



УДК 621.3.019.3

А.В. ФЕДУХИН, В.П. ПАСЬКО

К ВОПРОСУ О КОЛИЧЕСТВЕННЫХ ХАРАКТЕРИСТИКАХ БЕЗОТКАЗНОСТИ ИЗБЫТОЧНЫХ КОМПЬЮТЕРНЫХ СИСТЕМ

Анотація. Розглянуті питання оцінки безвідмовності надлишкових комп'ютерних систем з різними структурними схемами надійності. Розроблено базову модель безвідмовності надлишкової системи з використанням DN-розподілу та класифікацію систем на її основі.

Ключові слова: безвідмовність, надлишкова структура, базова модель, класифікація структур.

Аннотация. Рассмотрены вопросы оценки безотказности избыточных компьютерных систем с различными структурными схемами надежности. Разработаны базовая модель безотказности избыточной системы с использованием DN-распределения и классификация систем на ее основе.

Ключевые слова: безотказность, избыточная структура, базовая модель, классификация структур.

Abstract. The issues of evaluation reliability of redundant computer systems with different structural schemes of reliability are regarded. A basic model of redundant systems reliability using DN-distribution and systems classification on it basis is developed.

Keywords: reliability, redundant structure, basic model, structures classification.

1. Введение

При проектировании высоконадежных отказоустойчивых компьютерных систем необходимо введение различных форм избыточности. Высокая надежность и крайняя чувствительность безотказности таких систем и их характеристик предполагает широкое использование методов моделирования: аналитического, статистического и имитационного.

Аналитической моделью является символическое и математическое представление объекта, используемое для целей прогнозирования, оценки и контроля. Основными критериями качества модели являются адекватность представления объекта (насколько правильно она может описать зависимость свойств объекта от некоторых параметров), удобство использования и способность получить полезные результаты. Модели чрезвычайно полезны для принятия архитектурных решений, касающихся проектирования высоконадежных отказоустойчивых компьютерных систем.

В работе предлагается аналитическая модель для различных избыточных систем, так называемая базовая модель, которую возможно использовать в процессе проектирования для сравнения различных вариантов реализации систем.

2. Базовая модель безотказности систем

Автоматическая реконфигурация, использующая резервные модули, возможна с использованием специально спроектированных восстанавливающих органов (ВО), отказы которых, в принципе, не отличаются от отказов модулей. Отказы ВО препятствуют их правильному функционированию. Несмотря на то, что не все отказы ВО являются катастрофическими для системы в целом, ВО следует защищать от отказов и делать их максимально надежными. Для описания безотказности модулей введем следующие обозначения:

s – количество резервов, изначально доступных для подключения;

q – количество модулей одного типа, работающих параллельно (характеристика актуальна для систем, производительность которых зависит от количества одновременно работающих ресурсов);

c – степень компенсации последствий отказа [1] (условная вероятность того, что при возникновении отказа в работающей системе последняя способна восстановить информацию и продолжить ее обработку без долговременной потери данных);

f – способность модуля допускать f одиночных отказов до того, как он станет неработоспособным.

Способность системы восстанавливаться после отказа модуля и продолжать работу характеризуется степенью компенсации c . Для простоты это значение c будет использоваться для первых отказов из f в том же модуле и для $f + 1$ отказа, при котором восстановление осуществляется с использованием нового модуля. Восстановление – это важный вопрос, который должен решать разработчик системы [1]. В некоторых ситуациях восстановление означает выявление, локализацию и автоматическое исправление аппаратного отказа.

В других ситуациях восстановление может включать реставрацию оперативных данных, потерянных при отказе (в этом случае степень компенсации, как вероятность сохранения работоспособности после отказа, будет ниже, чем в предыдущем случае).

Основной характеристикой безопасности системы будем считать вероятность безотказной работы за время t ($R(t)$). Для удобства анализа и систематизации значений каждой функцию безотказности будем записывать в форме базовой модели ${}^f_c R_s^q$ [1].

$${}^f_c R_s^q = c^s (1 - {}^f F_s^q), \quad (1)$$

где ${}^f F_s^q$ – функция вероятности отказа.

