На правах рукописи

УДК 681.323

Ле Куанг Минь

МЕТОДИКА И СРЕДСТВА ОБЕСПЕЧЕНИЯ ОТКАЗОУСТОЙЧИВОСТИ БОРТОВЫХ ВЫЧИСЛИТЕЛЬНЫХ СИСТЕМ РЕАЛЬНОГО ВРЕМЕНИ

Специальность: 05.13.15 – Вычислительные машины и системы

АВТОРЕФЕРАТ
диссертации на соискание ученой степени
кандидата технических наук

Москва – 2008

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

Научный руководитель: кандидат технических наук, доцент
Романовский Александр Сергеевич

Официальные оппоненты:

доктор технических наук, профессор
Шубинский Игорь Борисович,

кандидат технических наук, доцент
Медведев Николай Викторович

Ведущая организация: ФГУП НИИ «Аргон»

Защита состоится 26 июня 2008 года на заседании диссертационного совета Д 212.141.10 в Московском государственном техническом университете им. Н.Э. Баумана по адресу: 105005, г. Москва, 2-я Бауманская ул., д.5.

Отзыв на автореферат, заверенный печатью организации, просим присылать по адресу: 105005, г. Москва, 2-я Бауманская ул., д.5.

С диссертацией можно ознакомиться в библиотеке МГТУ им Н.Э.Баумана.

Автореферат диссертации разослан «___» мая 2008 г.

Ученый секретарь
диссертационного совета к.т.н., доцент С.Р.Иванов

ОБЩАЯ ХАРАКТЕРИТИКА РАБОТЫ

Актуальность проблемы. В настоящее время, вычислительная техника находит все более широкое применение в различных сферах человеческой деятельности. Особую актуальность приобретает использование вычислительных систем для управления ответственными объектами, работающими в режиме реального времени. К таким системам в первую очередь следует отнести системы управления атомными электростанциями, бортовые вычислительные системы, системы спутниковой связи и другие. Подобные системы должны обладать свойствами отказоустойчивости и живучести за все время их активного функционирования, поскольку их отказы могут быть весьма дорогостоящими и иметь опасные последствия.

С появлением вычислительных машин начались исследования в области повышения надежности их работы. В классических работах на эту тему намечены пути повышения надежности, заключающиеся в основном во введении различных форм избыточности (аппаратурной, функциональной, временной и др.). Эти исследования и полученные результаты базировались в основном на математических методах (теории вероятностей и математической статистики, теории случайных процессов, теории графов, исследовании операций и др.). В области космической физики были сформулированы представления и получены исходные экспериментальные данные о характеристиках радиационных поясов Земли, космических лучей и т.д. В области радиационной стойкости были разработаны методические подходы к заданию требований по радиационной стойкости интегральных микросхем, проведены исследования дозовых и временных эффектов в комплектующих элементах и аппаратуре в условиях воздействия ионизирующих излучений (ИИ). Однако, существующие методы обеспечения надежности не всегда достигали требуемых показателей надежности бортовых вычислительных систем. Кроме того, указанные методы не позволяли в необходимой мере учитывать влияние специфических воздействий внешней среды космического пространства, прежде всего, низкоинтенсивных ионизирующих излучений на надежность бортовых вычислительных систем.

С возникшей в последнее время потребностью увеличения сроков активного существования космических аппаратов эта проблема приобрела особую актуальность и значимость и стимулировала проведение подобных

исследований во многих странах. Так, в современных условиях конкурентоспособность и рентабельность проектов предоставления услуг космической связи определяют необходимость создания космических аппаратов со сроком активного существования 12 и более лет. Опыт, накопленный предприятиями космической отрасли, показал, что прогресс в создании космических аппаратов с такими сроками активного существования невозможен без изменения традиционного подхода к обеспечению отказоустойчивости бортовых вычислительных систем.

Указанные соображения определили важность и актуальность решаемой в диссертации научно-технической задачи - разработки методики и средств обеспечения отказоустойчивости бортовых вычислительных систем реального времени.

Цель диссертационной работы состоит в разработке методики и средств обеспечения отказоустойчивости бортовых вычислительных систем реального времени, позволяющих повысить надежности систем в условиях воздействия низкоинтенсивных ионизирующих излучений за счет использования резервирования, активной защиты от отказов и режима принудительного переключения резервных комплектов.

Для достижения поставленной цели решаются следующие задачи:

1. Сравнительный анализ существующих концепций обеспечения отказоустойчивого функционирования и принципов построения современных отказоустойчивых вычислительных систем.
2. Разработка методики обеспечения отказоустойчивости бортовых вычислительных систем с целью предотвращения сбоев или отказов, вызванных воздействием низкоинтенсивных ионизирующих излучений на элементы системы с традиционной схемой резервирования.
3. Организация активной защиты от отказов в бортовых вычислительных системах реального времени с целью обеспечения отказоустойчивости системы в условиях воздействия низкоинтенсивных ионизирующих излучений.
4. Оценка эффективности применения активной защиты от отказов в иерархических бортовых вычислительных системах.

