УДК 681.3.06

ПАРАДИГМА ОГРАНИЧЕННОГО СТОХАСТИЧЕСКОГО КОНТРОЛЯ

Алексей Сергеевич Марков
кандидат технических наук
генеральный директор НПО «Эшелон»
Адрес: 107023, Москва, ул. Электрозаводская, д. 24
Тел.: +7(495)645-38-09, +7(495)971-22-98
E-mail: mail@cnpo.ru

Разработаны модели стохастического ограниченного контроля и резервирования. Предложены критерии выбора стохастических и детерминированных моделей.

The models of stochastic control and a limited backup are discussed. Criteria for selection of stochastic and deterministic models are done.

Ключевые слова: периодический контроль, резервное копирование, стохастический ограниченный контроль, стохастические модели.

Keywords: periodic monitoring, backup, stochastic limited monitoring, stochastic models.

Введение

Универсальным принципом обеспечения непрерывности функционирования автоматизированных систем управления (АСУ) является информационное резервирование, основным элементом которого является периодический контроль и резервное копирование [1]. Известны два основных подхода к организации информационного резервирования в АСУ [2-4]. Первый подход связан с возникновением некоторого события информационно-вычислительного процесса. Недостатком подхода является сложность выбора подмножества контролируемых событий информационно-вычислительного процесса и возможность неограниченного роста моментов контроля и резервирования. По этой причине реализация подхода затруднена в период реальной эксплуатации АСУ при заданных ограничениях на ресурсы и время функционирования задачи.

Во втором подходе предполагается периодическая проверка ресурсов АСУ через детерминированные промежутки времени, что согласуется с календарными планами, позволяет учесть имеющиеся ограничения на ресурсы, но не полностью отражает стохастическую природу возникновения разного рода ошибок и инцидентов. Важно, что по ряду субъективных факторов в эргатических системах сложно вообще организовать периодический контроль через строго заданные промежутки времени. В связи с указанным, представляет интерес подход, позволяющий учесть случайные внешние факторы непрерывной работы АСУ при заданных временных и экономических ограничениях.

В общем плане периодический контроль и резервирование ресурсов АСУ включает выполнение ряда стандартных процедур:

- выполнение резервного копирования на случай отказа,
- контроль ошибок программного обеспечения (ПО),
- контроль ошибок среды функционирования.

Разработка стохастических и детерминированных моделей периодического контроля и резервирования составляет основное содержание работы.

Процедуры резервного копирования

Процедуры резервного копирования обеспечивают восстановление нормального функционирования системы в случае отказа и инцидента. При этом восстановление происходит с момента последнего резервного копирования (*рисунок 1*) [3].

Задача управления механизмом резервного копирования сводится к разработке модели выставления так называемых контрольных точек (КТ), минимизирующей математическое ожида-

Известия
ИНСТИТУТА ИНЖЕНЕРНОЙ ФИЗИКИ

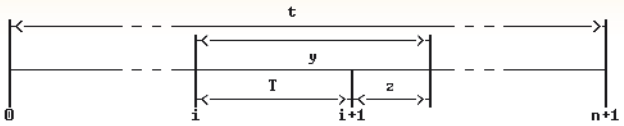

Рис. 1. Диаграмма функционирования программы с использованием механизма контрольных точек

ние времени задержки работы программы при ограничениях на общее время работы ПО и число КТ. Вопросы минимизации математического ожидания времени задержки за счет изменения частоты выставления КТ и величины детерминированного интервала между КТ рассмотрены в [2-4]. Рассмотрим ситуацию, когда интервал является случайной величиной.

Поток отказов считаем простейшим с плотностью распределения интервала $\hat{y}$ между отказами:

$$g_{\hat{y}} = \lambda^{-\lambda y},$$

где λ – интенсивность отказов.

Зададим стохастическую модель резервного копирования. В этом случае резервное копирование производится определенное число раз с равной вероятностью независимо друг от друга. Таким образом, образованный всеми КТ ограниченный поток является потоком Бернулли с плотностью распределения интервала $\hat{T}$ между КТ:

$$f_{\hat{T}} = n/t(1-T/t)^{n-1},$$

где n – число контрольных точек.

Можно показать, что значение времени задержки $\hat{z}=\hat{y}-\hat{T}$ является функцией двух случайных величин и имеет следующее математическое ожидание:

$$M_{\hat{z}}^{s} = \iint_{(s)} (y-T)\frac{n}{t}\left(1-\frac{T}{t}\right)^{n-1} \lambda e^{-\lambda y} dT dy,$$

где n – число моментов контроля среды;
λ – интенсивность отказов системы.

