На правах рукописи

Глухих Михаил Игоревич

Разработка методов синтеза информационно-управляющих систем специального назначения со структурным резервированием

Специальность

05.13.15 – Вычислительные машины и системы

АВТОРЕФЕРАТ

диссертации на соискание ученой степени

кандидата технических наук

Санкт-Петербург – 2006

Работа выполнена на кафедре «Автоматика и вычислительная техника» государственного образовательного учреждения высшего профессионального образования «Санкт-Петербургский государственный политехнический университет».

Научный руководитель	доктор технических наук, профессор Мелехин Виктор Федорович
Официальные оппоненты	доктор технических наук, профессор Черкесов Геннадий Николаевич
	кандидат технических наук, доцент Скорубский Владимир Иванович
Ведущая организация	ФГУП НПО «Импульс»

Защита состоится 25 января 2007 г. в 16 часов на заседании Диссертационного Совета Д 212.229.18 при ГОУ ВПО «Санкт-Петербургский государственный политехнический университет» по адресу: 195251, Санкт-Петербург, ул. Политехническая, д. 29, 9-й учебный корпус, ауд. 325.

С диссертацией можно ознакомиться в фундаментальной библиотеке ГОУ ВПО «Санкт-Петербургский государственный политехнический университет».

Автореферат разослан «___» декабря 2006 г.

Ученый секретарь
диссертационного совета Шашихин В.Н.

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Актуальность темы. Информационно-управляющие системы специального назначения (ИУССН) используются для автоматизации контроля и управления в сложных технических системах различного назначения: космических комплексах, летательных аппаратах разного класса, наземных станциях контроля и управления, судах различного назначения, энергетических комплексах и др.

Важнейшей характеристикой ИУССН является надежность. Надежность системы зависит от большого числа факторов: от ее функциональной организации, от технологии изготовления элементов, узлов и соединений между узлами, от окружающей среды и др.

Проблема повышения надежности вычислительных систем изучается довольно давно. Первая работа на эту тему датируется 1952 годом и принадлежит Джону фон Нейману. Сейчас широко разработанными являются задачи, связанные с повышением надежности отдельных компонент системы (работы У. Пирса, Д. Трайона, Э. Мура), с повышением надежности передачи данных (работы К. Шеннона, М. Голея, Р. Хэмминга), с определением надежностных характеристик вычислительных систем (работы И. А. Рябинина, Г. Н. Черкесова, А. М. Половко). Разработан ряд стандартов и рекомендаций, связанных с надежностью систем и их элементов.

ИУССН относятся к вычислительным системам, ошибка на выходе которых может иметь критические последствия для их окружения – иначе говоря, к системам высокой достоверности (ultradependable systems).При проектировании такого рода систем следует учитывать не только их надежность, но и их безопасность.

По этой причине в ИУССН крайне важно своевременное обнаружение отказа. Механизмы контроля надежности, применяющиеся в типовых элементах системы, обычно недостаточны или отсутствуют. В этом случае

необходимо применение структурного резервирования, контроль надежности осуществляется на системном уровне с помощью решающих элементов.

При проектировании вычислительной системы с применением решающих элементов встает задача выбора структуры системы. Используемые готовые элементы и инструментарий проектирования постоянно и весьма динамично развиваются. С учетом этих факторов, актуально обеспечение надежности и безопасности системы на этапе ее проектирования.

При эвристическом подходе к проектированию вычислительной системы основными источниками информации при синтезе служат сведения о системе-прототипе и ее недостатках, новые требования к вычислительной системе, новые средства реализации системы. По мере развития средств вычислительной техники, увеличения сложности вычислительных систем и ужесточения требований к ним число возможных вариантов функциональной организации резервированных систем быстро возрастает.

Существующие автоматизированные подходы связаны с выбором оптимальной структуры из множества некоторого узкого класса – в частности, из множества последовательно-параллельных систем с различной кратностью. Недостаток такого подхода состоит в том, что оптимальная структура может не оказаться в выбранном множестве.

Поэтому требуется разработка модели вычислительных систем, обладающей полнотой порождения множества вариантов структуры ИУССН. В модели должна существовать возможность на уровне функциональной организации рассматривать процессы распространения отказов и определять условия, обеспечивающие свойства надежности и безопасности. Модель должна позволять осуществлять сравнительную оценку характеристик систем при ограниченной информации (без детальной проработки вариантов) и обоснованно уменьшать многообразие вариантов, требующих детальной проработки. На базе такой модели можно разработать методику синтеза структур вычислительных систем с требуемыми свойствами.

Объектом исследования является информационно-управляющая система специального назначения (ИУССН). В соответствии с распределенностью в пространстве оборудования технических систем ИУССН строятся как системы распределенной обработки данных, реализуемые в виде локальной вычислительной сети. Обычно сеть содержит пульт управления, приборы, распределенные по отдельным объектам, и, возможно, встраиваемые системы (интеллектуальные датчики и исполнительные устройства).

Особенностью многих ИУССН являются сравнительно умеренные требования к производительности в сравнении с суперкомпьютерами и системами с массовым параллелизмом. Как правило, производительности современного процессора вполне достаточно для решения задач, определенных для одного прибора. Это ограничивает класс рассматриваемых в данной работе вычислительных систем. Рассматриваются следующие свойства системы.