Методы исследования, использованные в процессе выполнения диссертационной работы: имитационное моделирование, теория вероятностей, комбинаторный анализ, теория графов, теория случайных

процессов (марковские и полумарковские процессы), теория надежности технических систем.

Научная новизна диссертационной работы заключается в следующем:

- разработана методика построения отказоустойчивых вычислительных систем, использующая резервирование в нагруженном режиме и режим принудительного переключения резервных элементов, позволяющая обеспечить заданный уровень надежности системы в условиях воздействия ионизирующих излучений;

- разработана методика построения отказоустойчивых вычислительных систем, использующая механизм активной защиты от отказов и режим принудительного переключения резервных элементов, позволяющая повысить надежность бортовых вычислительных систем за счет предотвращения сбоев и отказов элементов системы, вызванных воздействием ионизирующих излучений;

- получены аналитические выражения для оценки вероятности безотказной работы системы активной защиты от отказов в общем случае для любого числа основных и дополнительных вычислительных модулей, позволяющие обосновано выбирать структуру системы, исходя из заданного значения вероятности безотказной работы.

Практическая ценность полученных в работе результатов состоит в том, что разработанные методики и средства организации активной защиты от отказов и принудительного переключения резервных комплектов в бортовых вычислительных системах могут быть использованы при разработке отказоустойчивых вычислительных систем, при проектировании вычислительных систем космического базирования, предназначенных для длительного использования в условиях воздействия низкоинтенсивных ионизирующих излучений.

Внедрение результатов работы: Полученные в диссертации результаты использованы в НИИ информатики и систем управления МГТУ им. Н.Э. Баумана при выполнении работы по созданию отказоустойчивой цифровой вычислительной системы для бортового Фурье-спектрометра, предназначенного для длительного использования в составе научной аппаратуры космического аппарата Метеор-3М.

Исходя из заданных требований к надежности всего прибора, путем моделирования с использованием разработанных в диссертации методов и

алгоритмов были выработаны рекомендации по построению отказоустойчивой цифровой вычислительной системы бортового Фурье-спектрометра.

Апробация работы и публикации. Тема и содержание диссертации отражены в 5 научных работах, из них по списку ВАК – 1 работа.

Основные положения и результаты работы заслушивались и обсуждались на научно-технических семинарах и заседаниях секции кафедры «Компьютерные системы и сети» МГТУ им. Н.Э. Баумана, на научно-технической конференции в МГТУ им. Н.Э. Баумана (Москва, 2005 г), 14-й всероссийской межвузовской научно-технической конференции студентов и аспирантов (Москва, 2007г)

Объем и структура диссертации.

Диссертация включает введение, четыре главы, выводы, список литературы из 103 наименований. Основная часть диссертационной работы изложена на 134 страницах и содержит 44 рисунки и 20 таблиц.

СОДЕРЖАНИЕ РАБОТЫ

Во введении обосновывается актуальность темы диссертационной работы, формулируется цель и основные задачи, перечисляются методы исследований, раскрывается новизна и практическая ценность работы, описывается структура и содержание диссертации.

В первой главе проведен обзор и анализ литературных данных по теме диссертации. Были проанализированы существующие концепции обеспечения отказоустойчивости вычислительных систем.

Рассмотрена проблема обеспечения отказоустойчивости бортовых вычислительных систем в условиях воздействия низкоинтенсивных ИИ. Проведен анализ результатов исследований, проведенных в МИФИ, РНЦ «Курчатовский институт» и др.

Было отмечено, что предельная накопленная доза интегральных микросхем в выключенном состоянии от 3 до 10 раз выше их предельной накопленной дозы в рабочем состоянии. В результате чего была обоснована необходимость разработки методики обеспечения отказоустойчивости бортовых вычислительных систем на основе совместного использования известных методов резервирования и режима принудительного переключения резервных комплектов.

Рассмотрены теоретические основы концепции активной защиты от отказов (АЗ) модульных вычислительных систем. АЗ предназначена для достижения требуемых уровней отказоустойчивости управляющих вычислительных систем реального времени в условиях незначительного резерва времени, ограниченной эффективности средств обнаружения неисправностей вычислителей системы, а также при условии, что объем резервного оборудования не должен превышать объем основного оборудования. Было отмечено, что в концепции АЗ хорошо использованы все известные подходы для обеспечения отказоустойчивости системы: динамическая реконфигурация, постоянный резерв, непостоянный резерв. Однако применение АЗ в бортовых вычислительных системах практически не исследовано в условиях воздействия ИИ. Кроме того, в известных работах по АЗ отсутствуют исследования по совместному применению АЗ и режима принудительного переключения резервных комплектов. Показана целесообразность проведения таких исследований и разработки методики построения отказоустойчивых вычислительных систем (ОУВС), использующей механизм АЗ и режим принудительного переключения резервных комплектов с целью предотвращения сбоев или отказов элементов систем, вызванных воздействием ИИ.

