На правах рукописи

НА ДОМ НЕ ВЫДАЕТСЯ

КАМЛЕХ Харб

КОМПЛЕКСНЫЕ МОДЕЛИ АНАЛИЗА И ОБЕСПЕЧЕНИЯ ОТКАЗОУСТОЙЧИВОСТИ БОРТОВЫХ ВЫЧИСЛИТЕЛЬНЫХ СИСТЕМ

Специальность – 05.13.15 - Вычислительные машины и системы

АВТОРЕФЕРАТ

диссертации на соискание ученой степени

кандидата технических наук

Москва 2004

Работа выполнена в Московском государственном техническом университете им. Н. Э. Баумана.

Научный руководитель: кандидат технических наук,

доцент Воробьев Г. Н.

Официальные оппоненты: доктор технических наук,

профессор Бархоткин В. А.

Д 1668339

Камлех Харб
Комплексные модели анализа и обеспечения отказоустойчивости бортовых вычислительных систем
2004 0-00

ехнических наук,

дведев Н. В.

Ведуг И " Аргон ", г. Москва

Защи 19 2004г. в 14 30 на заседа-
нии диссе Московском государственном
005, Москва, 2-я

Д 1668339

ВОЗВРАТИТЕ КНИГУ НЕ ПОЗЖЕ
обозначенного здесь срока

, просьба высы-

юсковс

ванов С. Р.

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Актуальность темы. Непрерывно возрастающие требования к задачам, решаемым современными комплексами бортового оборудования летательных аппаратов различного назначения, приводят к усложнению комплексов, к необходимости применения в составе этих комплексов современных вычислительных систем, использующих последние достижения электронной промышленности. Усложнение комплексов, увеличение количества и усложнение выполняемых ими функций выдвигает на первый план проблемы контроля работоспособности и комплексной обработки информации с целью повышения надежности, улучшения точностных и динамических характеристик комплексов. Так, например, согласно инструкции FAA Advisory Circular 25.1309.1A бортовые вычислительные системы должны выполнять свои функции с вероятностью наработки на отказ 10^{-9} за час полета.

Разработке методов обеспечения отказоустойчивости вычислительных систем (ВС) посвящено достаточно много работ российских и зарубежных исследователей. Большой вклад в развитие этих методов вносят как российские ученые – К. А. Иыуду, В. В. Липаев и др., так и зарубежные - Ж. К. Лапри, Ж. Д. Мусса, А. Авижиенис, Б. Ранделл, и др.

Результаты анализа существующих методов обеспечения отказоустойчивости показывают, что модели, учитывающие взаимосвязь поведения аппаратных и программных составляющих вычислительных систем в нештатных ситуациях, в настоящее время практически отсутствуют. Кроме того, известные модели не являются полными в связи с тем, что они не учитывают ряд параметров, существенно влияющих на корректное поведение ВС.

Теоретические исследования, направленные на обеспечение отказоустойчивости ВС, сдерживаются как отсутствием алгоритмов разработки решающих блоков, так и отсутствием методов для исследования влияния связанных неисправностей между версиями программного обеспечения (ПО).

Поэтому тема диссертационной работы, посвященной разработке моделей и методов анализа и обеспечения отказоустойчивости вычислительных систем реального времени с учетом аппаратных и программных составляющих ВС, является актуальной. Эта актуальность растет по мере расширения сфер применения и повышения требований к уровню отказоустойчивости и защищенности вычислительных систем. Актуальной также является разработка как алгоритмов для построения решающих блоков, необходимых для обеспечения надежности отказоустойчивых вычислительных систем, так и методов для исследования влияния связанных неисправностей между версиями программного обеспечения, поскольку доля отказов, обусловленных программными

МГТУ им. Н. Э. Баумана БИБЛИОТЕКА

проектными неисправностями, представляет приблизительно 60% неисправностей ВС.

Целью диссертационной работы является исследование и разработка комплексных методов анализа и обеспечения отказоустойчивости бортовых вычислительных систем, учитывающих надежность аппаратного и программного обеспечения.

В соответствии с поставленной целью исследования проводились по следующим основным направлениям:

- Анализ существующих методов обеспечения гарантоспособности вычислительных систем реального времени;
- Разработка моделей надежности мультипроцессорных вычислительных систем, учитывающих различные варианты размещения программных версий;
- Анализ методов и моделей обеспечения отказоустойчивости вычислительных систем;
- Разработка модели и исследование различных вариантов построения решающих блоков (РБ) отказоустойчивых вычислительных систем;
- Анализ методов повышения отказоустойчивости программного обеспечения и оценки их надежностных характеристик;
- Создание комплекса алгоритмов и программ анализа и оценки надежности различных структур отказоустойчивых вычислительных систем (ОУВС), учитывающих надежность аппаратного и программного обеспечения;

Методы исследования. В работе использованы методы теории вероятностей и математической статистики, теории марковских процессов, теории графов и теории надежности.

Научная новизна. Разработана комплексная модель надежности ОУВС, учитывающая надежностные характеристики аппаратного и программного обеспечения (АПО) и позволяющая исследовать влияние различных параметров АПО на отказоустойчивость вычислительной системы.