1. Безопасность. Вероятность возникновения необнаруженного отказа должна быть не выше определенного уровня (поскольку наличие необнаруженного отказа может привести к ошибкам в результатах на выходе системы и, как следствие – к критическим последствиям для окружения системы).
2. Безотказность. Система должна обеспечивать требуемый уровень безотказности.
3. Типовые элементы. В составе системы могут быть использованы типовые (готовые) элементы с недостаточными характеристиками по надежности и безопасности.
4. Невосстанавливаемость элементов. Во время работы системы, отказавшие элементы не могут быть восстановлены.

Цель работы. Сокращение времени проектирования и повышение качества разработки системы со структурным резервированием путем автоматизации синтеза.

Задачи исследования.

1. Разработка модели для представления произвольных вариантов структуры системы с резервированием, позволяющей анализировать процессы распространения отказов. Разработка правил построения и модификации модели.
2. Разработка методики сравнительного анализа характеристик ИУССН по предложенной модели и отбрасывания заведомо бесперспективных структур с последующей параметризацией оставшихся структур.
3. Создание методики поиска наилучшей структуры из ограниченного множества вариантов.
4. Разработка функциональной схемы системы-прототипа с целью иллюстрации методики и решения последующих задач.

Методы и средства исследования. Для теоретических исследований применяются методы теории отношений, теории графов, теории надежности, логико-вероятностные методы, теории случайных процессов, математического моделирования, математического программирования. Для построения моделей устройств использовались системы автоматизированного проектирования MAX+PLUS II, Quartus II и среда программирования Microsoft Visual Studio.

Положения, выносимые на защиту.

1. Модель структуры ИУССН на основе введенных в работе динамических типизированных графов, обладающая возможностью рассмотрения процессов распространения отказов и полнотой представления множества вариантов структуры.
2. Выделение подмножества структур ИУССН, оптимальных по комбинированному критерию надежности, безопасности и стоимости – доменных структур, включающих множество независимых узлов доменов с голосующим устройством на входе каждого.
3. Методика синтеза структур ИУССН с доменной организацией.

Научная новизна работы.

1. Разработана модель структуры ИУССН – динамический типизированный граф. Модель обладает возможностью рассматривать на функциональном уровне процессы распространения отказов и полнотой представления множества вариантов структуры ИУССН. Разработана программа расчета вероятности безотказной работы системы по динамическому типизированному графу.
2. Предложена методика упорядочения структур по комбинированному показателю, учитывающему свойства надежности, безопасности и стоимости, с использованием динамических типизированных графов. Методика позволяет осуществлять сравнительную оценку характеристик систем при ограниченной информации и обоснованно уменьшать многообразие вариантов, требующих детальной проработки.
3. С применением методики упорядочения структур выделено подмножество оптимальных структур и доказана возможность разделения структуры из данного множества на домены – наборы не связанных друг с другом узлов с голосующим устройством на входе и ациклической структурой.
4. Выделен новый класс из множества доменных структур ИУССН – масштабируемые структуры с резервированием. Главное преимущество данного класса структур заключается в возможности увеличения надежности системы путем увеличения числа однотипных устройств без изменения структуры голосующих устройств.
5. Разработана методика синтеза структуры ИУССН с доменной организацией, позволяющая осуществить обоснованный выбор числа доменов в системе, распределения устройств между доменами, числа однотипных устройств в системе и числа входов используемых голосующих устройств.

Достоверность результатов. Достоверность методики упорядочения структур и тезис о возможности разбиения оптимальной структуры на домены подтверждается доказательствами утверждений, положенных в

основу методики, а также включением в полученное множество оптимальных структур известного множества последовательно-параллельных систем.

Достоверность зависимостей вероятности безотказной работы системы от характеристик доменной структуры подтверждается получением некоторых результатов двумя различными методами, совпадением результатов с известными частными случаями и использованием автоматизированного подхода при их получении.

Практическая значимость работы. Полученные в диссертационной работе методики синтеза и анализа структур позволяют снизить трудоемкость и повысить качество проектирования ИУССН, а также обосновать правильность принятых решений на системном этапе проектирования. С использованием предложенных методик разработан прототип ИУССН на основе СБИС ПЛ. Он позволяет проводить экспериментальные исследования в системном окружении. Результаты диссертационной работы могут быть использованы в проектных организациях при создании отказоустойчивых вычислительных систем, а также в соответствующих дисциплинах при обучении студентов.

Реализация результатов работы. Результаты, полученные в диссертации, используются в учебном процессе на кафедре автоматики и вычислительной техники ГОУ ВПО «СПбГПУ» при чтении лекций по курсу «Проектирование аппаратных средств вычислительных систем», а также при выполнении практических занятий на экспериментальной установке системы-прототипа, спроектированной с использованием теоретических результатов работы.

Научно-исследовательские работы. Результаты диссертации были получены в ходе выполнения научно-исследовательских работ по следующим проектам.