Область интегрирования S удобно представить в графическом виде (*рисунок 2*). Определив пределы интегрирования и упростив, получим следующее выражение:

$$M_{\hat{z}}^{s} = \int_0^t n/t(1-T/t)^{n-1}\frac{e^{-\lambda T}}{\lambda}\,dT -$$

$$-\int_0^{t/2} n/t(1-T/t)^{n-1} e^{-2\lambda T}\left(T+\frac{1}{\text{Л}}\right) dT - b_1,$$

где $b_1 = \frac{e^{-\lambda t}}{2^n}\left(\frac{1}{\lambda} + nt/(2n+2)\right)$.

Разложив в ряд подынтегральные выражения, получим приближенное значение математического ожидания времени задержки:

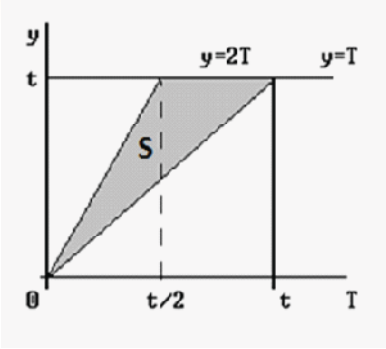

Рис. 2. Область интегрирования интервала времени задержки функционирования программы

$$M_{\hat{z}}^{s} \approx n\sum_{i=0}^{n-1}\sum_{j=0}^{r}(-1)^{j+i}C_{n+1}^{i}\frac{\lambda^j t^j b_2}{j!} - b_1, \quad (1)$$

где

$$b_2 = \frac{1}{(\lambda(i+j+1))} - \frac{t}{2^{i+2}(i+j+2)} - \frac{1}{2^{i+1}\lambda(i+j+1)},$$

r – число итераций.

Для сравнения полученной стохастической модели (1) с детерминированной моделью рассмотрим последнюю подробнее. В детерминированной модели КТ образуют регулярный поток с постоянной величиной интервала $T = \frac{t}{n+1}$. Плотность распределения времени задержки будет следующей:

$$g_{\hat{z}} = \lambda e^{-\lambda(T+z)}.$$

Можно показать, что выражение для математического ожидания времени задержки в детерминированной модели имеет вид:

$$M_{\hat{z}}^{d} = \frac{e^{-\lambda T}}{\lambda}(1 - e^{-\lambda T}(\lambda T + 1)). \quad (2)$$

Сравнивая выражения (1) и (2), получаем критерий, позволяющий сделать выбор той или иной модели при конкретных значениях λ,t и n:

$$M_{\hat{z}}^{s}(z) \lessgtr M_{\hat{z}}^{d}(z).$$

Считая время выставления КТ и рестарта мгновенным, получим модель общего времени работы ПО при наличии механизма КТ:

$$t'(n) = t + (n+1)M_{\hat{z}},$$

где t – время работы ПО;
n – число контрольных точек;
$M_{\hat{z}} = max\left(M_{\hat{z}}^{s}(z), M_{\hat{z}}^{d}(z)\right)$ – математическое ожидание времени задержки работы ПО в случае отказа.

Процедуры контроля ошибок программного обеспечения

Рассмотрим процесс функционирования ПО с учетом проводимого периодического контроля на предмет ошибок. При разработке расчет-

ных выражений будем придерживаться подхода, приведенного в предыдущем разделе.

Поскольку период времени t функционирования ПО во много раз превышает время контроля, положим последнее мгновенным. Тогда безотказность функционирования ПО характеризуется вероятностью $P(\hat{z}<Q)=F_{\hat{z}}(Q)$ того, что время обнаружения ошибки в межконтрольном интервале T не превосходит допустимое время Q работы системы при наличии ошибки. Фрагмент периодического контроля представлен на *рисунке 3*.