Разработана модель, учитывающая влияние связанных неисправностей между версиями программного обеспечения, и выработаны рекомендации по повышению отказоустойчивости вычислительных систем в таких ситуациях.

Разработана модель для исследования различных алгоритмов построения решающих блоков, позволяющая обоснованно выбирать структуру РБ и рассчитывать их вероятностные характеристики.

Предложены оригинальные алгоритмы построения РБ, упрощающие аппаратную реализацию и обладающие повышенной надежностью.

Получены оценки надежностных характеристик различных вариантов построения программного обеспечения, использующих блоки восстановления, N-вариантное программирование и N–самопроверяемое программирование. Даны рекомендации по построению программного обеспечения, обладающего повышенной отказоустойчивостью.

Практическая ценность. Разработанные модели и методы позволяют адекватно описывать поведение и структуры отказоустойчивых вычислительных систем с учетом надежностных характеристик аппаратного и программного обеспечения.

Предложены инженерные методики, позволяющие обоснованно выбирать структуру и конфигурацию аппаратного и программного обеспечения при проектировании ОУВС с заданными характеристиками.

На основе разработанных моделей и методов обеспечения отказоустойчивости разработан комплекс алгоритмов и программ анализа и оценки надежности различных структур ОУВС, учитывающих надежность аппаратного и программного обеспечения.

Внедрение результатов работы. Полученные в диссертации результаты использованы в Научно-учебном комплексе «Информатика и системы управления» МГТУ им. Н.Э. Баумана при выполнении опытно-конструкторской работы по созданию отказоустойчивой цифровой вычислительной системы для бортового Фурье-спектрометра, предназначенного для длительного использования в составе научной аппаратуры космического аппарата «Метеор-М». Результаты использованы при разработке ОУВС реального времени в научно-исследовательском центре и в университете Алеппо (Сирия), а также в учебном процессе при чтении лекций и проведении лабораторных работ по курсу "Управляющие ЭВМ и системы" в МГТУ им. Н.Э. Баумана.

Апробация работы и публикации. По материалам диссертации опубликовано 4 научные работы.

Основные положения и результаты работы заслушивались и обсуждались в НИИ информатики и систем управления МГТУ им. Н.Э. Баумана, на заседании кафедры "Компьютерные системы и сети" МГТУ им. Н.Э. Баумана и на восьмой конференции сирийского компьютерного общества 2003 г. Алеппо (Сирия).

Структура и объем работы. Диссертационная работа состоит из введения, четырех глав, общих выводов, списка литературы и приложения. Она изложена на 121 машинописных листах. Содержит 56 рисунков, и 13 таблиц. Список литературы включает 92 наименования.

Содержание работы

Во введении обосновывается актуальность диссертационной работы, и формулируются основные цели и задачи работы. Рассматриваются методы исследований, раскрывается новизна и практическая ценность работы. Рассматриваются пути развития вычислительных средств, сфер их применения и вытекающие отсюда требования к вычислительным системам. Описывается структура и содержание диссертации.

В первой главе проведен анализ методов достижения гарантоспособности ОУВС, которая в настоящее время становится обобщенным комплексным показателем функциональной надежности вычислительных систем в условиях возникновения новых угроз надежности. Приведенная в работе классификация неисправностей и отказов позволяет упростить построение графа состояний исследуемой системы, особенно при возникновении связанных неисправностей между версиями ПО. Рассмотрены атрибуты гарантоспособности вычислительных систем, среди которых основное внимание в работе уделено надежности вычислительных систем.

Приведены основные методы достижения отказоустойчивости: предотвращение, устранение, прогнозирование неисправностей и обеспечение отказоустойчивости, которая реализуется обработкой ошибок и неисправностей. Обработка ошибок состоит из обнаружения, диагностирования ошибок и восстановления системы, основные методы которого были проанализированы. Приведены методы статического и динамического тестирования программного обеспечения.

Рассмотрены различные методы восстановления работоспособности ВС, такие как обратное, прямое восстановление и восстановление путем компенсации ошибок. Рассмотрены также различные методы устранения неисправностей на этапе проектирования ПО. Приведена классификация методов оценки надежности ВС.

Во второй главе разработана комплексная модель анализа и обеспечения отказоустойчивости ВС реального времени, которая учитывает взаимосвязь поведения аппаратных и программных составляющих ВС. Разработанная модель учитывает все параметры ВС, которые оказывают большое влияние на ее надежность.

Рассмотрены принципы выбора числа процессоров ОУВС, учитывая требования, как к надежности системы, так и к ее производительности.

Проведена оценка влияния связанных неисправностей между различными версиями программного обеспечения на надежность ПО. Показано, что в случае использования только копий программы увеличение числа копий не улучшает общую надежность вычислительной системы, а в случае использования различных версий ПО происходит заметное улучшение общей надежности системы.