1. Разработка методики и инструментария для проектирования и верификации высоконадежных специализированных процессоров на базе СБИС ПЛ. Программа министерства образования РФ, подпрограмма

«Международное научно-образовательное сотрудничество», проект №1283 за 2003 год.

2. Разработка методики и инструментария для проектирования и верификации высоконадежных специализированных процессоров на базе СБИС ПЛ. Программа министерства науки и образования РФ, федерального агентства по образованию «Федерально-региональная политика в науке и образовании», подпрограмма «Международное научно-образовательное сотрудничество», проект №1647 за 2004 год.
3. Создание центра по коммерциализации разработок Санкт-Петербургского государственного политехнического университета в области проектирования радиоэлектронной аппаратуры с использованием технологий FPGA и ASIC. Программа министерства науки и образования РФ, федерального агентства по образованию «Развитие научного потенциала высшей школы», подпрограмма 3 «Развитие инфраструктуры научно-технической и инновационной деятельности высшей школы и ее кадрового потенциала» на 2005 год.
4. Развитие центра трансфера технологий проектирования ASIC/FPGA на базе Санкт-Петербургского государственного политехнического университета для промышленности региона. Программа и подпрограмма п. 3, 2005 год.
5. Развитие международного центра трансфера технологий проектирования ASIC на базе Санкт-Петербургского государственного политехнического университета. Программа и подпрограмма п. 3, 2005 год.

Апробация работы. Результаты работы докладывались и обсуждались на VIII Всероссийской конференции «Фундаментальные исследования в технических университетах» (2004 год) и на ежегодной конференции «Практические аспекты разработки отечественных СБИС класса «система на кристалле»» (2006 год).

Публикации. По результатам диссертационной работы опубликовано шесть печатных работ, в том числе в журнале «Научно-технические

ведомости СПбГТУ» (входит в «Перечень ведущих рецензируемых научных журналов и изданий, выпускаемых в Российской Федерации»). Всего опубликовано три журнальных статьи и три тезиса конференций.

Структура и объем работы. Диссертационная работа состоит из введения, пяти глав, заключения, списка используемых источников. Общий объем работы составляет 173 печатные страницы, работа включает 50 рисунков, список источников из 89 наименований, одно приложение.

СОДЕРЖАНИЕ РАБОТЫ

Во **введении** обосновывается актуальность темы, определяются основные направления и цель работы, формулируются положения, выносимые на защиту.

В **первой главе** рассматриваются основные требования при решении задачи синтеза ИУССН:

1. Система должна удовлетворять всем функциональным требованиям.
2. Заданы типовые устройства, входящие в ее состав, и характеристики этих устройств (показатели надежности, безопасности и стоимости).
3. Система должна обеспечивать требуемый уровень надежности и безопасности.
4. Стоимость системы должна быть минимальной.

В целях уточнения формулировки задачи синтеза ИУССН проводится обзор научных работ в следующих направлениях:

1. Терминология теории надежности и безопасности, употребляемые показатели качества.
2. Классификация методов повышения надежности и безопасности.
3. Основные методы расчета показателей надежности.
4. Существующие архитектуры вычислительных систем с резервированием.
5. Известные постановки и методы решения задачи синтеза.

Из проведенного обзора выявлено, что существующие автоматизированные подходы связаны с выбором оптимальной структуры из множества некоторого узкого класса (например, из множества последовательно-параллельных систем с различной кратностью). Недостаток такого подхода состоит в том, что выбор множества решений связан с удобством формализации задачи, и оптимальная структура в общем случае не содержится в выбранном множестве.

В новой постановке с учетом сформулированных выше требований задача синтеза разбивается на следующие этапы:

1. Порождение множества решений.
2. Выделение основных характеристик решений и сведение выбора к комбинаторной задаче перебора. Для этого необходимо упорядочить множество решений, отбросить заведомо невыгодные решения и выделить подмножество, в котором находится оптимальное решение.
3. Решение комбинаторной задачи одним из методов математического программирования. С этой целью необходимо параметризовать структуры, определить основные закономерности, которым подчиняются зависимости показателей надежности, безопасности и стоимости в выделенном множестве решений от параметров структуры и сформулировать алгоритм, позволяющий выделить оптимальное решение.
4. Реализация полученной структуры на практике. Для проверки теоретических положений синтезируется прототип ИУССН.

Во **второй главе** разрабатывается формализованная модель, позволяющая представить в абстрактной форме произвольную структуру системы с резервированием и анализировать надежность и безопасность при минимуме входной информации.

В **разделе 2.1** выбирается способ функциональной организации ИУССН и определяется набор подсистем, решающих различные задачи. При этом ИУССН разбивается на следующие подсистемы:

1. Вычислительная подсистема – отвечает за выполнение основной функциональной задачи ИУССН.
2. Подсистема коммутации и контроля – решает задачи передачи данных, обнаружения, маскирования и первичной диагностики отказов. В целях сокращения объемов передаваемой между подсистемами информации удобно совмещение указанных функций в одной подсистеме.
3. Подсистема конфигурации – решает задачи диагностики и изоляции отказов.