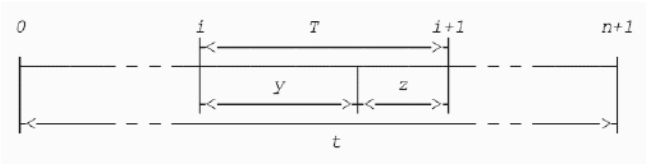

Рис. 3. Фрагмент периодического контроля программы

Полагая, что поток ошибок считаем простейшим, можно показать, что величина задержки $\hat{z}=\hat{y}-\hat{T}$ является функцией двух случайных величин и имеет следующую функцию распределения:

$$F_{\hat{z}}^{s} = \iint_{(s)} n/t(1-T/t)^{n-1}\,\lambda e^{-\lambda y} dT dy\,.$$

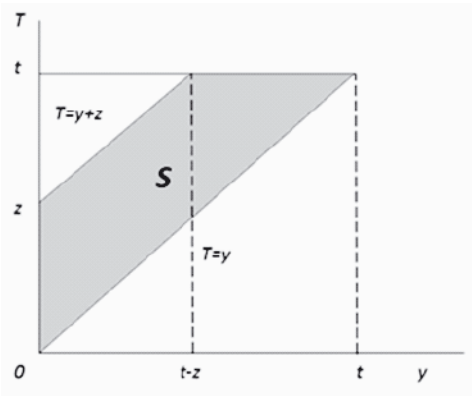

Рис 4. Область интегрирования интервала задержки времени обнаружения ошибки

Определив пределы интегрирования (*рисунок 4*), получим:

$$F_{\hat{z}}^{s} = \int_{0}^{t-z}\left(\int_{y}^{y+z} n/t(1-T/t)^{n-1}\,\lambda e^{-\lambda y}\,dT\right)dy +$$

$$+\int_{t-z}^{t}\left(\int_{y}^{t} n/t(1-T/t)^{n-1}\,\lambda e^{-\lambda y} dT\right)dy.$$

После упрощения имеем следующее выражение:

$$F_{\hat{z}}^{s} = \lambda/t^{n}\,(\int_{0}^{t-z} e^{-\lambda y}((t-y)^{n}-(t-z-y)^{n})\,dy +$$

$$+\int_{t-z}^{t} e^{-\lambda y}((t-y)^{n})\,dy).$$

Разложив в степенной ряд подынтегральные выражения, получим приближенное значение функции распределения, которое и является основным расчетным соотношением:

$$F_{\hat{z}}^{s} \approx \lambda \sum_{i=0}^{n}\sum_{j=0}^{r}\sum_{l=1}^{n+j+1}(-1)^{i+j+l+1}\times$$

$$\times C_{n}^{i}C_{n+j+1}^{l}\frac{\lambda^{j}t^{j+1-l}z^{l}}{j!\,(1+j+i)}\,, \qquad (3)$$

где r – число итераций.

Для сравнения стохастической модели обнаружения ошибок (3) с детерминированной рассмотрим последнюю подробнее. В детерминированной модели моменты контроля образуют регулярный поток с постоянной величиной интервала $T=t/(n+1)$ и плотностью распределения времени обнаружения ошибки:

$$g_{\hat{z}} = \lambda e^{-\lambda(T-z)};\ 0<z<T.$$

Можно показать, что выражение для функции распределения в детерминированной модели имеет следующий вид:

$$F_{\hat{z}}^{d} = e^{-\lambda T}(e^{\lambda z}-1);\ 0<z<T. \qquad (4)$$

Сравнивая выражения (3) и (4), можно говорить о соответствии рассмотренных моделей процессу появления ошибок (при заданных значениях λ, Q, t и n):

$$F_{\hat{z}}^{s}(z) \lesseqgtr F_{\hat{z}}^{d}(z).$$

Вероятность P_{n}^{p} обнаружения ошибок за t время решения задачи можно представить следующим образом:

$$P_{n}^{p} = (n+1)\cdot F_{\hat{z}},$$

где n – число моментов контроля;

$F_{\hat{z}} = max\left(F_{\hat{z}}^{s}(z), F_{\hat{z}}^{d}(z)\right)$.

Анализ рассмотренных моделей показал преимущество стохастической модели при небольшом числе моментов контроля. Понятийно это может быть объяснено тем, что даже при малом числе случайных моментов контроля программных ресурсов и процессов АСУ всегда существует вероятность того, что обнаружение ошибки будет произведено сразу же при ее возникновении, в то время как при использовании детерминированной модели период проверки не может быть меньше заданной величины.

Процедуры контроля ошибок среды функционирования

Требования к контролю среды задаются стандартами серии ИСО 15408. Выявление и локализация ошибок среды позволяет исключить появление ошибок программных ресурсов АСУ, касающихся внешнего интерфейса ПО. В этом

Известия
ИНСТИТУТА ИНЖЕНЕРНОЙ ФИЗИКИ

смысле процедуры обнаружения ошибок среды можно интерпретировать как механизм предупреждения ошибок ПО.