Обозначим через x долю связанных ошибок между версиями программы. Тогда интенсивность ошибок программы ξ может быть записана как $\xi = (1-x)\xi + x\xi$, а вероятность безотказной работы (ВБР) одной версии программы равна $R = R^{1-x}R^{x}$. При наличии m параллельных версий программы ВБР программного обеспечения выражается как

$$R_n(x) = [1-(1-R^{1-x})^m]R^x,$$

На рис. 1 приведена зависимость коэффициента улучшения надежности ПО K от доли связанных неисправностей x в случае $m=3$, при этом K определяется следующим образом:

$$K = \frac{R_n(x) - R_n(1)}{R}100\%.$$

Здесь и далее $R_n(x)$ - ВБР программы в зависимости от x.

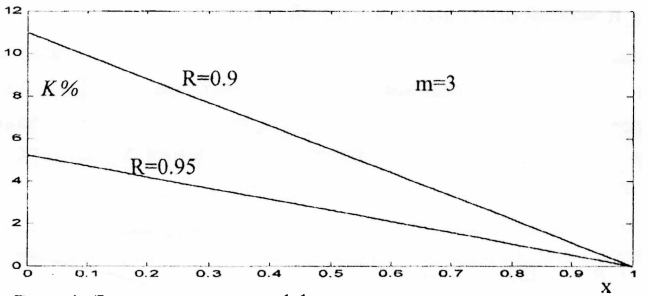

Рис. 1. Зависимость коэффициента улучшения надежности от доли связанных ошибок

Показано, что вторая версия улучшает надежность программы (ВБР которой R=0.95) на 5%, а третья - на 0.25% (относительно надежности программы с двумя версиями) и четвертая - только на 0.01% относительно надежности системы с тремя версиями. Поэтому выбор $m \geq 4$ нецелесообразен.

Рассмотрены варианты конфигурации отказоустойчивых вычислительных систем, состоящих из нескольких процессоров и программных версий. В общем случае аналитическая модель работы системы представляется в виде марковской модели древовидной структуры с непрерывным временем, описываемой системой обыкновенных дифференциальных уравнений следующего вида:

$$s\hat{p}_0(s) - p_0(0) = -n(\lambda+\gamma)\hat{p}_0(s) + \beta\hat{p}_1(s) + \eta\hat{p}_2(s);$$

$$s\hat{p}_1(s) - \hat{p}_1(0) = -((n-1)(\lambda+\gamma) + m\xi)\hat{p}_1(s) + n\lambda\hat{p}_0 + \beta\hat{p}_{12}(s) + \eta\hat{p}_{13}(s);$$

где: n - число процессоров; m - число программных версий в каждом процессоре; λ, γ - соответственно, интенсивность отказов и сбоев процессора; ξ - интенсивность ошибок программы; β, η- соответственно, интенсивность восстановления работы процессора после сбоя и восстановления работы программной версии; $\hat{p}_0(s)$- изображение по Лапласу вероятности отсутствия отказов в системе; $p_0(0)$- вероятность отсутствия отказов в системе в начальный момент времени; $\hat{p}_1(s)$- изображение по Лапласу вероятности отказа одного процессора; $p_1(0)$- вероятность наличия одного отказавшего процессора в системе в начальный момент времени; $\hat{p}_{12}(s)$- изображение по Лапласу вероятности отказа одного процессора и сбоя в другом процессоре и $\hat{p}_{13}(s)$- изображение по Лапласу вероятности отказа одного процессора и одной программной версии.

Систему обозначим символом $\{n/m\}$, где n, m, соответственно, число процессоров и версий программы в данной системе.

На основе разработанной модели в работе проведен детальный анализ надежности системы, состоящей из n процессоров ($n=\overline{1,3}$), каждый из которых имеет m – версий ПО ($m=\overline{1,3}$). На рис. 2 приведены зависимости вероятности отказа различных вариантов построения мультипроцессорной системы от времени.

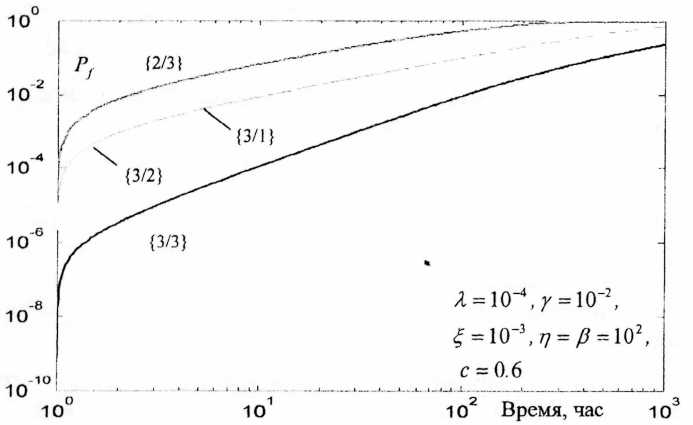

Рис. 2. Зависимость вероятности отказа различных вариантов построения системы от времени

Полученные результаты позволяют обоснованно выбирать тот или иной вариант технического решения в процессе проектирования и выбора конфигурации отказоустойчивой вычислительной системы.

Показано, что при определенных условиях, представление о независимости отказов аппаратуры и программного обеспечения в мультипроцессорных системах приводит к завышенной оценке надежности системы.