Выделяются элементы окружения ИУССН:

1. Пользователь – основной потребитель результатов системы. Им может быть человек, а может быть техническая система – объект управления и контроля. Выдача результатов системы происходит через устройства, которые не могут быть продублированы – в дальнейшем, они называются **уникальными.**
2. Оператор – осуществляет замену неисправных устройств, проводит тестирование системы и ручную настройку ее конфигурации.

Функциональная схема ИУССН приведена на рис. 1. По своему составу функциональная схема не является новой. Она необходима для конкретизации названий подсистем и как база для функциональной декомпозиции – основы процесса синтеза структуры.

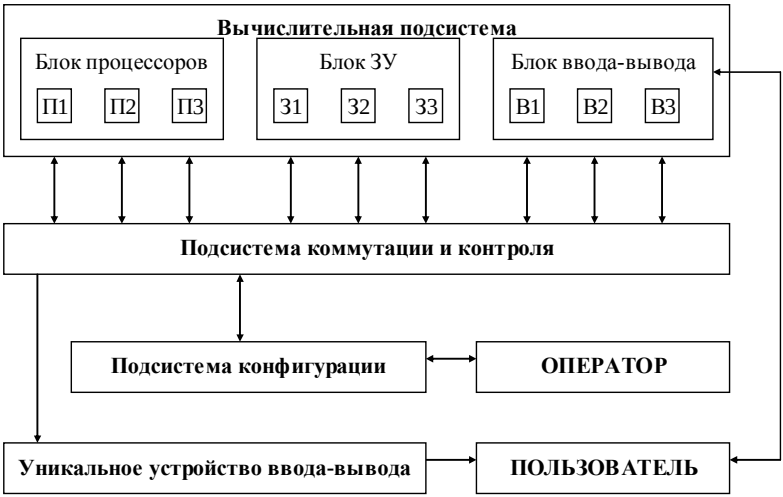

Рис. 1. Функциональная схема ИУССН и ее окружения.

Рассматриваются основные алгоритмы функционирования устройств коммутации и контроля (УКК) в зависимости от количества экземпляров коммутируемых устройств. Выделены три случая:

1. **Дублирование** (два экземпляра). В случае несовпадения результатов происходит остановка УКК и всех связанных с ним устройств.

2. **Троирование** (три экземпляра). Решение принимается голосованием. Если результаты одного устройства отличаются от двух других, они считаются неверными и маскируются. В случае систематического несовпадения результатов устройство считается отказавшим и изолируется, УКК при этом переходит в режим работы с двумя устройствами. Попарное несовпадение результатов приводит к остановке системы.
3. **N-кратное резервирование** (N>3 экземпляров). Если M>N/2 устройств дают совпадающие данные, они считаются верными. Другие результаты маскируются. При систематическом несовпадении устройство изолируется, УКК переходит в режим работы с N-1 устройством. Если не существует M>N/2 устройств, дающих совпадающие результаты, система останавливается.

В **разделе 2.2** рассматривается модель, отображающая блоки структуры и связи. Абстрагируемся от процессов внутри блоков. Правильность функционирования блоков определяется по результатам на их выходах. Основным объектом рассмотрения является процесс распространения отказов (неправильных результатов) в системе. Для этой цели модель должна отражать:

1. Различные функциональные типы блоков – для определения возможности контроля их результатов путем сравнения.
2. Связи между блоками – для определения направления распространения информации в системе.
3. Состояния блоков, характеризующие их работоспособность.

Для отражения отмеченных свойств структуры используется модификация ориентированных графов. Орграф отображает только наличие или отсутствие блока в структуре и связи между блоками.

Модификация орграфа заключается в «типизации» блоков (вершин графа) по функциональному признаку. Типизация выражается формой вершин графа и их именами. Выделяются **основные** вершины,

соответствующие вычислительным устройствам (ВУ), и **промежуточные** вершины, соответствующие устройствам коммутации и контроля (УКК). На графах основные вершины обозначаются кругами, промежуточные – квадратами. Вводится понятие **типа** вершины. Однотипные вершины соответствуют блокам, выполняющим одинаковые задачи, и обозначаются одинаковыми латинскими буквами с разными индексами.

Вторым видом модификации орграфа являются пометки вершин графа состоянием блока, характеризующим его работоспособность. Это состояние может изменяться при возникновении и распространении отказов. Выделяются работоспособное состояние (W, Work), состояние остановки, вызываемое обнаружением отказа внутри данного устройства или устройства, связанного с ним (S, Stop), и состояние аварии, вызываемое поступлением в устройство неверных результатов без обнаружения отказа (F, Fail).

С учетом отмеченных модификаций орграф, предложенный в качестве модели структуры системы, назван **динамическим типизированным графом (ДТГ).**

В **разделе 2.3** формулируются правила работы с моделью ДТГ. Правила основаны на неформальных требованиях к структурам систем с резервированием и разделены на 6 групп:

1. Правила представления системы в виде ДТГ. Устройство системы представляется вершиной. Связи для передачи информации представляются дугами. ВУ представляются основными вершинами, УКК – промежуточными вершинами.
2. Правила соединений вершин ДТГ. Основные вершины связываются только через промежуточные, причем имеют только одну входящую дугу (задача передачи информации решается УКК). ДТГ должен быть сильносвязным для возможности передачи информации между любой парой основных вершин. Промежуточные вершины, входные для основных, в дальнейшем называются **формирующими**.