На основе анализа процедур обработки неисправности был построен граф состояний ОУВС. Граф отображает стратегию поведения ОУВС в случае возникновения сбоя или отказа. Была разработана математическая модель оценки надежности бортовых вычислительных систем на основе марковского процесса, которая может быть использована в дальнейших расчетах.

На основе результатов анализа сформулирована цель работы и определены задачи, которые необходимо решить для достижения поставленной цели.

Во второй главе рассмотрены традиционные схемы резервирования в условиях воздействия низкоинтенсивных ИИ, приведен анализ и оценка эффективности различных методов резервирования.

Установлено, что вероятность безотказной работы $R_{ИИ}(t)$ одного элемента в условиях воздействия низкоинтенсивных ИИ определяется выражением:

$$R_{ИИ}(t) = e^{-\lambda \cdot t} \cdot (2 - e^{(K_p \cdot P \cdot t)^2}), \qquad (1)$$

где, λ - интенсивность отказа элемента;

K_p – коэффициент радиационного повреждения интегральных микросхем данного элемента, [$рад^{-1}$];

$D(t) = P \cdot t$ – доза, накопленная за время эксплуатации (T_{CAC}) при постоянной интенсивности, равной произведению мощности излучения *P[рад/ч]* на время облучения *t [ч]*.

Рассмотрены традиционные схемы резервирования с ненагруженным, нагруженным и сеансовым режимами. Для случая, когда в системе работает один основной элемент с одним резервным элементом, в условиях воздействия низкоинтенсивных ИИ были получены аналитические выражения для оценки ВБР системы в рассмотренных режимах.

Было получено выражение для ВБР системы дублирования в ненагруженном режиме:

$$R_{ненагр.,ИИ}(t) \approx e^{-\lambda \cdot t} \cdot (\frac{1}{30} \cdot \lambda \cdot (\eta \cdot k_a)^4 \cdot t^5 - \frac{1}{6} \cdot (\eta \cdot k_a)^4 \cdot t^4 - \frac{2}{3} \cdot \lambda \cdot (\eta \cdot k_a)^2 \cdot t^3 + \lambda \cdot t + 1), \qquad (2)$$

где k_a - коэффициент аппроксимации а $\eta = K_p \cdot P$.

Выражения для ВБР системы дублирования в нагруженном и сеансовом режимах записываются в виде:

$$R_{нагр.,ИИ}(t) = 1 - (1 - e^{-\lambda \cdot t} \cdot (2 - e^{(K_p \cdot P \cdot t)^2}))^2, \qquad (3)$$

$$R_{сеанс,ИИ}(t) = e^{-\frac{1}{2}\lambda \cdot t} \cdot (2 - e^{(\frac{K_p \cdot P \cdot t}{2})^2}), \qquad (4)$$

Анализ результатов, полученных по формулам (2-4), показывают, что ВБР системы дублирования в нагруженном режиме уменьшается на 3% в условиях воздействия ИИ при T_{CAC} = 7лет. Для систем дублирования с нагруженным и ненагруженным режимами значения ВБР быстро уменьшаются при заданных значениях коэффициентов K_p и *P*.

Рассмотрена задача анализа и оценки эффективности резервирования, с использованием понятия значимости элемента в системе. В результате проведенного в работе исследования выявлена возможность проектирования системы с большей надежностью путем введения аппаратурного резервирования отдельных элементов, имеющих наибольшее значение значимости.

Рассмотрены два подхода к выбору числа резервных элементов:

1) Определение требуемого количества резервных элементов, обеспечивающих максимальные значения показателей надежности системы при величине затрат, не превышающей заданную.

2) Определение требуемого количества резервных элементов, обеспечивающих заданное значение показателя надежности системы при минимальных затратах.

На основе метода неопределенных множителей Лагранжа в работе были решены поставленные задачи оптимизации, в результате чего даны рекомендации по достижению не только заданной надежности, но и к достижению этой надежности при минимальных затратах.

Исследована зависимость коэффициента улучшения надежности систем нагруженного режима от числа резервных элементов систем. Показано, что увеличение числа резервных элементов более 3 приводит к незначительному увеличению надежности системы.

Рассмотрена система с тройным резервированием в нагруженном режиме в условиях воздействия низкоинтенсивных ИИ. Было получено выражение для ВБР системы в условиях воздействия ИИ:

$$R_{ИИ}(t) = 1 - (1 - e^{-\lambda \cdot t} \cdot (2 - e^{(K_p \cdot D(t))^2}))^3. \qquad (5)$$

С введением режима принудительного переключения резервных комплектов (РПП) в рассмотренную систему получено выражение для ВБР системы:

$$R(t)_{РПП} = 1 - (1 - e^{-\lambda \cdot t} \cdot (2 - e^{(\frac{K_p \cdot D(t)}{3})^2}))^3. \qquad (6)$$

На основе полученных выражений для системы с тройным резервированием в нагруженном режиме были построены графики зависимости ВБР от времени (рис. 1). Графики показывают, что ВБР системы без РПП быстро снижается, а ВБР системы с введением РПП приближается к случаю без воздействия ИИ. Показано, что в данном случае при T_{CAC} = 7лет надежность системы повышается на 5,3%, благодаря введению РПП.