Полагая, что отказы программного обеспечения, аппаратуры и сбои аппаратуры являются событиями независимыми, вероятность отказа системы $\{3/1\}$, выраженная через вероятности $P_{f3/1\lambda}, P_{f3/1\xi}, P_{f3/1\gamma}$, учитывающие только λ, γ и ξ соответственно, запишется как

$$\begin{aligned} P_{f3/1} &= 1-(1-P_{f3/1\lambda})(1-P_{f3/1\xi})(1-P_{f3/1\gamma}) = \\ &= P_{f3/1\lambda}+P_{f3/1\xi}+P_{f3/1\gamma}-P_{f3/1\lambda}.P_{f3/1\gamma}-P_{f3/1\lambda}.P_{f3/1\xi}- \\ &-P_{f3/1\gamma}.P_{f3/1\xi}+P_{f3/1\lambda}.P_{f3/1\xi}.P_{f3/1\gamma}. \end{aligned} \quad (1)$$

Если $P_{f3/1\lambda} << 1, P_{f3/1\xi} << 1$ *и* $P_{f3/1\gamma} << 1$ то $P_{f3/1} \approx P_{f3/1\lambda}+P_{f3/1\xi}+P_{f3/1\gamma}$. (2)

В случае, если $P_{f3/1} \neq P_{f3/1\lambda}+P_{f3/1\xi}+P_{f3/1\gamma}$, то это означает, что отказы программ и аппаратуры и сбои аппаратуры зависимые случайные события и сумма $P_{f3/1\lambda}+P_{f3/1\xi}+P_{f3/1\gamma}$ (при допущении о независимости этих событий) дает лишь приближенную оценку надежности системы.

Исследована проблема увеличения значимости аппаратурных сбоев. Проблема становится более актуальной в связи с наметившейся тенденцией существенного превышения сбоев над отказами аппаратуры. На рис. 3 приведены зависимости вероятностей отказов системы {3/1} от ξ, γ и λ. Видно, что аппаратурные сбои сильно влияют на надежность системы.

На рис. 3 также показано, что учет программных и аппаратных ошибок совместно, дает более точную и достоверную оценку надежности системы.

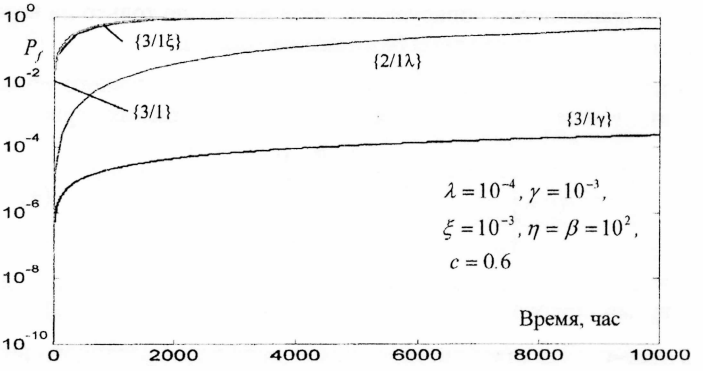

Рис. 3. Зависимость вероятности отказа системы {3/1} от времени

На основе разработанной модели получены зависимости надежности системы от интенсивностей отказов и сбоев аппаратуры и интенсивностей отказов программного обеспечения. Это позволяет обоснованно перераспределять требования к надежностным характеристикам аппаратного и программного обеспечения исходя из общих требований к надежности ОУВС.

На рис. 4 показана зависимость вероятности отказов системы {3/1} от интенсивности отказов процессора λ.

Это позволяет определить диапазон интенсивностей отказов аппаратуры и ошибок программы и аппаратуры, опасно влияющие на надежность системы с определенной вероятностью отказа.

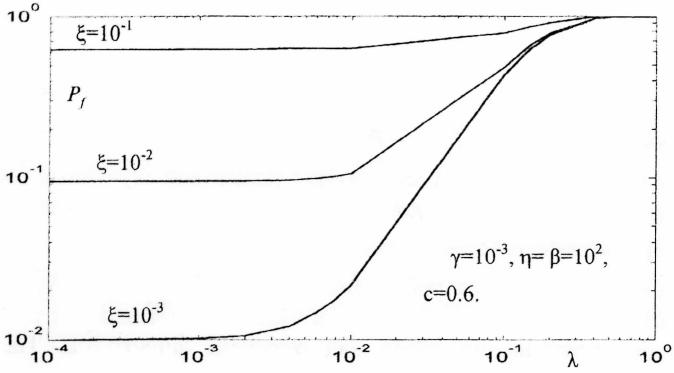

Рис. 4. Зависимость вероятности отказа системы {3/1} от интенсивности отказов аппаратуры

В работе исследована зависимость надежности системы от вероятности правильного обнаружения сбоя одного из двух процессоров c. Показано, что вероятность правильного обнаружения сбоя влияет не только на вероятность отказа системы, но и на ее время безотказной работы.

Показано, что в общем случае вероятность правильного обнаружения отказа зависит от текущего времени с момента наступления первого отказа t

$$c(t) = \begin{cases} 1 - \dfrac{(1-e^{-\lambda\tau}) - R^2(e^{\lambda\tau}-1)}{(1-R)^2} & t \geq \tau \\ 0 & t < \tau, \end{cases} \qquad (3)$$

где τ - время, требуемое для обнаружения отказа второго процессора с момента наступления отказа первого процессора в троированной системе.

