стали ключевым элементом инфраструктуры организационного управления, позволяющим повысить его эффективность, минимизировать затраты различных ресурсов, стимулировать рост производительности труда и других показателей эффективности управления.

Надежность функционирования любой автоматизированной информационной системы существенно зависит от уровня сохранности используемых в ней данных. Проблема обеспечения высокого уровня надежности системы и сохранности используемых ей данных особо актуальна для крупномасштабных территориально-распределенных многоуровневых систем различного назначения, к которым можно отнести большинство современных информационных систем российских железных дорог, как, например, система КАСАНТ – комплексная автоматизированная системы учета, контроля устранения отказов технических средств и анализа их надежности [1].

Объединение сотен и тысяч компьютеров каналами связи в крупномасштабные компьютерные сети различного масштаба и топологии позволило создать на их основе распределенные автоматизированные информационные системы (РАИС), которые по сравнению с локальными системами, приобрели качественно иные особенности и возможности [2, 3].

В частности, на сохранность данных, размещенных на многочисленных устройствах хранения, могут оказывать влияние различные негативные факторы [4]. Такими факторами могут быть: ошибки и неисправности [5] компьютерного оборудования, ошибки программного обеспечения, ошибки оператора при несоблюдении им требований инструкций и регламентов. Ошибки в работе устройств хранения данных могут привести к искажению и даже потере данных, к сбою в работе отдельных или нескольких узлов сети, а в серьезных случаях возможен отказ всей распределенной системы. В этом случае могут потребоваться большие затраты ресурсов и времени для восстановления разрушенных или искаженных данных.

Использование информационной избыточности в распределенных информационных системах является одним из эффективных методов обеспечения высокого уровня сохранности данных и надежности работы таких систем. В настоящее время информационная избыточность широко используется в виде двух типов резервирования данных [3, 6]:

- оперативное резервирование, которое заключается в создании оперативного резерва (ОР) данных из некоторого множества копий и/или предысторий массивов данных, которые используются для повышения надежности процессов обработки распределенной системой поступающих запросов при возникновении ошибок в данных или их частичной потере в процессе обработки запросов;

- восстановительное резервирование, которое заключается в создании специального восстановительного резерва (ВР) данных, который используется только для восстановления оперативных данных в случае их разрушения или возникновения в них ошибок.

Во-вторых, так как рассматриваемые информационные системы имеют распределенную в геопространстве топологию, то можно применять два основных способа хранения двух типов резерва: централизованное и децентрализованное. При централизованном хранении резерв размещается в одном, центральном узле системы. При децентрализованном варианте резерв данных размещается в нескольких узлах системы, выбранных в соответствии с некоторым алгоритмом размещения резерва [6].

В-третьих, наличие большого количества узлов в системе предоставляет возможности использования множества различных вариантов размещения резерва в узлах сети, что обуславливает большую сложность выбора наилучшего варианта. Это приводит к необходимости постановки и решения задачи поиска оптимального варианта размещения резерва.

В-четвертых, при поиске наилучшего варианта распределения резерва по узлам сети необходимо учитывать различные параметры самой сети. Такие, как: пропускная способность каналов связи, трафик и средняя задержка сообщений, стоимость использования компьютеров и каналов сети и т.д.

Стратегии оперативного и восстановительного резервирования данных

В настоящее время для обеспечения сохранности данных используются три стратегии оперативного резервирования ОР, которые учитывают особенности их использования в информационных системах [3]:

Стратегия I. В соответствии с данной стратегией создается и затем используется резерв из определенного количества копий массива постоянных (редко изменяемых) данных**.** Обработка каждого запроса к данным массива начинается с использования основного массива. Если массив при этом разрушен, то обработка запроса продолжается с использованием данных первой его копии и т.д.

Стратегия II. В данной стратегии используется резерв из некоторого количества предысторий массивов с часто изменяемыми данными. Предыстория массива AP_i это его точная копия, созданная в момент времени $t_i \left(\overline{i = 1, N}\right)$ и журнал изменений данных массива, произошедших в интервале времени (t_i+Δt). В случае, если основной массив разрушен, то для его восстановления используется предыстория AP_N. Если эта предыстория разрушается в процессе восстановления, то она восстанавливается с помощью предыстории $AP_{(N-1)}$.

Стратегия III. Данная стратегия смешанная и использует для восстановления разрушенного основного

массива сначала копии массива (согласно стратегии I), а в случае разрушения всех копий переходит к использованию резерва из предысторий (согласно стратегии II).

Использование ОР существенно увеличивает надежность работы распределенной системы при обработке запросов, но не исключает полностью возможность разрушения самого ОР. Для восстановления разрушенного ОР используется восстановительный резерв данных (ВР). Есть два основных варианта использования ВР [6]:

1) Первый вариант применяется при децентрализованном размещении ОР в нескольких узлах системы. В случае разрушения ОР в некотором узле системы он восстанавливается с помощью другого неразрушенного экземпляра ОР, расположенного в ближайшем узле. В этом случае этот ОР используется в качестве ВР.

2) Второй вариант предусматривает использование специального ВР – архива магнитных носителей (АМН). АМН используется исключительно для обработки запросов на восстановление разрушенного ОР. АМН может быть размещен в одном узле сети или несколько его копий могут быть размещены в нескольких узлах.