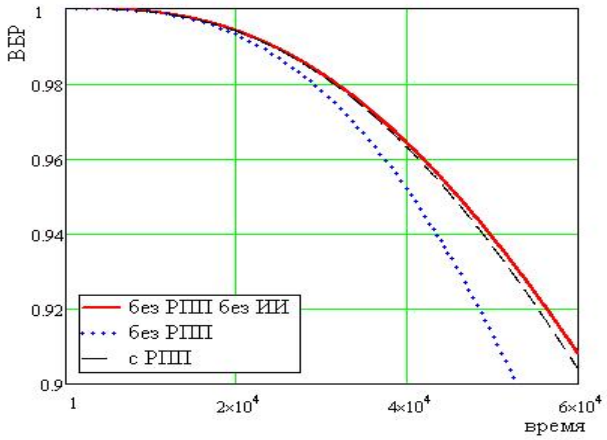


Рис. 1. Зависимость ВБР системы с тройным резервированием от времени для $\lambda = 10^{-6}(час^{-1})$, $K_p = 1{,}4 \cdot 10^{-4}(рад^{-1})$, $P = 4 \cdot 10^{-2}\,(рад/час)$

В работе даны рекомендации, позволяющие обосновано выбирать интервал переключения основных и резервных комплектов.

В работе также были получены аналитические выражения для оценки ВБР системы *N*-кратного резервирования в нагруженном режиме с учетом РПП в условиях воздействия низкоинтенсивных ИИ.

По результатам второй главы сформулирована методика построения ОУВС, использующая резервирование в нагруженном режиме и режим принудительного переключения резервных элементов, позволяющая эффективно выбирать не только структурное резервирование, но и число резервных элементов в нагруженном режиме и обеспечить заданный уровень надежности системы в условиях воздействия низкоинтенсивных ИИ за весь срок активного существования.

Третья глава посвящена организации активной защиты от отказов в бортовых вычислительных системах реального времени.

В работе были рассмотрены 2 способа построения системы АЗ:

- с фиксированными контролирующими модулями, когда избыточные вычислительные модули (ВМ) последовательно подключаются в качестве контролирующих к основным ВМ;
- с переназначаемыми модулями, когда предусматривается автоматическое перераспределение функций контроля между основными и избыточными ВМ.

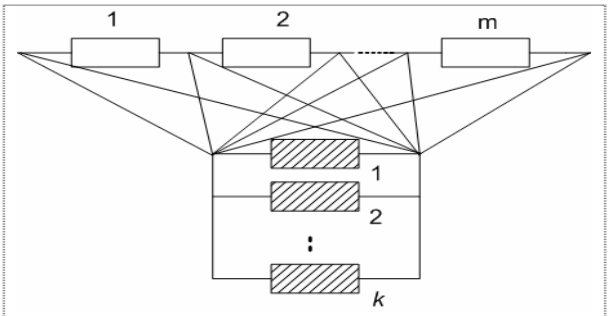


Рис. 2. Обобщенная структура системы АЗ

На основе системы, состоящей из *m* основных и *k* избыточных модулей (рис. 2), для *m*=3, *k*=2 была организована система активной защиты от отказов по постоянным тактам. Для способа формирования пар ВМ с фиксацией контролирующих модулей, было показано, что цикл контроля АЗ завершается за два такта, однако при этом один основной модуль и оба избыточные модули контролируются в обоих тактах. Через три такта АЗ все основные ВМ контролируются в двух тактах. Следовательно, при наличии двух и более модулей в защитной среде формируются два и более цикла АЗ, каждый из которых может обеспечивать более высокий уровень защиты.

Для системы АЗ с m=3, k=2 в предположениях, что все ВМ являются однородными, было получено аналитическое выражение для ВБР системы:

$$R_{A3}(t) = e^{-5\cdot\lambda\cdot t} + 5\cdot e^{-4\cdot\lambda\cdot t}(1-e^{-\lambda\cdot t})\cdot\alpha_{1A3} + 10\cdot e^{-3\cdot\lambda\cdot t}(1-e^{-\lambda\cdot t})^2\cdot\alpha_{2A3}, \qquad (7)$$

где α_{1A3} - вероятность правильного обнаружения отказа одноуровневой АЗ при его возникновении, α_{2A3} - вероятность правильного обнаружения отказа двухуровневой АЗ.

Установлено, что переназначение ВМ необходимо для сокращения цикла АЗ в условиях, когда количество основных ВМ существенно больше числа избыточных модулей. За определенными модулями защитной среды на время такта АЗ закрепляются функции основных модулей и наоборот. В результате этого устраняется недостаток, свойственный системе АЗ с фиксацией контролирующих модулей, когда модули вычислительной среды контролируются значительно реже, чем модуль защитной среды.