Принимая гипотезу о DN -распределении наработки до отказа элементов, модулей и системы в целом, вероятность отказа будем вычислять следующим образом [2]:

$${}^f F_s^q = DN(x; v, f, q, s),$$

где v – коэффициент вариации наработки до отказа;

x – относительная наработка ($x = \frac{t}{T}$, t – время работы, T – средняя наработка до отказа (на отказ).

Функция вероятности отказа для DN -распределения имеет следующий вид:

$$DN(x; v) = \Phi\left(\frac{x-1}{v\sqrt{x}}\right) + \exp(2v^{-2})\Phi\left(-\frac{x+1}{v\sqrt{x}}\right),$$

где $\Phi(*)$ – функция нормированного нормального распределения.

Если любой из параметров базовой модели (1) типа вероятность безотказной работы ${}^f_c R_s^q$ опускается, то по умолчанию предполагается $q = 1$, $c = 1$, $f = 0$, $s = 0$. Параметры s , c и f являются параметрами, увеличение которых приводит к увеличению общей безотказности системы.

3. Критерий сравнения систем

Средняя наработка (MTBF), как характеристика безотказности отказоустойчивой системы, часто не является эффективным средством сравнения конфигураций высоконадежных систем [1]. Причина в том, что средняя наработка до отказа исчисляется для интервала

$0 \leq t \leq \infty$, а в действительности функционирование самовосстанавливающей системы происходит в области $0 \leq t \leq T$, где T – среднее время выполнения основной функции. Дело в том, что безотказность всегда достаточно высока ($R > 0,9$) и то, что случается с ней при $t > T$, не особенно интересно для понимания основного назначения системы [1].

В качестве критерия сравнения конфигураций систем с позиций надежности в [1] предлагается характеристика I – отношение отрезков времени, по истечении которых вероятности безотказной работы конкурирующих конфигураций систем равны вероятности безотказной работы, установленной в спецификации $R_{\text{спец}}(t)$.

Иными словами, сравнение систем осуществляется на основе вычисления соотношения отрезков времени функционирования (I), в течение которых достигается заданный уровень безотказности.

$$I = \frac{t_B}{t_A},$$

где t_A – время достижения $R_A(t_A) = R_{\text{спец}}$;

t_B – время достижения $R_B(t_B) = R_{\text{спец}}$.

Характеристику I назовем относительным критерием безотказности и проанализируем его эффективность.

Пусть две системы A и B имеют характеристики безотказности $R_A(t)$ и $R_B(t)$, и пусть $R_A(t) \geq R_{\text{спец}}$ для $0 \leq t \leq t_A$ и $R_B(t) \geq R_{\text{спец}}$ для $0 \leq t \leq t_B$.

Теперь $I = \frac{t_B}{t_A}$ характеризует улучшение (ухудшение) времени исправного функционирования системы B относительно системы A для определенного уровня безотказности $R_{\text{спец}}$.

Из-за того, что $R_A(t_A) = R_B(t_B) = R_{\text{спец}}$, функции для R_A и R_B могут быть заменены их значениями, и результирующие уравнения решены относительно I . В некоторых случаях результирующие уравнения или невозможно получить в аналитике, или они являются слишком сложными для анализа и сравнения вариантов конфигураций систем.

Пример 1. Определить время достижения системой вероятности безотказной работы $R_{\text{спец}}$ и вычислить критерии I для различных конфигураций резервированных систем (рис. 1).