В статье рассматриваются две стратегии восстановления разрушенного ОР – В-1 и В-2, которые позволяют существенно повысить уровень сохранности данных в распределенных системах [7]. Согласно стратегии В-1 все копии массивов данных, которые необходимы для восстановления ОР, создаются последовательно на основе данных из ВР. Вторая стратегия В-2 отличается от первой тем, что при получении очередной копии используются данные не только из ВР, но и все ранее полученные копии восстанавливаемого массива данных.

Показатели надежности работы РАИС, использующей оперативный резерв для восстановления разрушенных данных

Рассмотрим основные показатели надежности функционирования РАИС, в которой для повышения надежности ее работы используется только оперативное резервирование, без использования АМН.

С точки зрения надежности, функционирование РАИС, в узлах которой расположен оперативный резерв данных, можно представить как процесс переходов такой системы в пространстве возможных состояний. Переходы системы из одного состояния в другое происходят в результате отказов узлов системы, обрабатывающих поступающие запросы к данным, и/или после восстановления работоспособности ранее отказавших узлов. Таким образом, состояние РАИС в любой момент времени можно охарактеризовать количеством отказавших и количеством работоспособных узлов.

При обработке в некотором узле системы запроса к данным ОР этого узла может быть разрушен. В итоге узел становится неработоспособным и в дальнейшем не может обрабатывать поступающие запросы. Переход узла в такое состояние будем считать отказом узла. Так как в рассматриваемой системе не используется восстановительное резервирование, то отказавший узел будет далее находиться в таком состоянии. Предположим, что после отказа узла все поступающие в него запросы будут равномерно распределяться для обработки между всеми оставшимися на этот момент работоспособными узлами системы с ОР. В случае отказа всех узлов с резервом, система не сможет обрабатывать поступающие запросы. Такое состояние РАИС будем также трактовать как отказ системы.

Обозначим через M количество узлов РАИС с размещенным в них оперативным резервом, а через H – множество всех состояний РАИС. Множество H состоит из следующих элементов: H_0 – работоспособны все узлы системы, H_m – отказ m-го узла, H_{mn} – отказ узлов m и n, $H_{1,2,\ldots,M}$ – отказали все M узлов системы с ОР данных и система не работоспособна.

Тогда множество H всех состояний системы и его мощность $|H|$ будут равны:

$$H=\left\{H_0,H_1,\ldots,H_M,H_{1,2},\ldots,H_{1,2,\ldots,M}\right\},\ |H|=\sum_{i=0}^{M}C_M^i=2^M.$$

Система может находиться в каждый момент времени t только в одном состоянии $\xi(t)=H(t)\in H$. Будем считать, что РАИС может оставаться в исходном состоянии или переходить в другое состояние через равные промежутки времени. По истечении каждого очередного такого промежутка времени с некоторой вероятностью система либо переходит в другое состояние (отказал один или несколько узлов одновременно), либо система остается в прежнем состоянии (ни один из узлов системы не отказал). Такие переходы между возможными состояниями системы называются шагами случайного процесса. Обозначим через $\xi(t)$, $t\geq 0$ случайную величину, описывающую процесс переходов системы из одного состояния в другое.

Предположим, что в момент времени t система находится в состоянии $\xi(t)$. Допустим, что узел j за единичный интервал времени обрабатывает $\lambda_j(t)$ запросов при условии, что система находится в состоянии $\xi(t)$.

Допустим также, что в начальный момент t_0 времени система полностью работоспособна и в ней нет отказавших узлов. Через $\xi(t_0)=H(t_0)$ обозначим исходное работоспособное состояние системы в момент времени t_0, а через $\lambda_j^0=\lambda_j(t_0)$ – число запросов, которое узел j обрабатывает в момент времени t_0.

По истечении некоторого периода времени функционирования системы работоспособный узел j в момент времени t будет обрабатывать $\lambda_j(t)$ запросов:

$$\lambda_j(t)=\lambda_j^0+M_P^{-1}(t)\sum_{i\in I_O(t)}\lambda_i^0. \qquad (1)$$

В формуле (1) $I_o(t)$ – это множество номеров узлов системы, отказавших к моменту времени t, а $M_P(t)=M-\left|I_O(t)\right|$ – это количество узлов системы с размещенных в них резервом, которые работоспособны в момент времени t.

При обработке одного запроса в узле j может произойти отказ с вероятностью Q_j. Тогда для единичного интервала времени $(t, t+1)$ вероятность $\tau_j(t)$ отказа узла j и вероятность $\beta_j(t)$ безотказной работы узла будут соответственно равны:

$$\tau_{j(t)} = 1 - P_j^{\lambda_j(t)};\ \beta_j(t) = 1 - \tau_{j(t)} = P_j^{\lambda_j(t)};\ P_j = 1 - Q_j. \quad (2)$$

Пронумеровав последовательно все элементы множества H, получим множество S состояний системы, состоящее из аналогичного количества элементов:

$$H = S = \{S_0, S_1, \ldots, S_M, S_{M+1}, \ldots, S_N\},\ N = 2^M.$$

Представленный выше процесс переходов системы из одного состояния в другое – это однородный процесс, так как будущее состояние системы не зависит от истории ее предыдущих переходов, но зависит только от текущего ее состояния [8, 9]. Тогда можно утверждать, что условная вероятность $P\{\xi(t) = S_j / \xi(u) = S_i\}$ того, что система в момент времени t находится в состоянии S_j при том условии, что система в момент времени u находилась в состоянии S_i, будет равна:

$$P\{\xi(t) = S_j / \xi(t_1) = S_{i_1}, \ldots, \xi(t_n) = S_{i_n}, \xi(t_u) = S_i\} =$$
$$= \{\xi(t) = S_j / \xi(t_u) = S_i\} = p_{ij}(t-u).$$

При этом: $u > t_n > \ldots > t_1;\ t > u;\ i, j \in \{0,1,\ldots,N\}$.