Третья глава посвящена анализу и синтезу комплексных моделей работы системы, учитывающих характеристики средств контроля и

голосования в отказоустойчивых системах. Проведен сравнительный анализ четырех алгоритмов голосования:

1. Мажоритарного алгоритма голосования.

2. Алгоритма голосования на основе взвешенного среднего значения результатов версий программы.

3. Алгоритма голосования на основе метода медианой фильтрации.

4. Оценивающего или прогнозирующего алгоритма голосования.

При моделировании первых трех алгоритмов голосования для имитации результатов трех версий $x_1(t)$, $x_2(t)$, $x_3(t)$ на результат какой-то версии программы можно наложить помеху, время появления которой z распределено по показательному закону и ее амплитуда записывается выражением пуассоновского распределения

$$P(z) = \xi z e^{-\xi z}, \qquad (4)$$

где ξ - интенсивность ошибок версии программы.

Показано, что работа мажоритарного алгоритма голосования значительно зависит от порога голосования δ. На выходе этого алгоритма может происходить скачок с амплитудой $\leq 2\delta$ и возникнуть неопределенность, которая появляется когда расстояние между результатами версий больше порога голосования, т.е. $d(x_i, x_j) > \delta$, где x_k - результат k-и версии программы. Это позволяет обнаруживать связанные ошибки между версиями программного обеспечения. На рис. 5 показан результат работы такого алгоритма, где x_v - выход алгоритма голосования.

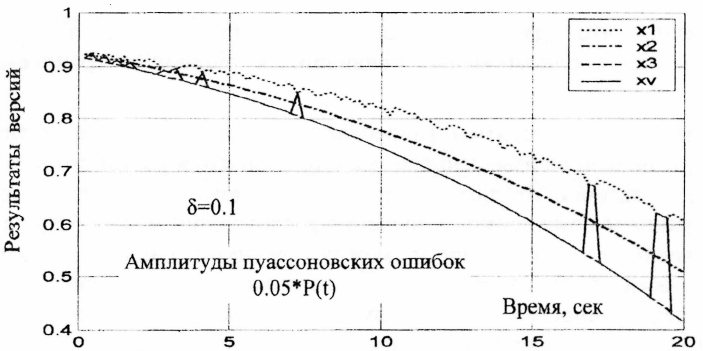

Рис. 5. Результат работы мажоритарного алгоритма голосования при значении порога δ=0.1 и при наличии помех на входе

Алгоритм голосования на основе взвешенного среднего значения результатов версий программы выбирает свой результат так, чтобы этот результат был самый близкий к двум ближайшим результатам версий.

Согласно алгоритму голосования на основе взвешенного среднего значения результатов версий программы выбирается значение x_v, которое минимизирует величину $J(x_v, d)$, т.е.

$$\min_d \; J(x_v, d) = \frac{1}{2}\int_I w_1(x_v - x_1)^2 + w_2(x_v - x_2)^2 + w_3(x_v - x_3)^2\, dt, \qquad (5)$$

где w_1, w_2 и w_3 взвешивающие коэффициенты.

Получена следующая зависимость для вычисления x_v

$$x_v = \sum_i w_i x_i \Big/ \sum_i w_i\,, \qquad (6)$$

которая позволяет оптимизировать результат по заданному критерию.

Значения взвешивающих коэффициентов w_1, w_2 и w_3 вычисляются следующим образом. Выбираются два ближайших результата, а результатам остальных версий присваиваются взвешивающие коэффициенты, которые обратно пропорциональны их расстоянию до ближайших результатов. Метод достаточно прост в реализации, однако выдает результат, который может отличаться от результатов версии программы, а также выдает наибольшее число фатальных ошибок.

В общем случае, согласно алгоритму голосования на основе метода медианной фильтрации при наличии N результатов версии x_i $(i = \overline{1, N})$, выходом решающего блока является медиана, вычисляемая следующим образом:

$$x_{мед} = \begin{cases} x_{(N+1)/2} & N \text{ нечетное} \\ (x_{N/2} + x_{(1+N/2)})/2 & N \text{ четное} \end{cases} \qquad (7)$$

Показано, что данный метод может быть использован для маскирования двух одновременно появившихся ошибок в троированной системе.

Очевидно, что алгоритмы голосования на основе метода медианой фильтрации и на основе взвешенного среднего значения результатов версий программы, в отличие от алгоритма мажоритарного голосования, всегда выдают результаты независимо от значения расхождений между результатов версий. Зависимые неисправности между версиями сильно влияют на надежность всех трех алгоритмов голосования, так как при наличии зависимых неисправностей можно получать одинаковые, но неправильные результаты. Хотя зависимых неисправностей между независимо отлаженными версиями мало, целесообразно использовать алгоритм мажоритарного голосования вместе с приемочными испытаниями или алгоритм голосования на основе метода медианой фильтрации.