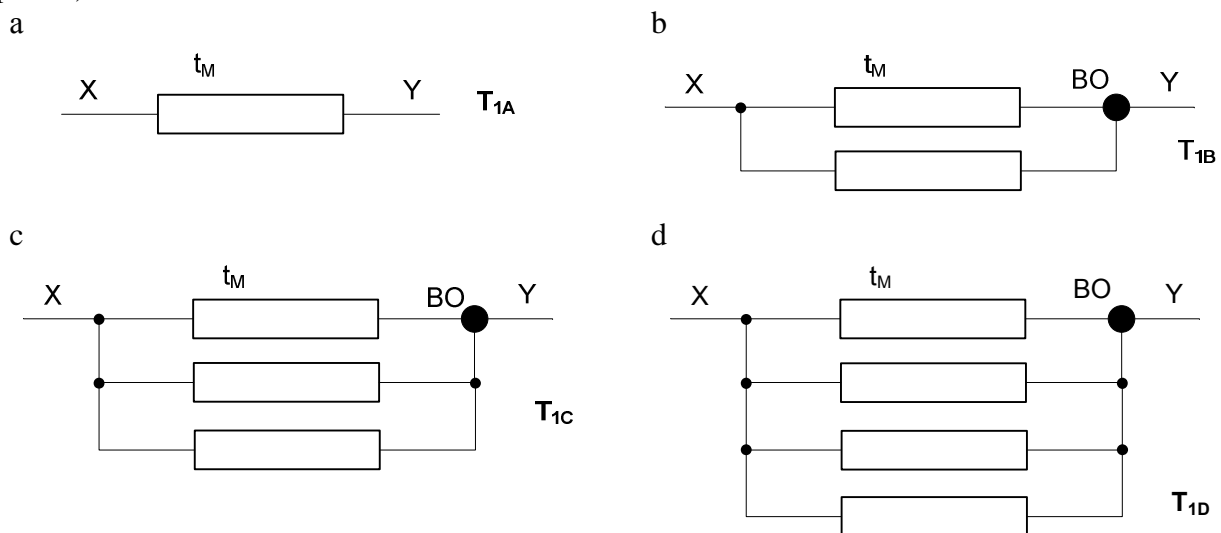


Рис. 1. Структуры резервированных систем

Исходные данные: средняя наработка до отказа модуля $t_M = 1000\text{ч}$, $\nu = 0,75$, $R_{\text{спец}} = 0,99$.

Решение:

1. Нерезервированная система.

Вычислим $F_{\text{спец}} = 1 - R_{\text{спец}} = 0,01$.

По таблицам DN -распределения [2, 3] определяем $x = 0,19$. Вычисляем среднюю наработку до отказа системы $T_{1A} = t_M$.

Так как $x = \frac{t_A}{T_{1A}}$, $t_A = x \cdot T_{1A} = 190\text{ч}$.

2. Дублированная система.

Вычислим среднюю наработку до отказа системы $T_{1B} = t_M \sqrt{n} = 1410\text{ч}$.

$$x = \frac{t_B}{T_{1B}}, t_B = 267,9\text{ч}.$$

3. Троирированная система.

Вычислим среднюю наработку до отказа системы $T_{1C} = t_M \sqrt{n} = 1730\text{ч}$.

$$x = \frac{t_C}{T_{1C}}, t_C = 328,7\text{ч}.$$

4. Четверированная система.

Вычислим среднюю наработку до отказа системы $T_{1D} = t_M \sqrt{n} = 2000\text{ч}$.

$$x = \frac{t_D}{T_{1D}}, t_D = 380\text{ч}.$$

Вычислим критерий I для отказоустойчивых систем относительно нерезервированной системы.

$$I_1 = \frac{t_B}{t_A} = 1,41, I_1 = \frac{t_C}{t_A} = 1,73, I_1 = \frac{t_D}{t_A} = 2.$$

Анализ критериев I показывает, что дублированная система в 1,41 раза более безотказна, чем нерезервированная система, троированная – в 1,73 раза и т.д.

Пример 2. Вычислим критерий I для системы типа " k из n " (рис. 2).