Получено выражение для ВБР системы АЗ с переназначаемыми модулями в условиях воздействия ИИ:

$$\begin{aligned} R_{A3,ИИ}(t) = {} & e^{-5\cdot\lambda\cdot t}\cdot(2-e^{(K_p\cdot P\cdot t)^2})^5 + 5\cdot e^{-4\cdot\lambda\cdot t}\cdot(2-e^{(K_p\cdot P\cdot t)^2})^4\cdot(1-e^{-\lambda\cdot t}\cdot(2-e^{(K_p\cdot P\cdot t)^2}))\cdot\alpha_{1A3} \\ & + 10\cdot e^{-3\cdot\lambda\cdot t}\cdot(2-e^{(K_p\cdot P\cdot t)^2})^3\cdot(1-e^{-\lambda\cdot t}\cdot(2-e^{(K_p\cdot P\cdot t)^2}))^2\cdot\alpha_{2A3}. \end{aligned} \qquad (8)$$

С целью предотвращения отказов элементов систем, вызванных воздействием ИИ, был введен РПП в систему АЗ с фиксацией контролирующих модулей.

Показано, что длительности интервала отключения контролирующих модулей должны быть кратны циклу контроля.

В результате введения РПП в систему АЗ с переназначаемыми модулями было получено выражение для ВБР системы:

$$\begin{aligned} R_{A3,РПП}(t) = {} & e^{-5\lambda t}(2-e^{(\frac{K_p\cdot P\cdot t}{3})^2})^5 + 5e^{-4\lambda t}(2-e^{(\frac{K_p\cdot P\cdot t}{3})^2})^4(1-e^{-\lambda t}(2-e^{(\frac{K_p\cdot P\cdot t}{3})^2}))\alpha_{1A3} \\ & + 10e^{-3\lambda t}(2-e^{(\frac{K_p\cdot P\cdot t}{3})^2})^3(1-e^{-\lambda t}(2-e^{(\frac{K_p\cdot P\cdot t}{3})^2}))^2\alpha_{2A3}. \end{aligned} \qquad (9)$$

На основании выражений (7), (8) и (9) для рассматриваемых значений параметров ИИ были получены графики зависимости ВБР системы от времени, приведенные на рис. 3. Графики показывают, что применение РПП в системе АЗ повышает надежность системы в условиях воздействия ИИ, особенно при долгосрочных применениях.

Из графиков следует, что при T_{CAC} = 7лет ВБР системы АЗ с введением РПП выше ВБР системы АЗ без РПП на 6,2%.

Для системы АЗ с фиксированными контролирующими модулями получено выражение для ВБР в виде:

$$R_{A3,PПП}(t) = e^{-5\cdot\lambda\cdot t}\cdot(2-e^{(\frac{K_p\cdot P\cdot t}{3})^2})^2\cdot(2-e^{(K_p\cdot P\cdot t)^2})^3 +$$
$$+5\cdot e^{-4\cdot\lambda\cdot t}\cdot(2-e^{(\frac{K_p\cdot P\cdot t}{3})^2})\cdot(2-e^{(K_p\cdot P\cdot t)^2})^3\cdot(1-e^{-\lambda\cdot t}(2-e^{(K_p\cdot P\cdot t)^2}))\cdot\alpha_{1A3}+ \qquad (10)$$
$$+10\cdot e^{-3\cdot\lambda\cdot t}\cdot(2-e^{(K_p\cdot P\cdot t)^2})^3\cdot(1-e^{-\lambda\cdot t}(2-e^{(K_p\cdot P\cdot t)^2}))^2\cdot\alpha_{2A3}.$$

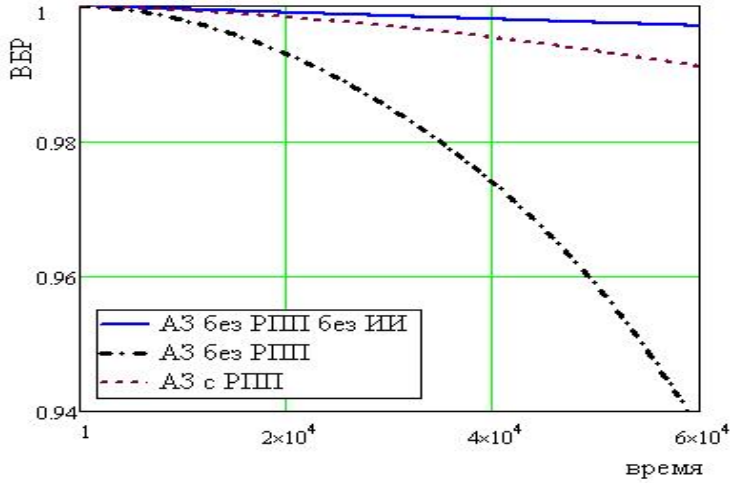
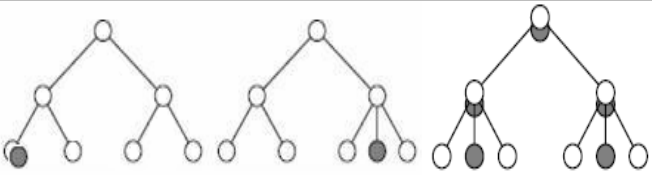


Рис. 3. Зависимость ВБР системы АЗ от времени

для $\lambda = 10^{-7}(час^{-1})$, $K_p = 1{,}4\cdot10^{-4}(рад^{-1})$, $P = 4\cdot10^{-2}\,(рад/час)$

Анализ выражений (9), (10) показывает, что организация РПП для системы АЗ с фиксированными контролирующими модулями менее эффективна по сравнению с организацией РПП для системы АЗ с переназначаемыми модулями. Это объясняется тем, что в системе АЗ с фиксированными контролирующими модулями был введен РПП только в контролирующих модулях, поэтому в условиях воздействия ИИ основные вычислительные модули снижают свою надежность.