В случае, когда результаты двух или более версий программного обеспечения неправильные, предлагается использовать оценивающий или прогнозирующий алгоритм голосования. Согласно этому алгоритму

выполняется прогнозирование параметров путем применения метода наименьших квадратов, линейного прогноза или выполняется прогноз по методу Бурга. По сравнению с алгоритмом Бурга или алгоритмом линейного прогноза метод наименьших квадратов требует меньшего времени выполнения, однако является менее точным.

Проведенное в работе сравнение алгоритма линейного прогнозирования и алгоритма Бурга показало, что последний на несколько порядков точнее, чем алгоритм линейного прогнозирования. Кроме того, алгоритм линейного прогнозирования дает неправильные прогнозируемые значения, если количество заданных предыдущих значений мало.

Предложено несколько вариантов построения решающих блоков, формирующих решение на основе не всегда безошибочных результатов многоканальной обработки. Для двухпроцессорной системы синтезирована структура, вероятность отказа которой меньше вероятности отказа системы, состоящей из двух параллельных процессоров (если вероятность обнаружения отказа одного из двух процессоров меньше или равна 0.7). Предложенная структура использована при проектировании реальных ОУВС в научно-исследовательском центре (SSRC - Сирия) и позволили получить 10-15% повышение надежности систем.

Для трехпроцессорной системы получены различные решения, зависящие от того, проверяется ли работа двух процессоров путем сравнения их результатов одним из этих двух процессоров (т.е. *(a=b)a*), или третьим процессором (т.е. *(a=b)c*). На рис. 6. приведены зависимости вероятности безотказной работы этих вариантов от π, где π - вероятность того, что отказавший процессор выдает сигнал о том, что сравниваемые этим отказавшим процессором (например, а) результаты работы двух процессоров, например, а и b, отличаются друг от друга.

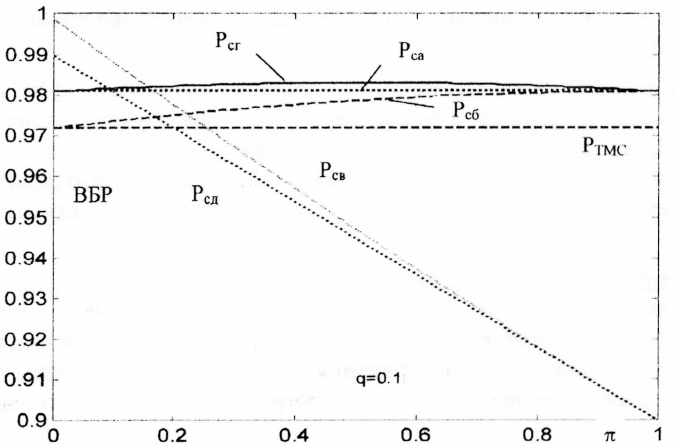

Рис. 6. Зависимости ВБР различных вариантов построения РБ от π

Кроме того, показано, что результаты работы системы зависят от того, результаты каких процессоров сравниваются и в какой последовательности, а также от числа сравнений. Через $P_{ca}, P_{cб}, P_{cв}, P_{cг}$ и $P_{cд}$ обозначим ВБР предложенных в работе различных вариантов построения ОУВС.

Показано, что ВБР троированной мажоритарной системы $P_{ТМС} = 1 - 3q^2 + 2q^3$ меньше ВБР двух из предлагаемых структур решающих блоков, в которых два процессора сравнивают результаты на одном из процессоров. В одной из предлагаемой структур выполняется два сранения (P_{ca}), а в другой – три. Последняя обладает наиболее высокой вероятностью безотказной работы - $P_{cг}$. На основе сравнения полученных результатов сделан вывод о целесообразности организации голосования средствами основных процессоров системы без привлечения дополнительных аппаратных средств.

В случае числа процессоров больше трех целью является обеспечение получения правильного результата при отказа не более заданного числа процессоров. Предложены и рассмотрены системы и возможности их аппаратной реализации.

В случае, если число процессоров более трех, предлагается использовать понятие d_0 – диагностируемости, которая определяется как возможность однозначного определения отказавших процессоров в многопроцессорной системе на основе взаимных проверок, при условии, что число отказавших процессоров не превышает d_0.

Предложены алгоритмы, реализующие кольцевые структуры с диагоналями. Показано, что реализация предложенных алгоритмов наталкивается на различные трудности не обеспечивая при этом значительного повышения надежности системы. Кроме того, наличие большого числа процессоров влечет за собой малую эффективность данного технического решения. Показано, что наибольшей эффективностью обладает система из трех процессоров.

В заключении главы показано, что наиболее простым и эффективным решением, является структура решающего блока, реализующая голосование типа 2 из 3, где два процессора сравнивают результаты на одном из этих процессоров путем выполнения двух сранений. Показано, что надежность такой структуры превышает надежность троированной мажоритарной системы.

Четвертая глава посвящена анализу некоторых вариантов программ, обеспечивающих отказоустойчивость ВС. Эти варианты программ используют: блоки восстановления (БВ), N-вариантное программирование (NBII) и N-самопроверяемое программирование (NСПП). Получены оценки надежности рассмотренных вариантов программ. Показано, что наиболее

высокой надежностью обладает вариант программы, использующий N-самопроверяемое программирование.