То есть, условная вероятность $P\{\xi(t) = S_j / \xi(u) = S_i\}$ не зависит от моментов времени t и u, а зависит от расстояния $(t–u)$ между этими моментами. Следовательно, данная условная вероятность зависит от интервала времени, прошедшего от момента времени u до момента t.

Предположим, что $p_{ij}(t–u)$ – это условная вероятность такого события, которое соответствует переходу системы из состояния S_i в состояние S_j за интервал времени, равный $(t–u)$. Допустим, что переходы системы из одного состояния в другое происходят за единичный интервал времени. Тогда разница между моментами времени t и u будет равна 1 ($t–u$=1), а условная вероятность $p_{ij}(t-u) = p_{ij}(1) = p_{ij}$ – это переходная вероятность системы для состояний S_i и S_j.

Значения p_{ij} переходных вероятностей рассматриваемого процесса будут рассчитываться по формуле:

$$p_{ij} = \begin{cases} 0, при (i < j) или\ когда\ \xi(t) = S_j \neq S_i = \xi(t-1) \\ u|I_0(t)| = |I_0(t-1)|; \\ \prod_{n \in R} \tau_n(S_i) \left[\prod_{n \in R} \beta_n(S_i)\right]^{-1} \prod_{n \in I_p(S_i)} \beta_n S_i, в\ остальных\ случаях. \end{cases} \quad (3)$$

В формуле (3) использованы следующие обозначения:

$I_0(t)$ – множество номеров узлов системы, которые отказали к моменту времени t;

$I_p(S_i)$ – множество номеров работоспособных узлов системы, находящейся в состоянии S_i;

$\tau_n(S_i)$ – вероятность отказа узла n за единицу времени, когда система в состоянии S_i;

$R=[I_0(S_i) – I_0(S_j)]$ – множество номеров узлов, отказавших за переход системы за один шаг между двумя состояниями;

$I_p(S_i)$ – множество номеров узлов, работоспособных при состоянии S_i системы.

$$\beta_n(S_i) = \tau_n(S_i).$$

В рассматриваем процессе переходы системы между различными состояниями можно формально представить в виде ориентированного графа. Состояния системы в графе представляются его вершинами, а ориентированные дуги соответствуют переходам системы между состояниями (вершинами графа).

На рис. 1 представлен пример ориентированного графа случайного процесса переходов системы. Система состоит из $M = 2$ узлов с множеством состояний: $S_0=H_0$; $S_1=H_1$; $S_2=H_2$; $S_3=H_{1,2}$; $\xi(t_0)=S_0$.

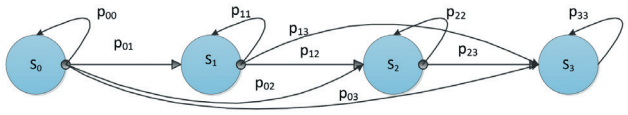

Рис. 1. Граф процесса случайных переходов для системы из 2-х узлов.

Так как отказавшие узлы в рассматриваемом случае не восстанавливаются, то систему можно считать невосстанавливаемым объектом, который имеет конечное множество работоспособных состояний и одно состояние полного отказа [8, 9]. А сам процесс переходов системы между разными состояниями является поглощающей цепью Маркова с дискретным временем [9, 10].

Рассмотрим следующие важные показатели надежности системы: T_1 – среднее время работы системы до отказа; $Q(t_0)$ и $Q(t,t+t_0)$ – вероятность отказа системы в интервалах времени $[0,t_0]$ и $[t,t+t_0]$; $P(t_0)$ и $P(t,t+t_0)$ – вероятность безотказной работы системы в интервалах времени $[0,t_0]$ и $[t,t+t_0]$.

Перечисленные показатели надежности получим и проанализируем на примере системы, функционирующей на основе однородной полносвязной вычислительной сети (для ситуации неоднородной сети получение и анализ показателей производится аналогично с помощью формул (1)–(3)).

Обозначим через $S=\{S_0, S_1, \ldots, S_N\}$ множество всех состояний системы, у которой множество узлов с оперативным резервом равно N. Через S_j обозначим такое состояние системы, в котором отказали j узлов с оперативным резервом. Пусть начальная интенсивность запросов, обрабатываемых каждым из узлов системы, находящейся в состоянии S_0, будет равна λ_0. А интенсивность запросов, обрабатываемых узлами сети, работоспособными в состоянии S_j системы, обозначим как λ_j. Тогда в соответствии с формулой (1) получим следующую формулу для расчета λ_j:

$$\lambda_j = \lambda_0 + \lambda_j (N-j)^{-1} = \lambda_0 N (N-j)^{-1}. \quad (4)$$

Вероятность τ_j того, что за единичный интервал времени откажет один из узлов сети, находящейся в

состоянии S_j, с учетом формулы (2) будет вычисляться следующим образом:

$$\tau_j = 1 - p^{\lambda}. \quad (5)$$

Переходные вероятности для рассматриваемой сети с учетом (3) будут вычисляться по следующей формуле:

$$p_{ij} = \begin{cases} 0, \textit{ при } i < j; \\ C_{N-j}^{j-i} \tau_i^{j-i} \beta_i^{N-j}, \textit{ при } 0 \le i \le j \le N. \end{cases} \quad (6)$$

Так как в системе не используется восстановительное резервирование, то отказавший узел не восстанавливается, и система через какое-то время перейдет в состояние S_N, в котором все узлы системы будут неработоспособны. Причем p_{NN}=1, так как S_N – это поглощающее состояние.