В работе была проведена оценка эффективности АЗ в иерархических вычислительных системах (ИВС). Была исследована ИВС со структурой 1-2-2 (рис. 4), рассмотрены 3 варианты введения аппаратурного резервирования для повышения надежности системы без восстановления:



а) ***б)*** ***в)***

Рис. 4. Конфигурации ИВС

1) вариант с применением традиционного аппаратурного резервирования;

2) вариант с введением дополнительных ветвей в структуру системы для организации активной защиты от отказов;

3) комбинированный вариант.

Были получены аналитические выражения для оценки ВБР ИВС с различными конфигурациями. В результате проведенного анализа показано, что в ИВС наиболее рациональным подходом является использование традиционного резервирования (дублирование, троирование) на уровне модулей управления (верхний уровень иерархии) совместно с активной защитой на уровне модулей обработки данных (нижний уровень иерархии).

Четвертая глава посвящена моделированию и оценке показателей надежности и отказоустойчивости вычислительных систем.

Были разработаны модели, описывающие надежностные характеристики различных систем с учетом влияния принудительного переключения, степени полноты контроля и восстановления γ для различных типов систем.

Для модели системы, работающей в ненагруженном режиме, с использованием методов комбинаторного анализа в работе были получены выражения для математического ожидания и плотности вероятностей времени пребывания системы, состоящей из N процессорных модулей (ПМ), в работоспособном состоянии:

$$E[t] = \sum_{i=1}^{N-1} \gamma^{i-1}(1-\gamma)\sum_{j=1}^{i}\frac{j}{\lambda} + \gamma^{N-1}\sum_{j=1}^{N}\frac{j}{\lambda}; \qquad (11)$$

$$f(t) = \sum_{k=0}^{N-2}\frac{\lambda^k t^{k-1} e^{-\lambda t}}{(k-1)!}\ \gamma^k(1-\gamma) + \frac{\lambda^n t^{n-1} e^{-\lambda t}}{(n-1)!}\gamma^{N-1}. \qquad (12)$$

Для модели системы, работающей в нагруженном режиме без аппаратной деградации и с аппаратной деградацией были получены выражения в виде дифференциальных уравнений состояний марковской модели системы с N ПМ.

На основе полученных моделей разработан комплекс алгоритмов и программ анализа надежности и оптимального выбора параметров процедур восстановления, предназначенный для использования разработчиками ОУВС на этапах технического и рабочего проектирования.

Результаты моделирования позволили сделать следующие выводы:

1. При увеличении коэффициента полноты контроля вероятность безотказной работы системы в ненагруженном режиме увеличивается более интенсивно при долгосрочных применениях, а надежность системы без аппаратной деградации увеличивается более интенсивно в краткосрочных применениях.

2. При больших и средних значениях λ система в ненагруженном режиме работы имеет преимущество перед другими системами в долгосрочных применениях, а система, работающая в режиме без аппаратной деградации, имеет преимущество в краткосрочных применениях.

3. При малых значениях λ система без аппаратурной деградации имеет наибольшую вероятность безотказной работы в течение достаточно продолжительного времени.

Для эффективного применения механизма АЗ и РПП, в работе была разработана методика построения ОУВС, использующая механизм АЗ и РПП, состоящая из 3 этапов, позволяющая обоснованно выбирать структуру системы активной защиты от отказов, обеспечивающую требуемую надежность.

На втором этапе разработанной методики были получены аналитические выражения для оценки ВБР систем в общем случае, для системы с *m* основными и *k* дополнительными модулями:

$$R_{АЗ}(t) = \sum_{i=0}^{k-1} C_{m+k}^{i} \cdot e^{(m+k-i)\cdot\lambda\cdot t}(1-e^{\lambda\cdot t})^{i} \cdot \alpha_{iАЗ}, \qquad (13)$$

где C_n^i - число *i* сочетаний из *n*;

$\alpha_{iАЗ}$ - вероятность правильного обнаружения отказа АЗ при его возникновении на *i*-м уровне.

