УДК 681.3

ОЦЕНКА ФУНКЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ ДУБЛИРОВАННЫХ ВЫЧИСЛИТЕЛЬНЫХ СИСТЕМ

В.А. Богатырев, С.В. Бибиков

Предложена уточненная оценка функциональной безопасности дублированной вычислительной системы с учетом периодичности контроля и возможности перехода в опасное состояние из-за необнаружения отказа одной из машин системы.
Ключевые слова: безопасность, опасный отказ, защищенный отказ, дублированная система.

Задача обеспечения высокой надежности компьютерных систем, связанных с безопасностью, в том числе на транспорте, требует оценки интегральной и функциональной безопасности. Под интегральной понимается безопасность всей системы управления, а под функциональной – безопасность подсистемы, обеспечивающей безопасность [1]. В двухмашинных компьютерных системах, связанных с безопасностью, все вычисления, как правило, дублируются, при этом реализуется взаимоконтроль машин, основанный на сравнении результатов, а также на периодическом тестировании, проверке контрольных сумм и других методах [2–4]. Для дублированных систем к опасным состояниям относят состояния с отказом двух машин (с отказом процессора или памяти в каждой из них), так как при отказе одной из машин в результате взаимоконтроля этот отказ будет обнаружен и система переведена в защищенное (безопасное) состояние.

Вероятности опасного и безопасного отказа, интенсивность опасных отказов и среднее время до опасного отказа дублированной системы определяют [2] следующим образом:

$$Q_{\text{оп}}(t) = (1-e^{-\lambda t})^2 \approx \lambda^2 t^2 ; \;\; P_{\text{Б}}(t) = 1-(1-e^{-\lambda t})^2 \cong 1-\lambda^2 t^2 ;$$

$$\lambda_{\text{оп}}(t) = -\frac{P'_{\text{Б2}\vee 2}(t)}{P_{\text{Б2}\vee 2}(t)} = \frac{2\lambda(1-e^{-\lambda t})}{2-e^{-\lambda t}} \cong 2\lambda^2 t ; \;\; T_{\text{оп}} = \int_0^\infty P_{\text{Б}}(t)dt = \int_0^\infty (2e^{-\lambda t} - e^{-2\lambda t})dt = \frac{2}{\lambda} - \frac{1}{2\lambda} = \frac{3}{2\lambda},$$

где λ – суммарная интенсивность отказов одного компьютера (включая отказы процессора, оперативной памяти и постоянной памяти, используемой для начальной загрузки).

Для уточнения оценки будем рассматривать в качестве опасного не только состояние с отказом двух каналов устройства, но и с отказом одного канала при необнаружении средствами контроля соответствующего отказа. Показатели безопасности дублированной системы в этом случае определим как

$$Q_{\text{оп}}(t) = (1-e^{-\lambda t})^2 + 2(1-e^{-\lambda t})e^{-\lambda t}(1/(2^m-1)) ; \; T_{\text{оп}} = \int_0^\infty P_{\text{Б}}(t)dt = \int_0^\infty (1-((1-e^{-\lambda t})^2 + 2(1-e^{-\lambda t})e^{-\lambda t}(1/(2^m-1)))dt ,$$

где $1/(2^m-1)$ вероятность не обнаружения ошибки при контрольном суммировании. Учитывая, что при отсчете каждого периода контроля $i\tau$ (i = 1, 2, …) возможен переход в состояние опасного отказа или отсчет следующего (i+1)-го интервала, среднее время до опасного отказа определим как

$$T_{\text{оп}} = \tau Q_{\text{оп}}(t) \sum_{i=1}^{\infty} (i+1)\left(1-Q_{\text{оп}}(t)\right)^i .$$

Расчетами установлено, что при периодичности контроля τ = 15 с и λ = $0{,}2245\cdot10^{-6}$; $6{,}209\cdot10^{-6}$; $20{,}9\cdot10^{-6}$ 1/ч среднее время до опасного отказа равно соответственно $T_{\text{оп}} = 3{,}18\cdot10^{15}$; $6{,}11\cdot10^{12}$; $5{,}46\cdot10^{11}$ ч, что показывает высокую безопасность исследуемых систем. Дополнительно увеличить надежность и безопасность дублированных вычислительных систем при необходимости можно в результате их реконфигурации [5, 6].

Таким образом, предложена оценка функциональной безопасности дублированных вычислительных систем с учетом периодичности контроля и возможности необнаружения отказа одной из машин комплекса, что исключает требуемый переход системы в защищенное состояние.

1. ГОСТ Р МЭК 61508-1-2007. Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью. Часть 1. Общие требования. – Введ. 27.12.2007. – М.: Госстандарт России. – 96 с.
2. Сапожников В.В., Сапожников В.В., Шаманов В.И. Надежность систем железнодорожной автоматики, телемеханики и связи. – М.: Маршрут, 2003. – 263 с.
3. Богатырев В.А., Башкова С.А., Беззубов В.Ф. Надежность дублированных вычислительных комплексов // Научно-технический вестник СПбГУ ИТМО. – 2011. – № 6. – С. 74–78.
4. Богатырев В.А., Богатырев С.В., Богатырев А.В. Оптимизация кластера с ограниченной доступностью кластерных групп // Научно-технический вестник СПбГУ ИТМО. – 2011. – № 1. – С. 63–67.
5. Bogatyrev V.A. Exchange of Duplicated Computing Complexes in Fault tolerant Systems // Automatic Control and Computer Sciences. – 2011. – V. 46. – № 5. – P. 268–276.
6. Богатырев В.А. Отказоустойчивость вычислительных систем с функциональной реконфигурацией // Приборы и системы. Управление, контроль, диагностика. – 2001. – № 11. – С. 51–53.

Богатырев Владимир Анатольевич – Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики, доктор технических наук, профессор, Vladimir.bogatyrev@gmail.com
Бибиков Сергей Викторович – ООО "Центр речевых технологий", зам. техн. директора, bibikov@speechpro.com