Рассмотрим работу АСУ при наличии механизма предупреждения ошибок ПО. В процессе работы системы через некоторые промежутки времени T осуществляется диагностика наиболее важных с точки зрения надежности компонентов среды функционирования (например, сетевых интерфейсов, системных таблиц, цепочек общей памяти и др.). При выявлении нарушения запускается программа обслуживания ошибок среды функционирования.

Будем считать, что безошибочность функционирования ПО характеризуется вероятностью $P(\hat{z} < Q) = F_{\hat{z}}(Q)$ того, что время предварительного контроля $\hat{z}$ между моментом контроля среды и возможным моментом наступления ошибки ПО не превосходит допустимое время Q. Зададим стохастическую модель контроля ошибок среды (*рисунок 5*).

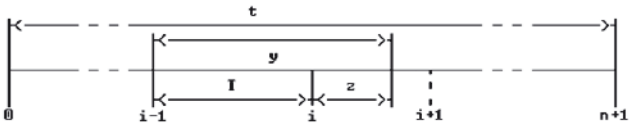

Рис 5. Диаграмма функционирования системы при наличии механизма предупреждения ошибок

Можно показать, что величина времени предварительного контроля является функцией двух случайных величин $\hat{z}=\hat{y}-\hat{T}$ и имеет следующую функцию распределения:

$$F_{\hat{z}}^{s} = \iint_{(s)} n/t(1-T/t)^{n-1}\,\lambda e^{-\lambda y} dT dy\ ,$$

где n – число моментов контроля среды;
λ – интенсивность ошибок ПО.

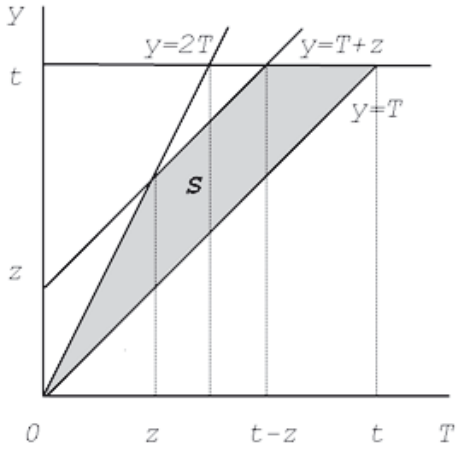

Рис 6. Область интегрирования интервала времени предупреждения ошибки

Определив пределы интегрирования (*рисунок 6*) и упростив выражение, получим:

$$F_{\hat{z}}^{s} = \int_0^z n/t(1-T/t)^{n-1}\, e^{-\lambda T}\left(1-e^{-\lambda T}\right) dT +$$
$$+\int_z^{t-z} n/t(1-T/t)^{n-1}\, e^{-\lambda T}(1-e^{-\lambda z})dT +$$
$$+\int_{t-z}^{t} n/t(1-T/t)^{n-1}\, e^{-\lambda T} dT - e^{-\lambda t}(\frac{z}{t})^n \quad ,$$

Разложив в степенной ряд подынтегральные выражения, получим приближенное значение функции распределения, которое является основным расчетным соотношением:

$$F_{\hat{z}}^{s} \approx n\sum_{i=0}^{r}\left(\sum_{j=0}^{n-1} b_1\, b_2\right) - e^{-\lambda t}(\frac{z}{t})^n \quad , \qquad (5)$$

где r – число итераций;

$$b_1 = (-1)^{-I+J} C_{n-1}^{i}\, \frac{\lambda^j}{(j!\, t^{i+1}(i+j+1))}\ ;$$

$$b_2 = t^{i+j+1} - z^{i+j+1}\,(2^j - e^{-\lambda z})(t-z)^{i+j+1}\, e^{-\lambda z}\ .$$

Сравним полученную стохастическую модель предупреждения ошибок с детерминированной. В детерминированной модели моменты контроля образуют регулярный поток с постоянной величиной интервала $T=t/(n+1)$ и следующей плотностью распределения времени предварительного контроля:

$$g_{\hat{z}} = \lambda e^{-\lambda(T+z)}\ .$$

Следовательно, выражение для функции распределения в детерминированной модели будет иметь следующий вид:

$$F_{\hat{z}}^{d} = e^{-\lambda T}(1-e^{-\lambda z});\ 0<z<T. \qquad (6)$$

Сравнивая выражения (5) и (6), при заданных значениях λ, Q, t и n получаем критерий, позволяющий сделать выбор той или иной модели:

$$F_{\hat{z}}^{s}(z) \lesseqgtr F_{\hat{z}}^{d}(z)).$$

Вероятность P_n^e предупреждения ошибок за t период времени работы АСУ можно представить следующим образом:

$$P_n^e = (n+1)\cdot F_{\hat{z}}\ ,$$

где n – число моментов контроля;

$$F_{\hat{z}} = max\left(F_{\hat{z}}^{s}(z), F_{\hat{z}}^{d}(z)\right).$$

Управление непрерывностью функционирования системы

Выбор модели (стохастической или детерминированной) и числа моментов контроля и резервного копирования позволяет управлять уровнем устойчивости, целостности и доступности системы. Например, с учетом рассмотренных процедур можно определить коэффициент