В условиях воздействия ИИ, ВБР системы АЗ определяется выражением:

$$R_{АЗ,ИИ}(t) = \sum_{i=0}^{k} C_{m+k}^{i} \cdot e^{(m+k-i)\cdot\lambda\cdot t} \cdot (2-e^{(K_p\cdot P\cdot t)^2})^{m+k-i} \cdot (1-e^{\lambda\cdot t}.(2-e^{(K_p\cdot P\cdot t)^2}))^{i} \cdot \alpha_{iАЗ}. \qquad (14)$$

Для системы АЗ с РПП выражение для ВБР системы определяется согласно выражению:

$$R_{АЗ,РПП}(t) = \sum_{i=0}^{k} C_{m+k}^{i} \cdot e^{(m+k-i)\cdot\lambda\cdot t} \cdot (2-e^{(\frac{K_p\cdot P\cdot t}{3})^2})^{m+k-i} \cdot (1-e^{\lambda\cdot t} \cdot (2-e^{(\frac{K_p\cdot P\cdot t}{3})^2}))^{i} \cdot \alpha_{iАЗ}. \qquad (15)$$

На основе предложенной методики построения ОУВС с АЗ и РПП была разработана программа, позволяющая исследовать влияние параметров системы на надежность ее работы. На рис. 5 приведены графики зависимости ВБР различных систем от времени.

Полученные графики показывают, что в случае без использования РПП надежность системы АЗ быстро снижается, а при применении РПП надежность системы АЗ сохраняется и приближается к случаю без воздействия ИИ.

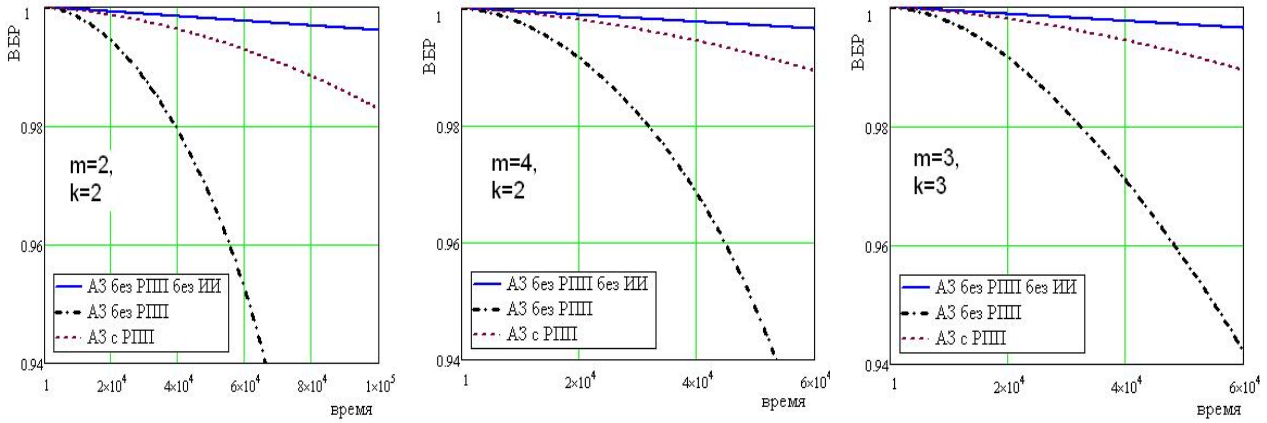


Рис. 5. Зависимость ВБР системы АЗ от времени

для $\lambda = 10^{-7}(час^{-1})$, $K_p = 1{,}4 \cdot 10^{-4}(рад^{-1})$, $P = 4 \cdot 10^{-2}\,(рад/час)$

В таблице приведены значения ВБР различных систем АЗ с m основными и k дополнительными модулями для рассматриваемых значений параметров систем и параметров ИИ при T_{CAC} = 7лет.

Таблица

ВБР системы АЗ в условиях воздействия ИИ

	m = 2, k = 2	m = 3, k = 2	m = 4, k = 2	m = 5, k = 2	m = 3, k = 3	m = 4, k = 3	m = 5, k = 3	m = 6, k = 3
ВБР без РПП	0,950	0,933	0,914	0,891	0,940	0,931	0,921	0,909
ВБР с РПП	0,993	0,991	0,989	0,987	0,989	0,987	0,986	0,984
улучшение, %	4,5%	6,2%	8,2%	10,8%	5,2%	6,0%	7,1%	8,3%

Приведенные в таблице значения ВБР показывают, что введение РПП в систему АЗ повышает надежность системы на 5%-10%, особенно при увеличении числа основных вычислительных модулей.

Анализ результатов моделирования показал, что надежность, рассчитанная с использованием разработанных в диссертации моделей,

совпадает с экспериментально полученными данными. Это свидетельствует об адекватности моделей рассматриваемых систем и о достоверности результатов, которые могут быть получены с использованием разработанных в диссертации моделей и программ.

На основе проведенного анализа расчета надежности невосстанавливаемых систем, была разработана методика расчета надежности, состоящая из следующих основных этапов:

1. Построение структурно-логической схемы (СЛС), однозначно отображающей все элементы структурной схемы и связи между ними.

2. Построение графа связности (ГС) и получение матрицы смежности (МС) системы из СЛС.