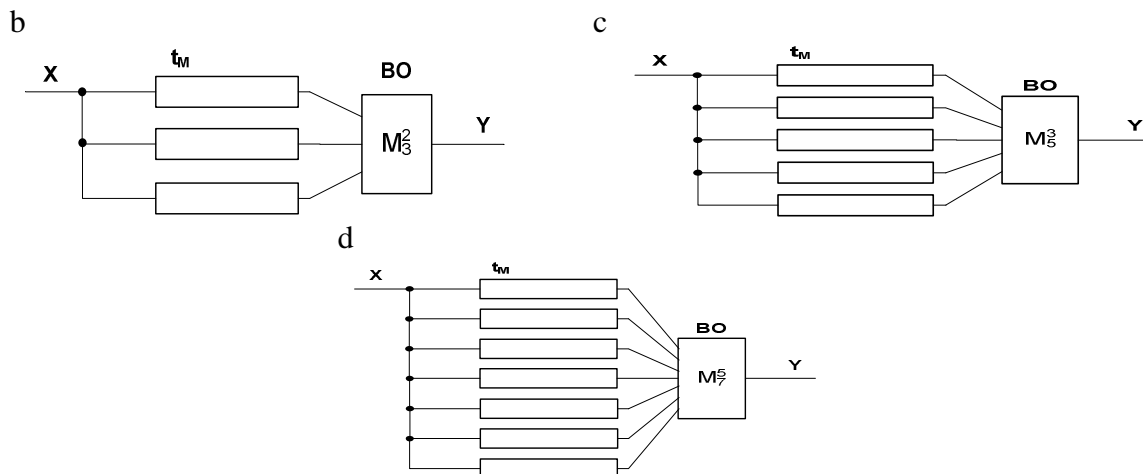


Рис. 2. Структуры систем типа " k из n "

Решение:

1. Система "k из n" (k = 2, n = 3) с ВО типа M₃².

$$T_{1B} = \frac{t_M(n-k+1)}{\sqrt{n}} = 1156ч, x = \frac{t_B}{T_{1B}}, t_B = 219,6ч.$$

2. Система "k из n" (k = 3, n = 5) с ВО типа M₅³.

$$T_{1C} = \frac{t_M(n-k+1)}{\sqrt{n}} = 1339ч, x = \frac{t_C}{T_{1C}}, t_C = 254,4ч.$$

3. Система "k из n" (k = 5, n = 7) с ВО типа M₇⁵.

$$T_{1D} = \frac{t_M(n-k+1)}{\sqrt{n}} = 1132ч, x = \frac{t_D}{T_{1D}}, t_D = 215,1ч.$$

Вычислим критерий I для отказоустойчивых систем типа "k из n" относительно резервированной системы.

$$I_1 = \frac{t_B}{t_A} = 1,156, I_2 = \frac{t_C}{t_A} = 1,339, I_3 = \frac{t_D}{t_A} = 1,13.$$

Анализ критериев I показывает, что при n > 5 безотказность систем типа "k из n" падает. Системы типа "k из n" уступают по безотказности системам с «горячим» резервированием при одинаковых аппаратных затратах на их реализацию (I₁ = 1,156 и I₂ = 1,73).

В этом случае оценка средней наработки до отказа вычисляется следующим образом:

$$T_1 = t_M \sqrt{n} = (t_M \sqrt{f}) \cdot \sqrt{n}$$

при t_M = 1000ч, f = 3, n = 2.

$$T_1 = 1000\sqrt{3}\sqrt{2} = 1000 \cdot 1,73 \cdot 1,41 = 2439ч.$$

4. Классификация типов конфигураций систем

Перечень типов конфигураций систем приведен в табл. 1. Для каждой из рассмотренных конфигураций систем поставим в соответствие запись базовой модели безотказности типа вероятность безотказной работы системы в виде ${}^f R_s^a$. При этом сформулируем следующее примечание.

Примечание 1. Если модуль системы является избыточным и спроектирован как f – безотказный автомат, то в пределах f отказов f = 1, 2, 3... и c = 1.

Таблица 1. Классификация типов конфигураций систем

Класс	Подкласс	Обозначение структурной схемы надежности системы	Обозначение характеристики	
			Базовая модель	Без учета Примечание 1
1	2	3	4	5
I			${}^f R_0^1$	${}^0 R_1^1$

II			${}^f_1 R_1^2$	${}^0_1 R_1^2$
	IIa		${}^f_0 R_1^2$	${}^0_0 R_1^2$
III			${}^f_1 R_2^3$	${}^0_1 R_2^3$
	IIIa		${}^f_0 R_2^3$	${}^0_0 R_2^3$
IV			${}^f_1 R_1^3$	${}^0_1 R_1^3$
V			${}^f_1 R_2^5$	${}^0_1 R_2^5$

Оценка базовой модели безотказности для различных классов систем в рамках гипотезы о DN -распределении наработки до отказа имеет вид (1)

$${}_c^f R_s^q = c^s (1 - {}^f F_s^q) = c^s [1 - DN(x; v, f, q, s)].$$

Пример 3. Вычислить ${}_c^f R_s^q$ системы III класса для следующих исходных данных: $n = 3, c = 1, q = 3, s = 2, f = 0, t = 200 \text{ ч}, t_M = 1000 \text{ ч}, v = 0,75$.