3. Правила введения типов вершин. Устройства, имеющие одинаковую внутреннюю структуру и выполняющие идентичные операции, считаются **однотипными**, и отображаются **однотипными вершинами** ДТГ. УКК считаются однотипными, если их входные и выходные потоки данных совпадают.
4. Правила изменения состояний вершин. Три состояния – работа W, остановка S, авария F. Начальное состояние – W. В вершинах могут происходить обнаруженные и необнаруженные отказы, переводящие их в состояние S или F. Отказы могут повлечь за собой изменение состояния связанных вершин.
5. Правила распространения отказа. При изменении состояния формирующей вершины основная вершина переходит в то же состояние. Изменение состояния вершины X, входной для промежуточной вершины K, ведет к изменению состояния вершины K. При отсутствии входных вершин одного типа с X, вершина K переходит в то же состояние. При наличии одной вершины того же типа, вершина K переходит в состояние S. При наличии двух и более вершин того же типа, вершина K остается в состоянии W.
6. Правила изменения состояния ДТГ. ДТГ находится в состоянии W, если и только если существует связный подграф из вершин в состоянии W, включающий, по меньшей мере, одну вершину каждого типа. В противном случае, ДТГ находится в состоянии S, если хотя бы одна его вершина перешла в это состояние. Иначе ДТГ находится в состоянии F.

В **разделе 2.4** определяется и формализуется постановка задачи синтеза ИУССН с использованием модели ДТГ. Функциональность системы обеспечивается наличием заданного набора типов основных вершин графов. При этом отдельно выделяется множество типов вершин D, соответствующих уникальным устройствам – **решающих** вершин, и множество типов остальных вершин P. На основании этого, выделяется множество ДТГ, **совместимых по типам**, обозначаемое G(P, D).

С учетом введенных понятий, задача синтеза формулируется следующим образом. Заданы множества типов основных вершин P и D. Для всех элементов этих множеств заданы характеристики вычислительных устройств, соответствующих данным типам вершин. Выбрать из множества G(P, D) динамический типизированный граф g, обеспечивающий выполнение требований по надежности и безопасности и минимальное значение стоимости.

Решение задачи синтеза предполагает полный или частичный перебор множества G(P, D) и выбор лучшего решения по заданному критерию. Применение полного перебора крайне трудоемко. Частичный перебор требует усечения множества G(P, D) без потери оптимального решения.

Поэтому необходим аппарат, позволяющий отбросить решения из G(P, D), обладающие заведомо худшими характеристиками. Одним из возможных аппаратов является теория отношений.

Для его применения необходимо задание на множестве G(P, D) отношения порядка с точки зрения заданных критериев оптимальности. В этом случае, перебор решений может быть ограничен множеством максимальных элементов для заданного отношения.

В **третьей главе** для сокращения перебора элементов множества G(P, D) ставится и решается задача выделения подмножества элементов, оптимальных по критериям надежности, безопасности и стоимости. Для этой цели, на множестве G(P, D) задаются бинарные отношения порядка, отдельно для критериев надежности, безопасности и стоимости. Эти отношения обозначаются R_b, T_b, C_b, где символы R, T и C соответствуют надежности (Reliability), безопасности (safeTy) и стоимости (Cost). Например, для графов $g_1 \in G, g_2 \in G$ выполняется отношение R_b ($g_1 R_b g_2$), если граф g_2 может быть заменен графом g_1 с получением выигрыша в надежности системы.

Данный набор отношений позволяет задать общее отношение порядка для комбинации заданных критериев. Это отношение обозначается символом O (Optimal). Отношение $g_1 O g_2$ выполнено, если граф g_2 может быть заменен

графом g_1 с получением выигрыша в надежности, безопасности и стоимости системы. Это происходит при $g_1R_bg_2$, $g_1T_bg_2$, $g_1C_bg_2$ (оптимизация по Слейтеру).

В **разделе 3.1** формулируются отношения порядка на множестве G(P, D). Для формулировки этих отношений необходимо знать, как соотносятся друг с другом характеристики различных устройств, входящих в систему, и соответствующих им вершин ДТГ. Для основных вершин характеристики считаются известными, причем для однотипных вершин они совпадают. Для сравнения характеристик промежуточных вершин формулируется отношение порядка по критерию стоимости C_b, определяемое числом их связей с другими вершинами (при увеличении числа связей соответствующее устройство становится хуже по критерию стоимости, а также по критериям надежности и безопасности).

Для сравнения характеристик двух систем по ДТГ необходимо построить графы состояний этих систем. Вершинами графов состояний являются различные конфигурации ДТГ, дуги соответствуют отказам отдельных вершин. При рассмотрении всех видов отказов образуется **граф надежности**, при рассмотрении только отказов, приводящих к авариям, образуется **граф безопасности**. Пример формирования этих графов рассмотрен на рис. 2 и рис. 3. В графах состояний 0 – стартовая конфигурация, E – отказавшая конфигурация.

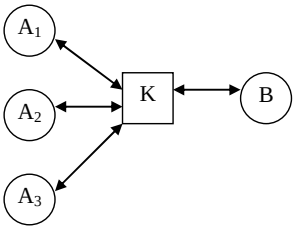

Рис. 2. ДТГ простой системы.