оперативной готовности системы:

$$К^{ог} = \left(\frac{t}{\left(t + M^{r}_{n_r}\right)}\right)\left(p + (1-p)\left(P^{e}_{n_e} + \left(1 - P^{e}_{n_e}\right)P^{p}_{n_p}\right)\right),$$

где – время решения задачи;

$M^{r}_{n_r}$ – математическое ожидание времени задержки работы программы в случае n_r-моментов резервного копирования;

p – вероятность безошибочной работы ПО (степень отлаженности ПО);

$P^{e}_{n_e}$ – вероятность предупреждения ошибок в случае n_e-моментов контроля среды;

$P^{p}_{n_p}$ – вероятность обнаружения ошибок в случае n_p-моментов контроля ПО.

Заключение

В работе рассмотрены стохастические и детерминированные модели резервированного копирования и контроля АСУ, учитывающие ограничения на время и ресурсы. Представление моментов резервирования и контроля в виде ограниченного потока Бернулли позволяет получить случайные временные интервалы при заданном числе этих интервалов, что позволяет учесть стохастические внешние факторы на процесс работы системы.

Сравнительный анализ стохастических и детерминированных моделей показал эффективность первых при малом числе моментов контроля и резервирования. Поэтому при управлении устойчивостью АСУ численными методами можно определить предпочтительные модели (стохастическую, детерминированную либо комбинированную), повышающие уровень устойчивости функционирования АСУ. Это дает эффект, подобный введению структурной избыточности, то есть можно говорить об особом виде избыточности - стохастической, использование которой практически не увеличивает затрат [5]. Для удобства применения стохастических моделей в технических системах можно использовать генератор случайных импульсов, позволяющий формировать случайные ограниченные потоки Бернулли [6].

Аналогичный подход был положен в основу решения задачи оценки эффективности механизма диагностики сбоев информационных массивов [7, 8]. Помимо области контроля и резервированного копирования ресурсов АСУ изложенные результаты могут быть полезны при оценке экономической эффективности реализуемых мер и механизмов контроля в различных технических системах, системах менеджмента, а также при инспекционном контроле [9].

Литература

1. Р 50-54-82-1988. Рекомендации. Надежность в технике. Выбор способов и методов резервирования / Г.Н. Черкесов, А.М. Половко, И.Б. Челпанов, А.И. Кубарев, В.Л. Аршакуни, Ю.Д. Литвиненко. М.: ВНИИНМАШ, 1988. 46 с.

2. Дорохов А.Н., Керножицкий В.А., Миронов А.Н., Шестопалова О.Л. Обеспечение надежности сложных технических систем. СПб.: Лань, 2011. 352 с.

3. Кузовлев В.И., Шкатов П.Н. Математические методы анализа производительности и надежности САПР. М.: Высшая школа, 1990. 142 с.

4. Розенберг Е.Н., Шубинский И.Б. Методы и модели функциональной безопасности технических систем. М.: ВНИИАС, 2004. 188 с.

5. Марков А.С. Решение вычислительной задачи при наличии временных ограничений // Известия высших учебных заведений. Приборостроение. 1992. Т. 35, №5. С. 54-57.

6. Генератор случайных импульсов: А.с. № 840856 СССР, М.Кл3, G 07 C 15/00. / В.А.Керножицкий и др. Заявл. 06.10.78; опубл. 25.06.81. Бюлл.23.

7. Марков А.С. К вопросу об обеспечении бесперебойной работы электронного архива // Наука и образование: электронное научно-техническое издание. 2011. №7. С. 1-8.

8. Markov A., Kernozitsky B. Economically effective data bases diagnostics method // Advances in Modeling and Analysis B: Signals, Information, Data, Patterns.1995. Vol. 33, No.1-3, P. 5-12.

9. Марков А.С., Маслов В.Г., Олексенко И.А., Цирлов В.Л. Тестирование и испытания программного обеспечения по требованиям безопасности информации // Известия Института инженерной физики. 2009. №2(12). С. 2-6.