Решение:

1. Вычислим среднюю наработку до отказа системы:

$$T_1 = t_M \sqrt{n} = 1000 \cdot 1,73 = 1730 \text{ ч}.$$

2. Вычислим величину относительной наработки x :

$$x = \frac{t}{T_1} = \frac{200}{1730} = 0,11.$$

3. По таблицам DN -распределения [2,3] вычислим вероятность отказа:

$${}^0 F_2^3 = 0,00032.$$

Вычисляем базовую модель безотказности:

$${}^0 R_2^3 = c^2 (1 - {}^0 F_2^3) = 1^2 (1 - 0,00032) = 0,9997.$$

Рассмотрим более подробно оценку характеристики c . Определение степени компенсации c представляет собой условную вероятность того, что при возникновении отказа в работающей системе она (система) способна восстановить утраченную информацию и продолжить ее обработку без длительной потери работоспособности.

В некоторых ситуациях восстановление может означать только выявление, локализацию и автоматическое исправление аппаратного отказа, в других ситуациях оно может включать также очень сложную реставрацию базы данных. В первом случае c выше, чем во втором.

Таким образом, для систем II, III, IV, V классов величина c приближается к 1 и ограничивается диагностическими и коммутационными возможностями ВО и его надежностью. Для систем подклассов IIa и IIIa величина c значительно ниже, так как вероятность потери информации при ненагруженном («холодном») резервировании достаточно высока. Характеристика c изменяется путем добавления дополнительного оборудования к модулю и может быть доведена до 1, при этом аппаратная надежность модуля уменьшается. Поэтому для получения более достоверной оценки c необходимо провести анализ диагностических и коммутационных возможностей ВО и вычислить его вероятность безотказной работы R_{BO} . При этом всегда будет иметь место неравенство $c \leq R_{BO}$.

Характеристика f зависит от уровня избыточности, заложенного при проектировании в модуль. Если при проектировании модуля использованы методы синтеза f -безотказных цифровых автоматов [4], то, в принципе, можно спроектировать автомат с любым уровнем отказоустойчивости f . Причем исследованиями установлено, что при одном и том же уровне отказоустойчивости f аппаратная реализация f -безотказного автомата оказывается более простой, чем простое f -

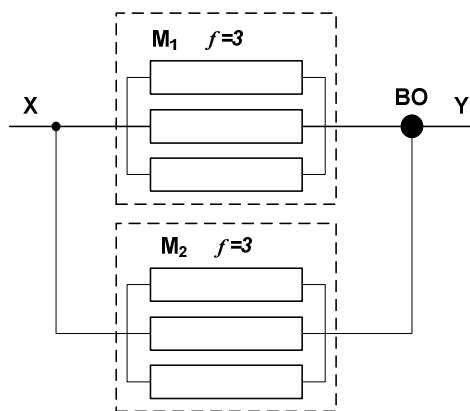


Рис. 3. Структурная схема дублированной системы с f -безотказными модулями ($f = 3$)

резервирование. Однако в первом приближении структурная схема системы с f -безотказными модулями будет иметь, например, следующий вид (рис. 3).

Покажем влияние изменения c на безотказность конкурирующих систем. Для этого воспользуемся исходными данными предыдущего примера.