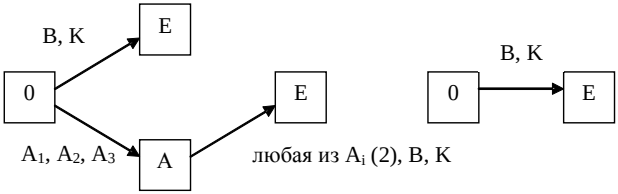

Рис. 3. Графы надежности (слева) и безопасности (справа).

Показатели надежности и стоимости системы подчиняются нескольким основным правилам, верным независимо от закона распределения отказов отдельных устройств. Правила для безопасности аналогичны правилам для надежности.

1. Если любая вершина ДТГ g_1 не уступает в стоимости соответствующей вершине g_2, и хотя бы одна вершина g_1 выигрывает в стоимости у соответствующей вершины g_2, то $g_1 C_b g_2$ (на практике система или устройство являются более дешевыми).
2. Если графы надежности для ДТГ g_1 и g_2 имеют совпадающую структуру и выполняется условие п. 1 о стоимости вершин g_1 и g_2, то $g_1 R_b g_2$.
3. Если граф надежности для ДТГ g_2 отличается от графа надежности для ДТГ g_1 последовательным добавлением дуги, то $g_2 R_b g_1$.
4. Если граф надежности для ДТГ g_2 отличается от графа надежности для ДТГ g_1 параллельным добавлением дуги, то $g_1 R_b g_2$.

В **разделе 3.2** производится упорядочение множества G(P, D) по критерию безопасности. Безопасность системы напрямую связана с наличием в ее составе уникальных вершин. В **леммах 3.2.1 – 3.2.3** доказывается, что отказ любой решающей вершины ДТГ, а также любой вершины, формирующей для решающей вершины, всегда приводит к его переходу в состояние F.

В **теореме 3.2.4** определяется оптимальная по критерию безопасности структура ДТГ для случая, когда множество решающих вершин D содержит одну вершину. В оптимальной структуре, решающая вершина α имеет

формирующую вершину К с **ровно двумя** входными вершинами одного типа. При большем количестве входных вершин формирующая вершина К хуже по критерию безопасности – поэтому ДТГ хуже по критерию безопасности. При одной входной вершине в цепочке входных вершин рано или поздно встретится вершина с двумя входными вершинами одного типа, и ДТГ также будет хуже по критерию безопасности.

Пример приведен на рис. 4. При наличии нескольких решающих вершин в множестве D оптимальная по критерию безопасности структура строится аналогичным образом.

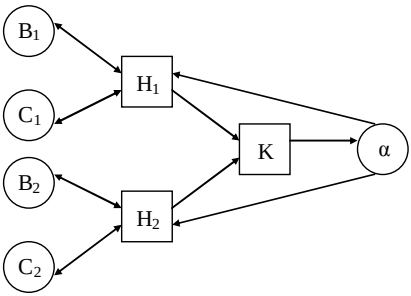

Рис. 4. Пример ДТГ, оптимального по критерию безопасности.

В **разделе 3.3** производится упорядочение множества G(P, D) по критериям надежности и стоимости. С этой целью, анализируются возможные преобразования фрагментов ДТГ, не ухудшающие данные характеристики.

В **леммах 3.3.1 – 3.3.3** обосновываются три возможных преобразования структуры ДТГ $g_1 \rightarrow g_2$, обеспечивающие $g_2 R_b g_1$ и $g_2 C_b g_1$:

1. Устранение из ДТГ избыточных связей, не обеспечивающих сдерживание отказов.
2. Устранение связей между независимыми частями ДТГ, каждая из которых обеспечивает сдерживание отказов.
3. Устранение связей между однотипными вершинами.

Теорема 3.3.4 на основании приведенных лемм доказывает, что ДТГ, входящий в множество максимальных элементов по отношениям надежности и стоимости, может быть разбит на непересекающиеся узлы доменов. Узлом домена называется ациклический связный подграф, не имеющий в своем составе однотипных начальных вершин и удовлетворяющий двум свойствам:

1. Любая начальная вершина узла домена имеет однотипные входные вершины или решающую входную вершину, являющиеся одновременно вершинами других узлов доменов.
2. Внутренние вершины узлов доменов не имеют входных вершин, принадлежащих другим узлам.

Доменом при этом называется объединение узлов с одинаковой структурой, соответствующие вершины которых однотипны.

В **подразделе 3.3.5** анализируются доменные структуры. В рамках используемого подхода (сравнение графов состояний) определение лучшей или худшей из двух доменных структур невозможно. Поэтому необходима параметризация доменной структуры с целью упрощения поиска оптимальной из них путем сравнения численных показателей. Вводятся следующие параметры: число доменов в ДТГ, максимальное число однотипных вершин в каждом домене (размер домена) **σ(h)** и устойчивость домена к отказам на его входе **φ(h)** (максимальное число вершин входного домена, отказ которых не влияет на состояние данного домена).