Таким образом, в результате имеется матрица вероятностей P=p_{ij} переходов системы между состояниями, известно S_0 начальное состояние системы, система имеет одно поглощающее состояние S_N и множество $\{S_0, S_1..., S_{N-1}\}$ работоспособных состояний системы. Тогда можно утверждать, что имеется поглощающая цепь Маркова с дискретным временем. Для нее определено множество S^1= $\{S_0, S_1..., S_{N-1}\}$ невозвратных состояний. Т.е. множество состояний работоспособности системы, в которых не все узлы отказали. А также одноэлементное множество поглощающих состояний S^2= $\{S_N\}$ (когда все узлы системы находятся в неработоспособном состоянии).

Так как цепь Маркова имеет одно поглощающее состояние, то через какое-то время она из начального состояния обязательно попадет в это поглощающее состояние. Определим, за какое среднее количество n_{ij} шагов цепь будет находиться в одном из невозвратных состояний $S_j \in S^1$ до поглощения при условии, что состояние S_i было ее начальным состоянием. Каждый шаг по переходу из состояния в состояние совершается системой за единичный интервал времени. Следовательно, величину n_{ij} можно рассматривать как среднее время нахождения системы в состоянии S_j до момента поглощения при условии, что S_i было начальным состоянием системы. Само начальное состояние S_i привносит в значение n_{ij} вклад, который равен 1 при $i = j$ и 0 в остальных случаях, т.е.:

$$\delta_{ij} = \begin{cases} 1, \textit{ при } i = j; \\ 0, \textit{ при } i \ne j. \end{cases}$$

В состояние S_m цепь переходит за один шаг из состояния S_i с вероятностью p_{im}. Если предположить, что $S_m \in S^2$, то в состояние S_j цепь не попадет никогда. Если же $S_m \in S^1$, то в течение n_{mj} шагов цепь будет находиться в состоянии S_j. Следовательно, мы можем записать:

$$n_{ij} = \delta_{ij} + \sum_{S_m \in S^1} p_{im} n_{mi}.$$

Данное равенство в матричной форме выглядит так:

$$\tilde{N} = I + \bar{Q}\tilde{N} \text{ или } \left(I - \bar{Q}\right)\tilde{N} = I.$$

В этой формуле I=δ_{ij} – это единичная матрица, соответствующая символу Кронеккера, размерности (N×N); $\bar{Q}$ – это матрица размерности (N×N), которая описывает поведение цепи во множестве невозвратных состояний S^1. Она получается из матрицы P=p_{ij} путем удаления из нее последнего столбца и последней строки.

Фундаментальную матрицу $\tilde{N}$ для поглощающей цепи Маркова получим, умножив слева на $\left(I - \bar{Q}\right)^{-1}$ обе части выше приведенного равенства [10]:

$$\tilde{N} = \left(I - \bar{Q}\right)^{-1}. \quad (7)$$

Определим среднее время t_i пребывания цепи во множестве состояний S^1, используя матрицу $\tilde{N}$, с учетом того, что начальным состоянием цепи является состояние S_i. Очевидно, что t_i=0 при $S_i \in S^2$. Следовательно:

$$t_i = \sum_{S_j \in S^1} n_{ij}; \; S_i \in S^1. \quad (8)$$

Справедливость формулы (8) следует из того, что она основывается на том, что время пребывания цепи во множестве состояний S^1 равно сумме случайных величин. Или, другими словами, равно результату сложения каждого из отдельных времен пребывания цепи в каждом из невозвратных состояний множества S^1. Более того, значение средней суммы случайных величин всегда равно сумме средних значений величин, входящих в данную сумму [11].

Как было ранее определено, $p_{ij}(n)$ – это вероятность перехода системы из состояния S_i в состояние S_j за n шагов. Затем, с учетом формулы полной вероятности, мы получим, что эта вероятность будет вычисляться по формуле:

$$p_{ij}(n) = \sum_{S_m \in S^1} p_{im} p_{mj}(n-1); \; p_{mj}(0) = \delta_{mj}.$$

Полученная формула в матричной форме будет выглядеть следующим образом: $P(n)$=P^n. Т.е. матрица вероятностей переходов системы за n шагов равна n-й степени матрицы переходных вероятностей системы.

На интервале времени от 0 до t_0 система совершит t_0 шагов, так как за единичный интервал времени система выполняет один шаг процесса переходов. Тогда, с учетом того, что, $p_{0N}(n)$=0 при n<N, мы получим, что

$$P(t_0) = 1 - \sum_{n=N}^{t_0} p_{0N}(n); \; Q(t_0) = \sum_{n=N}^{t_0} p_{0N}(n).$$

По формуле условной вероятности вероятность $P(t,t+t_0)$ безотказной работы системы на интервале от t до $(t+t_0)$ определяется как $P(t+t_0)$=$P(t+t_0)/P(t)$. Из этого следует, что вероятность $Q(t+t_0)$ отказа системы на интервале времени от t до $(t+t_0)$ будет равна $Q(t+t_0)$=1–$P(t+t_0)/P(t)$.