Пример 4. Рассмотрим две системы II и III классов. Вычислим базовые модели безотказности:

1. Система II класса:

$$T_1 = t_M \sqrt{n} = 1000 \cdot \sqrt{2} = 1410 \text{ ч},$$

$$x = \frac{t}{T_1} = \frac{200}{1410} = 0,14,$$

$${}^0F_1^2 = 0,00194; c = 0,8,$$

$${}_{0,8}R_1^2 = c^1(1 - {}^0F_1^2) = 0,8^1 \cdot 0,99806 = 0,79845.$$

2. Система III класса:

$$T_1 = t_M \sqrt{n} = 1000 \cdot \sqrt{3} = 1730 \text{ ч},$$

$$x = \frac{t}{T_1} = \frac{200}{1730} = 0,11,$$

$${}^0F_1^2 = 0,00032, c = 0,8,$$

$${}_{0,8}R_2^3 = c^2(1 - {}^0F_2^3) = 0,8^2 \cdot 0,99968 = 0,63979.$$

Анализ результатов показывает, что при низкой степени компенсации ($c = 0,8$) более избыточная система III класса оказывается менее надежной, чем система II класса.

Определим, при каком значении c система III класса станет более надежной, чем система II класса.

В табл. 2 приведены результаты расчетов базовой модели безотказности системы для различных значений c .

Таблица 2. Результаты расчетов базовой модели безотказности системы

Класс системы	Характеристика c	${}_c^f R_s^q$ системы
II	0,9	0,89825
	0,95	0,94816
	0,99	0,98808
	0,995	0,99307
	0,999	0,99706
III	0,9	0,80974
	0,95	0,90221
	0,99	0,97979
	0,995	0,98971
	0,999	0,99768

5. Выводы

Анализ полученных результатов позволяет сделать следующий вывод: система III класса является более надежной по сравнению с системой II класса только при степени компенсации, близкой к 1 ($c = 0,999$). При меньшей степени компенсации система II класса является более надежной, чем система III класса.

Каждый раз, когда степень компенсации оказывается недостаточно высокой, добавление разумного количества дополнительного оборудования для повышения степени компенсации является в целом эффективным. И тот факт, что каждый индивидуальный модуль становится более ненадежным через привлечение дополнительного оборудования, является менее решающим, чем увеличение степени компенсации c .

Чрезмерная чувствительность вариантов отказоустойчивых систем к параметрам c и f предполагает тщательный, хорошо продуманный процесс моделирования и анализа перед техническим проектированием.

Для систем, которые должны работать с высоким уровнем безотказности в течение длительного времени, восстановление за счет резерва имеет наибольший потенциал. Однако расчеты показывают, что степень компенсации, определенная как вероятность восстановления системы после отказа, является единственной важнейшей характеристикой безотказной системы. Изменение степени компенсации от 1 до 0,98 может привести к снижению безотказности системы на несколько порядков. Большинство методов повышения безотказности системы (например, добавление резервных модулей) являются неэффективными по сравнению с методами повышения степени компенсации. Добавление проверок, диагностик и т.п. для увеличения степени компенсации является наиболее преобладающим. Точная оценка степени компенсации c трудна и требует точного измерения влияния ошибок компонентов на работоспособность модулей. Это предполагает широкое применение методов моделирования на всех этапах проектирования системы.

Так как средняя наработка до отказа (МТBF) не является достаточно эффективной характеристикой для сравнения отказоустойчивых систем, то в дополнение к этой характеристике предлагается использовать базовую модель типа вероятности безотказной работы и отношение отрезков времени работоспособности для достижения заданного уровня безотказности (I).

СПИСОК ЛИТЕРАТУРЫ

1. Bouricius W.G. Reliability modeling techniques for SELF – Repairing computer Systems / Bouricius W.G., Carter W.C., Schneider P.R. – New-York: IBM Watson Research Center Yorktown Heights, 1969. – P. 295 – 309.
2. Стрельников В.П. Оценка и прогнозирование надёжности электронных элементов и систем / В.П. Стрельников, А.В. Федухин. – К.: Логос, 2002. – 486 с.
3. Федухин А.В. К вопросу о табулировании функций распределения отказов / А.В. Федухин, Н.В. Сеспедес-Гарсия // Математичні машини і системи. – 2006. – № 2. – С. 147 – 152.
4. Сапожников В.В. Методы синтеза надёжных автоматов / В.В. Сапожников, Вл.В. Сапожников. – Л.: Энергия, 1980. – 96 с.

Стаття надійшла до редакції 05.10.2011