В **лемме 3.3.6** и **теореме 3.3.7** анализируется структура домена с заданными параметрами. Доказывается связь параметров входного домена $h_{вх}$ и выходного домена $h_{вых}$: $\sigma(h_{вх})\geq\varphi(h_{вых})+2$. Учитывая это соотношение, в **подразделе 3.3.8** доменные структуры делятся на два класса.

1. Последовательно-параллельные структуры, $\sigma(h_{вх})=\varphi(h_{вых})+2$. В них резервирование осуществляется на уровне групп устройств. Пример приведен на рис. 5. Во всех доменах, кроме одного, имеется $\sigma=3$ узла, число входных вершин для сдерживающих вершин **совпадает** с размером домена, устойчивость доменов $\varphi=\sigma-2$.

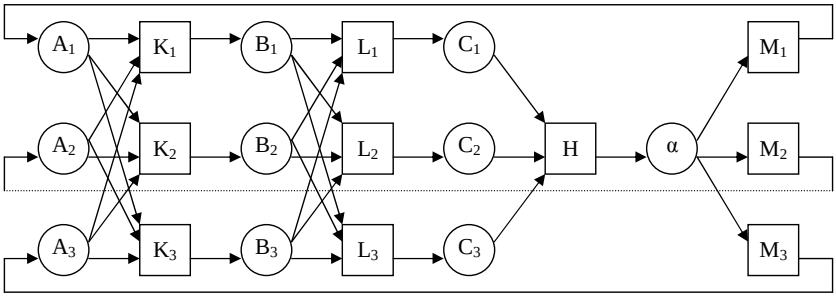

Рис. 5. ДТГ с последовательно-параллельной структурой.

2. Класс структур, не упоминающийся в литературе – **масштабируемые структуры с резервированием**, $\sigma(h_{вх})>\varphi(h_{вых})+2$. В приведенном на рис. 6 примере сдерживающие распространение отказа вершины K, L имеют по три входа (**меньше** размера домена). Достоинством данного класса структур является возможность добавления узлов в домены без модификации используемых устройств коммутации и контроля (при этом структура с $\sigma=4$, $\varphi=1$ преобразуется в структуру с $\sigma=5$, $\varphi=1$).

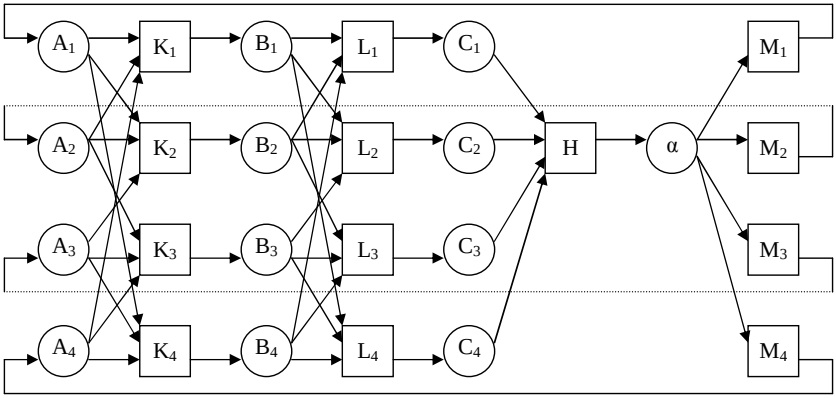

Рис. 6. ДТГ масштабируемой структуры с резервированием.

В **четвертой главе** решается задача оптимизации доменной структуры – выбор оптимального числа доменов, оптимальных характеристик доменов, варианта распределения устройств между доменами.

При этом в качестве показателя надежности используется вероятность безотказной работы (ВБР) за определенный срок.

В **разделе 4.1** для ускорения процесса расчета характеристик разрабатывается программа расчета ВБР системы по ДТГ. Программа работает путем формирования функции работоспособного состояния (ФРС) для ДТГ в виде совершенной дизъюнктивной нормальной формы (СДНФ). СДНФ формируется полным перебором возможных комбинаций состояний вершин (для сокращения перебора каждый узел домена представляется одной вершиной). Затем осуществляется переход к вероятностной функции и упрощение получившегося полинома.

В **разделе 4.2** анализируется характер зависимости ВБР от параметров доменной структуры – числа доменов, устойчивости доменов, размера доменов. С этой целью для каждого из трех параметров рассматриваются структуры, в которых изменяется только данный параметр. С помощью программы расчета вычисляются ВБР для некоторого количества структур, после чего делаются выводы о характере рассматриваемых зависимостей.

Основные результаты сравнительного анализа структур:

1. Эффект от увеличения устойчивости доменов быстро снижается с ее повышением. Для высоких начальных значений устойчивости дальнейшее ее повышение может приводить к ухудшению показателей системы. Влияние устойчивости на показатели системы выше при сравнительно высокой ВБР используемых УКК по сравнению с ВБР используемых ВУ (рис. 7, здесь и далее логарифмическая ВБР системы рассчитывается как –lg(1–ВБР)).