С использованием формулы (8) определим значение среднего времени T_1 функционирования системы до отказа. Так как в нашей системе начальное состояние – S_0, а поглощающее состояние – S_N, то искомое время T_1 определится по формуле

$$T_1 = t_0 = \sum_{S_j \in S^1} n_{0j} = \sum_{j=0}^{N-1} n_{0j}.$$

Если для рассматриваемой цепи Маркова вычислить в соответствии с формулой (7) матрицу $\tilde{N} = n_{ij}$, мы получим:

$$n_{ij} = \begin{cases} 0, \textit{ при } j < i; \\ \prod_{m=i}^{j-1} p_{m,m+1} \left[\prod_{n=i}^{j} (1 - p_{nn}) \right]^{-1}, \textit{ при } i \le j. \end{cases}$$

Так как при этом $n_{ii}=(1-p_{ii})^{-1}$, то мы получим, что среднее время T_1 функционирования системы до отказа равно:

$$T_1 = \prod_{j=0}^{N-1} \prod_{m=0}^{j-1} p_{m,m+1} \left[\prod_{n=i}^{j} (1 - p_m) \right]^{-1}.$$

Сделаем предположение о том, что параметры системы и величина единичного интервала времени таковы, что вероятность события, заключающегося в одновременном отказе двух и более узлов в системе близка к нулю, т.е.:

$$p_{jj} + p_{j,j+1} \gg \sum_{n=2}^{N-j} p_{j,j+n}; \left(p_{jj+p_{j,j+1}} = 1 \right). \quad (9)$$

С учетом этого предположения рассмотрим величину T_1 среднего времени функционирования системы до отказа. На рис. 2 показан граф переходов для системы, соответствующий рассматриваемым предположениям.

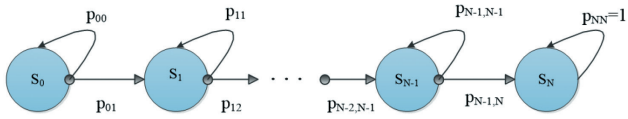

Рис. 2. Граф случайного процесса переходов системы во множестве состояний S

Определив матрицу $\tilde{N}$ с использованием формулы (7), получим, что: $n_{jj}=1$ при $i>j$ и $n_{jj} = p_{j,j+1}^{-1}$ при $i \le j$. Тогда среднее время T_1 работы системы до отказа равно:

$$T_1 = \sum_{j=0}^{N-1} p_{j,j+1}^{-1} = \sum_{j=0}^{N-1} (1 - p_{jj})^{-1}.$$

Рассмотрим вероятности $\rho_{jj}^{\gamma} (\gamma = I, II, II)$ события, которое заключаются в том, что система за единичный интервал времени не покинет состояние S_j. При условии, что в узлах системы используется ОР, созданный в соответствии с одной из трех стратегий оперативного резервирования $(\gamma = I, II, II)$. Докажем, что для рассматриваемых вероятностей справедливо соотношение (10)

$$\rho_{jj}^{I} > \rho_{jj}^{III} > \rho_{jj}^{II}. \quad (10)$$

С учетом формул (4)–(6) мы получим:

$$\rho_{jj} = \beta_j^{(N-j)} = p^{\lambda N}; \; j = 0,1,\ldots,(N-1). \quad (11)$$

В работе [7] было доказано, что в случае создания ОР с помощью трех стратегий оперативного резервирования $(\gamma = I, II, II)$, для вероятностей P^{γ} успешной обработки запросов (при не разрушении ОР узла, в котором обрабатывается запрос) справедливо соотношение:

$$P^{I} > P^{III} > P^{II}.$$

Тогда справедливо и соотношение (10), и выражение для T_1^{γ} среднего времени функционирования системы до ее отказа:

$$T_1^{I} > T_1^{III} > T_1^{II}.$$

Последние полученные результаты можно сформулировать как следующее утверждение.

Утверждение 1. Использование стратегии I резервирования для создания ОР в распределенных системах, не использующих восстановительное резервирование, обеспечивает наибольшее среднее время функционирования таких систем до отказа по сравнению с остальными стратегиями оперативного резервирования (стратегии II, III).

Величина $P(t_0)$ вероятности безотказной работы системы в интервале времени $[0,t_0]$ с учетом формулы (9) для рассматриваемого варианта распределенной системы, т.е. без использования восстановительного резервирования, будет равна:

$$P(t_0) = 1 - p_{0N}(N) \sum_{n=0}^{t_0 - N} B^n;$$

$$\textit{где: } p_{0N}(N) = \prod_{i=0}^{N-1} p_{i,i+1} = \left(1 - p^{\lambda N}\right)^N;$$

$$B = \sum_{i=0}^{N-1} p_{ii} = N p^{\lambda N}.$$

Причем $P(t_0)=0$ при $t_0<N$.

Показатели надежности работы РАИС, использующей архивы магнитных носителей для восстановления разрушенных данных

Рассмотрим показатели надежности функционирования РАИС, которая использует восстановительное резервирование на основе архивов магнитных носителей.

Архив магнитных носителей представляет собой специальный набор или несколько наборов из некоторого множества копий и/или предысторий массивов данных. АМН хранится в одном узле (централизованный вариант архива) системы или в нескольких узлах в случае децентрализованного хранения нескольких идентичных копий архивов магнитных носителей. [12]. АМН применяются исключительно для восстановления ОР, разрушенного в одном или нескольких узлах распределенной системы, и повышают тем самым надежность системы.