Основным недостатком программы, использующей блоки восстановления, является зависимость среднего времени выполнения программы $E[T_{БВ}]$ от наличия ошибок в алгоритмах и программах. Показано, что в блоках восстановления с двумя алгоритмами, зависимость среднего времени выполнения варианта программы, использующего блоки восстановления от вероятности успешного выполнения первого алгоритма p имеет линейный характер. На рис. 7а приведена такая зависимость для экспоненциального распределения времени выполнения двух алгоритмов T_1, T_2 с параметрами λ_1 и λ_2, а на рис. 7б – для равномерного распределения T_1, T_2 в интервале [a,b].

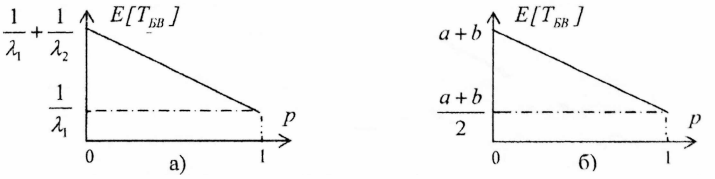

Рис. 7. Зависимость времени выполнения варианта программы, использующего блоки восстановления от вероятности успешного выполнения первого алгоритма

Получены выражения для вероятностей возникновения отказа каждого из рассматриваемых вариантов ПО Q_X, где $X \in [БВ, NСПП, NВП]$. Эти вероятности записываются следующими формулами

$$Q_{БВ} = q_{RVD,БВ} + q_{2V} + q_{ID,БВ} + q_{IV} q_{RVD,БВ} + q_{IV}^2 (1 - q_{ID,БВ}). \quad (8)$$

$$Q_{NСПП} = [4(q_{IV})^2 (1 - q_{IV})^2 + 4(q_{IV})^3 (1 - q_{IV}) + \\ + 4q_{2V}] p_{D,NСПП} + q_{2V} + 4q_{3V} + q_{4V} + q_{RVD,NСПП}. \quad (9)$$

$$Q_{NВП} = q_{D,NВП} + (3q_{2V} + q_{3V})(1 - q_{D,NВП}) + q_{RVD,NВП}., \quad (10)$$

где q_{IV}, $q_{ID,X}$ - вероятность независимой неисправности одной версии ПО и решающего блока соответственно; $q_{RVD,X}$ - вероятность связанной неисправности между версиями ПО и решающим блоком; $q_{iV,X}$ - вероятность связанной неисправности между i-ми версиями; $q_{D,X}$ - вероятность различных видов неисправностей, присущих решающему блоку.

На рис. 8. приведена зависимость вероятности отказа каждого из рассматриваемых вариантов программ, использующих БВ, NВП и NСПП от времени.

Из приведенных графиков следует, что наибольшей надежностью обладает вариант программ NСПП.

Показано также, что вероятности необнаруженных отказов рассматриваемых вариантов программ удовлетворяют уравнению

$$q_{U,NCПП} \le q_{U,NВП} << q_{U,БВ}, \qquad (11)$$

а вероятности обнаруженных отказов удовлетворяют другому уравнению

$$q_{d,БВ} < q_{d,NВП} < q_{d,NCCП}. \qquad (12)$$

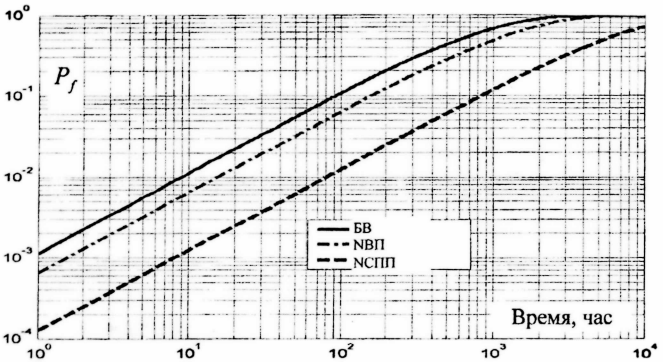

Рис. 8. Зависимость вероятности отказа вариантов программ, использующих БВ, NВП и NСПП от времени

Кроме того, вероятности независимых отказов решающих блоков трех вариантов программ удовлетворяют следующему уравнению

$$q_{ID,NCПП} \le q_{ID,NВП} << q_{ID,БВ}. \qquad (13)$$

На основе введения понятия степени отказоустойчивости в работе проанализированы системы со степенью отказоустойчивости к программным ($f_П = 1$) и аппаратным ошибкам ($f_A = 1$). Такие системы в работе обозначены как $X / f_П / f_A$, где $X \in$[БВ, NВП, NСПП].

На основе разработанной модели надежности рассматриваемых систем были получены выражения, описывающие интенсивности обнаруженных и необнаруженных сбоев программы $\xi_{d,X}$ и $\xi_{U,X}$.