3 Нахождение всех путей успешного функционирования системы в виде элементарных конъюнкций, представляющих собой функцию работоспособности (ФРС) системы, с помощью ГС и МС.

4. Преобразование ФРС к ортогональной или ортогонально-бесповторной форме, от которой переходят к вероятностной функции.

5. Расчет показателей надежности системы с помощью её вероятностной функции работоспособности.

Было показано, что для полносвязанного графа количество путей между двумя вершинами пропорционально $(n\text{-}2)!$, где n – размер графа. Показано, что одной из наиболее трудоемких операций при выполнении этой методики является этап поиска всех путей успешного функционирования.

Для поиска всех путей успешного функционирования системы в существующих алгоритмах теории надежности используется ряд операций умножения матрицы смежности на вектор столбец, обладающих достаточно большой вычислительной сложностью. Целью третьего этапа данной методики расчета является нахождение всех путей от одной вершины графа к другой. На основе метода поиска в глубину с возвращением был разработан оригинальный алгоритм поиска всех путей успешного функционирования, обладающий приемлемой для инженерных расчетов вычислительной эффективностью, позволяющий сократить время решения задачи поиска за счет использования рекурсии.

В результате анализа метода преобразования ФРС к ортогональной или ортогонально-бесповторной форме был выбран метод ортогонализации по формуле Порецкого, обладающий инвариантностью к размерам конъюнкции и удобством в реализации.

Полученные в диссертации результаты использованы при выполнении работы по созданию отказоустойчивой цифровой вычислительной системы для бортового Фурье-спектрометра ИКФС-2. Исходя из заданных требований к надежности всего прибора, путем моделирования с использованием разработанных в диссертации методов и алгоритмов были выработаны рекомендации по построению отказоустойчивой цифровой вычислительной системы бортового Фурье-спектрометра ИКФС-2, предназначенной для длительного использования в составе научной аппаратуры космического аппарата Метеор-3М.

Основные результаты диссертационной работы

1. Разработана методика построения отказоустойчивых вычислительных систем, использующая резервирование в нагруженном режиме и режим принудительного переключения резервных элементов, позволяющая эффективно выбирать не только структурное резервирование, но и число резервных элементов в нагруженном режиме и обеспечить заданный уровень надежности системы в условиях воздействия ионизирующих излучений за весь срок активного существования. Показано, что при долгосрочных применениях использование режима принудительного переключения резервных элементов в системе с тройным резервированием повышает надежность не менее, чем на 5%.

2. Разработана методика построения отказоустойчивых вычислительных систем, использующая механизм активной защиты от отказов и режим принудительного переключения резервных комплектов. Получены аналитические выражения для оценки вероятности безотказной работы системы активной защиты от отказов в общем случае для любого числа основных и дополнительных вычислительных модулей, позволяющие обоснованно выбирать структуру системы активной защиты от отказов, обеспечивающую требуемую надежность. Показано, что при совместном использовании активной защиты от отказов и режима принудительного переключения резервных комплектов надежность систем при долгосрочных применениях повышается не менее чем на 5-7%.

3. Получены оценки эффективности применения активной защиты от отказов в иерархических бортовых вычислительных системах. Показано, что в иерархических бортовых вычислительных системах наиболее рациональным подходом является использование традиционного

резервирования на уровне модулей управления совместно с активной защитой на уровне модулей обработки данных.

4. Разработаны модели надежности отказоустойчивых вычислительных систем с учетом полноты контроля и восстановления для различных режимов функционирования отказоустойчивых вычислительных систем, позволяющие исследовать влияние различных параметров системы на ее надежность.

5. Разработана методика расчета надежности невосстанавливаемых систем, использующая оригинальный алгоритм решения задачи поиска всех путей успешного функционирования на основе метода поиска в глубину с возвращением. Предложенный алгоритм позволяет сократить время решения задачи за счет использования рекурсии.

Работы по теме диссертации

1. Ле Куанг Минь, Романовский А.С. Оценка эффективности применения методов активной защиты от отказов в иерархических вычислительных системах // Вестник МГТУ. Сер. Приборостроение. - 2007. - №4. - С. 62-69.

2. Ле Куанг Минь, Смирнов А.С. Разработка программы поиска всех путей успешного функционирования системы для расчета показателей надежности структурно-сложных систем // Материалы межвузовской научно-технической конференции. – СПб., 2003. - Ч.V - С. 95-97.

3. Ле Куанг Минь, Романовский А.С. Алгоритмы поиска всех путей успешного функционирования для расчёта показателей надёжности структурно-сложных систем // Информатика и системы управления в XXI веке: Сборник трудов - М.: МГТУ, 2007.- № 5 - С. 180-184.

4. Ле Куанг Минь. Анализ эффективности применения методов повышения отказоустойчивости ИВС реального времени // Микроэлектроники и информатики – 2007: Тез. докл. Всероссийской конференции. - М., 2007. - С.253.

5. Ле Куанг Минь. Анализ методов обеспечения отказоустойчивости и живучести вычислительных систем // Естественные науки и технологии- 2007.- №5- С. 236-238.