Предположим, что при обработке в узле с АМН запроса на восстановление разрушенного оперативного резерва с некоторой вероятностью может произойти отказ самого узла с АМН. С учетом такой возможности выполним анализ показателей надежности функционирования РАИС, которая использует восстановительное резервирование в виде архивов магнитных носителей, которые сами могут быть в состоянии отказа.

При обработке запроса к данным в узле с ОР он может быть разрушен, в результате чего происходит отказ этого узла. Восстановление работоспособности отказавшего узла производится с помощью одной из двух восстановительных стратегий: В-1 или В-2, использующих АМН.

Под отказом всей системы РАИС будем понимать такое состояние системы, когда отказали все узлы системы с ОР и отказали все АМН.

В состоянии отказа РАИС не способна обрабатывать поступающие запросы к данным и у нее нет возможности восстановить работоспособность узлов с ОР из-за отказа всех АМН.

Допустим, что справедливы следующие несколько предположений: 1) запросы, поступающие в отказавший узел с ОР, не переадресуются в работоспособные узлы и не обрабатываются до момента восстановления узла; 2) в случае отказа узла с АМН он не восстанавливается; 3) все поступающие в отказавший узел с АМН запросы на восстановление узлов с разрушенным ОР, равномерно распределяются и переадресуются в другие работоспособные узлы с АМН; 4) запросы на восстановление отказавших узлов с ОР равномерно распределяются между всеми работоспособными узлами с АМН.

Для описания работы такой РАИС будем использовать однородную поглощающую цепь Маркова с дискретным временем. Предположим, что параметры системы таковы, что вероятность отказа одновременно более одного узла с ОР или более АМН за единичный интервал работы системы близка к нулю. С учетом данного предположения определим множество H состояний информационной системы $H = \{H_{m,n}\}$, $m = \overline{0,M}, n = \overline{0,N}$.

Состоянию $H_{m,n}$ соответствует такое состояние РАИС, при котором в системе в состоянии отказа находятся m архивов магнитных носителей и n узлов с ОР. Предположим, что из состояния $H_{m,n}$ система за единичный интервал времени функционирования (за один шаг Марковского процесса) может перейти при n=0 в состояние $H_{m+1,0}$. А при $m = M$ система переходит в состояние $H_{M,n+1}$ или же система может остаться в исходном состоянии. С учетом сделанных выше предположений граф процесса переходов системы будет иметь вид, представленный на рис. 3а.

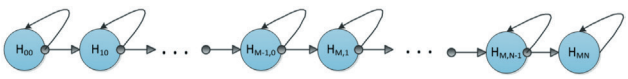

Рис. 3а. Граф переходов распределенной системы в множестве H возможных состояний

На основе множества состояний H построим множество состояний $S = \{S_i\}, i = \overline{1,K}$, K=M+N–1, где S: $S = \{S_i,\ (i = \overline{1,K}, k = M + N - 1)\}$. Элементу S_i множества S при $0 \le i < M$ соответствует состояние $H_{i,0}$, а при i=M состояние $H_{M,1}$, и при $M < i \le K$ состояние $H_{M,i}$. Построенному множеству S соответствует граф переходов системы, представленный на рис. 3б.

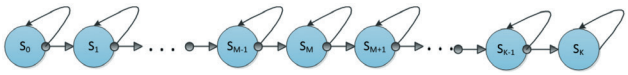

Рис. 3б. Граф переходов распределенной системы во множестве S возможных состояний

Допустим, что система с вероятностью p_{ij} может за один шаг процесса перейти из состояния S_i в состояние S_j. С учетом сделанных предположений можно утверждать, что:

$$p_{ij} \neq 0 \text{ при } i=j \text{ или}$$
$$j=i+1,\ p_{kk}=1 \text{ и } p_{ii}+p_{i,i+1}=1 \text{ при } 0 \le i \le K-1.$$

Допустим, что в системе за единичный интервал времени в каждый из N узлов с оперативным резервом поступает λ запросов к данным. Каждый узел в процессе обработки одного запроса может отказать с вероятностью Q=1–P или с вероятностью P успешно его обработать. Поскольку мы предположили, что все запросы на восстановление узлов с ОР распределяются среди работоспособных узлов с АМН равномерно, то, если система находится в состоянии S_0, в каждый узел, имеющий АМН, поступает μ_0 запросов на восстановление за единичный интервал времени работы системы:

$$\mu_0 = \lambda Q N M^{-1}.$$

С другой стороны, в процессе обработки запроса на восстановление ОР сам АМН может быть разрушен с вероятностью Q_A=1–P_A. Здесь P_A – вероятность успешной обработки в узле с АМН запроса на восстановление ОР. При отказе узла с АМН поступавшие в него запросы на восстановление ОР начинают равномерно распределяются между остающимися в работоспособном состоянии другими узлами с АМН.