Вероятности обнаруженных и необнаруженных связанных неисправностей между двумя версиями после отказа одной из трех версий систем (NВП/1/1, NСПП/1/1) $q_{d,2V}$ и $q_{U,2V}$ определяются выражениями

$$q_{d,2V} = 2q_{1,2V} - q_{1,2V}^2 + q_{ID,2V},$$

$$q_{U,2V} = q_{RVD,2V}. \qquad (14)$$

Используя уравнения (13), а также неравенство $q_{RVD,БВ} < q_{RVD,NBП} < q_{RVD,NCCП}$ можно записать $\xi_{м,БВ} >> \xi_{м,NBП}$ и $\xi_{м,БВ} >> \xi_{м,NCПП}$.

Вероятность обнаруженных отказов системы, использующей БВ, меньше вероятности обнаруженных отказов систем, использующих NCПП и NBП. Вероятность необнаруженных отказов систем, использующих NCПП и NBП, меньше вероятности обнаруженных отказов системы, использующей БВ.

Проведено моделирование отказоустойчивых систем, использующих блоки восстановления, N-самопроверяемое программирование и N-вариантное программирование. На рис. 9. показана вероятность отказов систем, использующих БВ, NCПП и NBП. Из графиков следует, что надежность систем, использующих N-самопроверяемое программирование и N-вариантное программирование на 20% превышает надежность системы, использующей блоки восстановления.

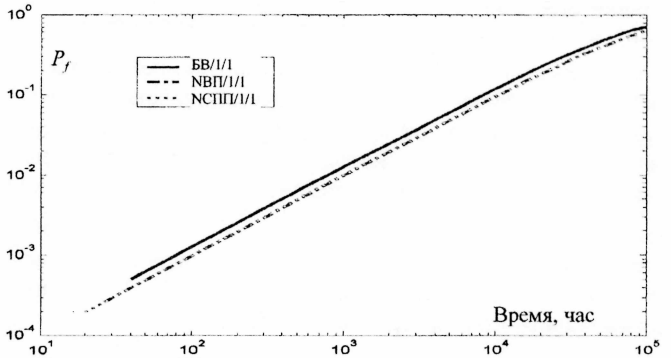

Рис. 4.14. Зависимость вероятности отказа систем БВ/1/1, NBП/1/1 и NCПП/1/1 от времени

Основные результаты диссертационной работы

1. Проведен анализ методов обеспечения гарантоспособности вычислительных систем реального времени. Предложена оригинальная классификация неисправностей и отказов ОУВС.
2. Разработаны модели надежности мультипроцессорных отказоустойчивых вычислительных систем с различными версиями программ, позволяющие оценивать комплексное влияние отказов аппаратуры и сбоев программы и аппаратуры и дающие более точную и достоверную оценку надежности системы. Модели позволяют обоснованно подходить к выбору архитектуры и организации ОУВС в процессе проектирования системы. На базе разработанных моделей исследовано влияние на надежность системы связанных неисправностей между версиями ПО, интенсивностей отказов аппаратного и программного обеспечения, получено выражение

для вероятности правильного обнаружения отказа второго процессора в троированной системе.

3. Разработана модель, учитывающая влияние связанных неисправностей между версиями программного обеспечения, и выработаны рекомендации по повышению отказоустойчивости вычислительных систем в таких ситуациях.

4. Разработана модель для исследования различных алгоритмов построения решающих блоков, позволяющая обоснованно выбирать структуру РБ и оптимизировать его вероятностные характеристики. Предложены оригинальные алгоритмы построения РБ, упрощающие аппаратную реализацию и обладающие повышенной надежностью.

5. Получены оценки надежностных характеристик различных вариантов построения программного обеспечения, использующих блоки восстановления, N-вариантное программирование и N-самопроверяемое программирование. Даны рекомендации по построению программного обеспечения, обладающего повышенной отказоустойчивостью.

6. Проведены сопоставительный анализ и синтез некоторых вариантов программ, обеспечивающих отказоустойчивость ВС: блоки восстановления, N-вариантное программирование и N-самопроверяемое программирование. Предложен метод для вычисления среднего времени выполнения варианта программы, использующего блоки восстановления.

7. На основе разработанных моделей и методов обеспечения отказоустойчивости разработан комплекс алгоритмов и программ анализа и оценки надежности различных структур ОУВС, учитывающих надежность аппаратного и программного обеспечения.

8. Предложенные модели использованы при проектировании реальных ОУВС в научно-исследовательском центре (SSRC - Сирия) и позволили получить 10-15% повышение надежности систем.

Публикации по теме диссертации

1. *Воробьев Г.Н., Камлех Х.* Интегрированная модель мультипроцессорных отказоустойчивых систем реального времени // Вестник МВТУ. Серия Приборостроение. – 2000. -№2. – С. 83-91.

2. *Kamleh H., Vorobiof G.N.* Fault-tolerance of real-time systems // Informatics (Damascus): Journal of Syrian Computer Society. – 1998. – Vol. 7, № 2. 65. – P. 156-163.

3. *Kamleh H.* Comparison of a voting algorithms for fault-tolerant real-time systems // Informatics (Damascus): Journal of Syrian Computer Society. – 1999. – Vol. 8, № 2. 74. – P .57-64.

4. *Kamleh H.* Fault-tolerance of critical systems // VIII Syrian computer society symposium. – Aleppo, 2003. – P 65-73.