Предположим, что система находится в состоянии $S_i\ \left(i = \overline{1, M-1}\right)$, тогда в каждый узел с АМН за единичный интервал времени поступает μ_i запросов на восстановление разрушенных оперативных резервов в узлах сети:

$$\mu_i = \mu_0 + i\mu_0 \left(M-i\right)^{-1} = \mu_0 M \left(M-i\right)^{-1}.$$

Тогда работоспособный АМН, находящийся в состоянии S_i, за единичный интервал времени может отказать с вероятностью φ_i. Вероятность φ_i равна $\varphi_i = 1 - P_A^{\mu_i}$. С другой стороны, узел с АМН может успешно обработать запрос на восстановление ОР с вероятностью $\Psi_i = 1 - \varphi_i$. Переход системы за один шаг из состояния S_i в состояние $S_{i+1}\left(i = \overline{1 = M-1}\right)$ происходит с вероятностью $p_{i,i+1}$, которая рассчитывается в соответствии со следующей формулой:

$$p_{i,i+1} = 1 - \Psi_i^{M-i} = 1 - P_A^{\mu_0 M} = 1 - P_A^{\lambda Q N};$$
$$p_{ii} = 1 - p_{i,i+1} = P_A^{\mu_0 M}. \qquad (12)$$

С учетом полученных в предыдущем параграфе результатов, получим, что значение вероятности $p_{i,i+1}$ при $i = M,(K-1)$ будет равно:

$$p_{i,i+1} = 1 - p^{\lambda N}; \;\; p_{ii} = p^{\lambda N}. \qquad (13)$$

Предположим, что в случае, когда разрушены все узлы с АМН ($i \geq M$), отказавший узел с ОР не восстанавливается. Все поступающие в этот узел запросы к данным распределяются равномерно по оставшимися в работоспособном состоянии узлам с оперативным резервом.

Для рассматриваемого варианта распределенной системы в соответствии с формулой (7) и с учетом формул (12) и (13) получим фундаментальную матрицу $\tilde{N} = n_{ij}$ поглощающей цепи Маркова, в которой ее элемент равен:

$$n_{ij} = \begin{cases} 0, \; при \; i > j; \\ p_{j,j+1}^{-1}, \; при \; i \leq j. \end{cases}$$

Далее определим показатели надежности функционирования рассматриваемой системы, которая использует восстановительное резервирование в виде ненадежных АМН. Узлы с АМН могут выходить из строя при обработке запросов на восстановление разрушенного ОР в узлах системы. Такую распределенную систему можно рассматривать как невосстанавливаемый объект.

Предположим, что система находится в начальном состоянии S_0. Тогда можно утверждать, что среднее время T_1 функционирования распределенной системы до отказа равно среднему времени, которое система проведет во множестве $S^1 = \{S_0, \ldots, S_{K-1}\}$ невозвратных состояний. Формула для расчета времени T_1 представлена ниже:

$$T_1 = \sum_{j=0}^{K-1} n_{0j} = \sum_{j=0}^{K-1} p_{j,j+1}^{(K-1)}$$

С учетом формул (12) и (13) формула для расчета T_1 преобразуется к следующему виду:

$$T_1 = \sum_{j=0}^{M-1} \left[1 - P_A^{\lambda QN}\right]^{-1} + \sum_{j=0}^{K-1} \left(1 - P^{\lambda N}\right)^{-1}$$

Для двух восстановительных стратегий В-1 и В-2 в работе [7] было доказано следующее неравенство $P_A^{B-1} < P_A^{B-2}$, из которого следует, что справедливо следующее аналогичное неравенство для среднего времени работы системы до отказа:

$$T_1^{B-1} < T_1^{B-2}.$$

Из этого неравенства следует справедливость следующего утверждения.

Утверждение 2. Применение восстановительной стратегии В-2 в распределенных системах, использующих АМН, обеспечивает среднее время работы системы до отказа большее, чем восстановительная стратегия В-1.

В работе [7] было доказано, что в случае создания ОР с помощью трех стратегий оперативного резервирования $(\gamma = I, II, II)$, для вероятностей P^{γ} успешной обработки запросов (при не разрушении ОР узла, в котором обрабатывается запрос) справедливо соотношение, показанное ниже.

$$P^{I} > P^{III} > P^{II}.$$

Если ОР в узлах распределенной системы создан при использовании одной из трех стратегий резервирования, с параметрами резервирования $(x_i > 1, 0 < q_i < 1/2)$, то в соответствии с результатами работы [7] для вероятности (P=1–Q) успешной обработки запросов к данным в узле i справедливо соотношение:

$$P_i^{I}(x_i) > P_i^{III}(x_i) > P_i^{II}(x_i).$$

С учетом данного соотношения доказывается справедливость следующего неравенства:

$$T_1^{I} > T_1^{III} > T_1^{II}.$$

Полученные результаты сформулируем в форме следующего утверждения.

Утверждение 3. Применение стратегии I оперативного резервирования в распределенных информационных системах позволяет получить среднее время работы таких систем до отказа большее, чем при использовании стратегий II и III оперативного резервирования.

Рассмотрим вероятность $P(t_0)$ безотказной работы и вероятность $Q(t_0)$ отказа распределенной системы на интервале времени $[0,t_0]$.

На основе полученных ранее результатов получим, что:

$$P(t_0) = 1 - \sum_{n=K}^{t_0} p_{0,K}(n) = 1 - p_{0,K}(K) \sum_{m=0}^{t_0-K} B^m,$$

где:

$$p_{0,K}(K) = \prod_{i=0}^{K-1} p_{i,i+1} = \left[1 - P_A^{\mu_0 M}\right]^M \left[1 - P^{\lambda N}\right]^{(N-1)};$$

$$B = \sum_{i=0}^{K-1} p_{ii} = MP_A^{\mu_0 M} + (N-1)P^{\lambda N}.$$

На интервале времени $[0,t_0]$ система откажет с вероятностью $Q(t_0)$=1–$P(t_0)$. На интервале времени $[t,t+t_0]$ значения вероятности P безотказной работы системы и вероятности Q отказа системы будут рассчитываться в соответствии со следующими формулами:

$$P(t, t+t_0) = P(t+t_0) / P(t);$$

$$Q(t, t+t_0) = 1 - P(t, t+t_0).$$

Заключение

В статье рассмотрены методы повышения надежности функционирования распределенных автоматизированных информационных систем методами информационной избыточности. Проведен анализ эффективности

стратегий оперативного резервирования массивов данных в узлах распределенной системы и стратегий восстановления разрушенного ОР. Выполнен анализ влияния стратегий оперативного и восстановительного резервирования на такие показатели надежности функционирования РАИС, как среднее время работы системы до отказа, вероятность отказа системы и вероятность безотказной работы системы в заданном интервале времени. Доказано несколько утверждений связанных с эффективностью рассмотренных стратегий с точки зрения времени функционирования РАИС до отказа.

Приведенные в данной работе результаты могут быть использованы на этапах проектирования, создания и эксплуатации РАИС различного класса и назначения. Особую актуальность эти результаты могут иметь для таких крупномасштабных территориально-распределенных многоуровневых автоматизированных систем, как системы класса АСУ железнодорожного транспорта. Для таких систем проблемы обеспечения надежности функционирования и сохранности используемых ими данных приобретают особую важность и актуальность.

Библиографический список

1. Шерстюков О.С. Автоматизированная система учёта, контроля устранения отказов устройств и анализа их надёжности // Мировые тенденции развития науки, образования, технологий: сборник научных трудов по материалам Международной научно-практической конференции 11 июня 2021г. : Белгород : ООО Агентство перспективных научных исследований (АПНИ), 2021. С. 42-46. URL: https://apni.ru/article/2543-avtomatizirovannaya-sistema-uchyota-kontrolya (дата обращения: 05.02.2022).

2. Шубинский И.Б. Надежные отказоустойчивые информационные системы. Методы синтеза. М.: «Журнал Надежность», 2016. 546 с.

3. Информационное обеспечение систем организационного управления (теоретические основы): В 3-х частях / Под ред. Е.А. Микрина, В.В. Кульбы. М.: Изд-во физико-математической литературы, 2012. Ч.1: 464 с. Ч.2: 496 с. Ч.3: 528 с.

4. Восстановление данных [Электронный ресурс]. URL: http://www.datarecovery.ru/datarecovery.htm (дата обращения 10.09.2021).

5. Шубинский И.Б., Шебе Х. Ошибки, неисправности и отказы // Надежность. 2021. № 2. С. 24-27.

6. Сомов С.К. Сохранность информации в распределенных системах обработки данных. М.: ИПУ РАН, 2019. 254 с.

7. Кульба В.В., Сомов С.К., Шелков А.Б. Резервирование данных в сетях ЭВМ. Казань: Издательство казанского университета, 1987. 175 с.

8. Тихонов В.И. Случайные процессы. Примеры и задачи. Том 1 – Случайные величины и процессы: Учебное пособие для вузов / В.И. Тихонов, Б.И. Шахтарин, В.В. Сизых. М.: Горячая линия–Телеком, 2014. 400 с.

9. Розанов Ю.А. Случайные процессы. М.: Наука, 1979. 184 с.

10. Кемени Д., Снелл Д. Конечные цепи Маркова. М.: Мир, 1970. 271 с.

11. Коваленко И.Н., Филиппова А.А. Теория вероятностей и математическая статистика. М.: Высшая школа, 1978. 368 с.

12. Микрин Е.А., Сомов С.К. Анализ эффективности стратегий восстановления информации в распределенных системах обработки данных // Информационные технологии и вычислительные системы. 2016. № 3. С. 5–19.

Сведения об авторах

Владимир Васильевич Кульба – заслуженный деятель науки Российской Федерации**,** доктор технических наук, профессор, главный научный сотрудник, Федеральное государственное бюджетное учреждение науки Институт проблем управления им. В.А. Трапезникова Российской академии наук. Адрес: ул. Профсоюзная, 65, г. Москва, Российская Федерация, 117997, e-mail: kulba@ipu.ru.

Сергей Константинович Сомов – кандидат технических наук, старший научный сотрудник, Федеральное государственное бюджетное учреждение науки Институт проблем управления им. В.А. Трапезникова Российской академии наук. Адрес: ул. Профсоюзная, 65, г. Москва, Российская Федерация, 117997, e-mail: ssomov2016@ipu.ru.

Алексей Борисович Шелков – кандидат технических наук, ведущий научный сотрудник, Федеральное государственное бюджетное учреждение науки Институт проблем управления им. В.А. Трапезникова Российской академии наук. Адрес: ул. Профсоюзная, 65, г. Москва, Российская Федерация, 117997, e-mail: shelkov@ipu.ru.

Вклад авторов в статью

Кульба В.В. Автор идеи использования информационной избыточности для обеспечения сохранности данных и надежности работы информационных систем. Общее руководство и участие в подготовке статьи.

Сомов С.К. Выполнена постановка задачи исследования**.** Разработана формальная модель информационной системы, использующей оперативное резервирование данных и архивы магнитных носителей. Выполнен анализ модели, доказана справедливость утверждений, сформулированных в статье.

Шелков А.Б. Участие в подготовке раздела «Введение» статьи и в подготовке формальной модели системы. Консультирование по специфике информационных систем, используемых в РЖД.

Конфликт интересов

Авторы заявляют об отсутствии конфликта интересов.