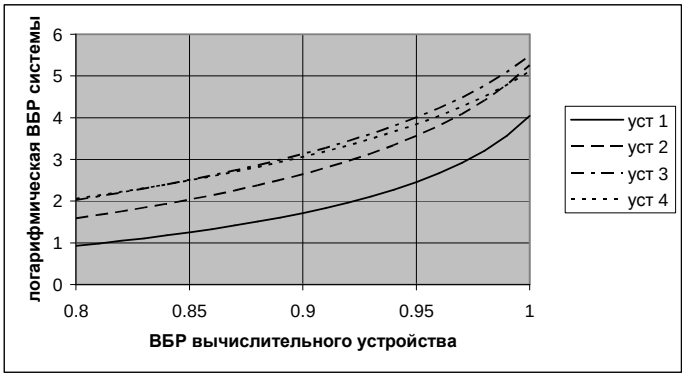

Рис. 7. Зависимость ВБР системы от ВБР ее устройств при различной устойчивости доменов системы (2 домена, σ=6).

2. Эффект от увеличения размера доменов может носить ступенчатый характер – ВБР системы меняется скачком при определенных значениях размера. Влияние размера на показатели не зависит от сравнительной ВБР используемых УКК и ВУ (рис. 8).

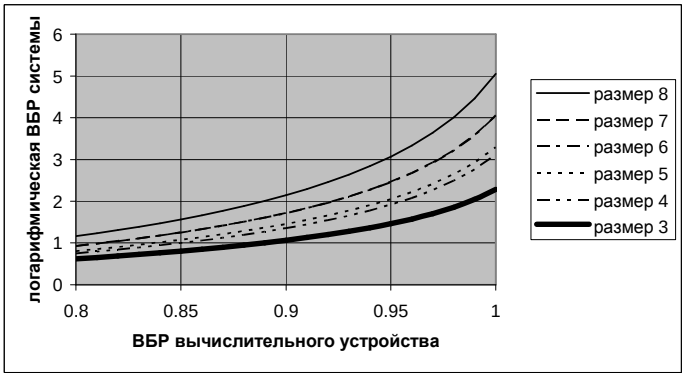

Рис. 8. Зависимость ВБР системы от ВБР ее устройств при различном размере доменов системы (2 домена, φ=1).

3. Для заданных значений (φ, σ) и вероятностей безотказной работы устройств системы существует некоторое оптимальное число доменов d. Оно увеличивается при сравнительно высокой ВБР используемых УКК по сравнению с ВБР используемых ВУ (рис. 9).

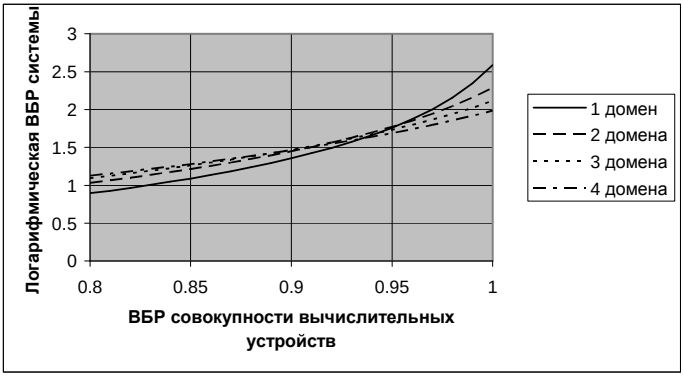

Рис. 9. Зависимость ВБР системы от ВБР ее устройств при различном числе доменов системы (φ=1, σ=3).

4. Для повышения эффективности распределения устройств системы между доменами следует производить его так, чтобы ВБР узлов различных доменов были близки друг к другу.

В **разделе 4.3** на основании анализа полученных результатов формулируется и обосновывается методика синтеза вычислительных систем с доменной структурой. Методика носит эвристический характер, поскольку сложность зависимости между характеристиками структуры системы и итоговыми показателями ее надежности затрудняет создание точного алгоритма, позволяющего найти оптимальное решение. Однако полученные рекомендации позволяют предложить порядок модификации структуры системы с целью получения требуемых характеристик без неоправданно высоких затрат.

Основные рекомендации методики сводятся к следующему.

1. Повышение устойчивости доменов целесообразно применять для повышения надежности системы в тех случаях, когда ВБР УКК существенно выше ВБР ВУ. Повышение характеристик этим способом имеет предел.

2. Повышение размера доменов целесообразно применять для повышения надежности системы в тех случаях, когда ВБР УКК и контроля сравнима с ВБР ВУ, а также в тех случаях, когда повышение устойчивости доменов без повышения их размеров невозможно (при $\sigma=\varphi+2$).
3. Выбор количества доменов в системе и распределения устройств между ними целесообразно осуществлять **после** выбора устойчивости и размеров доменов (данные показатели оказывают значительное влияние на оптимальное число доменов). Распределение устройств между доменами целесообразно осуществлять таким образом, чтобы ВБР узлов различных доменов были близки друг к другу и были существенно ниже ВБР используемых УКК.

Результатом применения методики является структура, удовлетворяющая требованиям по надежности или структура с характеристиками, близкими к максимально возможным при данных условиях.

В **пятой главе** рассматривается задача синтеза на примере прототипа ИУССН на основе СБИС программируемой логики семейства Stratix.

В **разделе 5.1** определяется функциональный состав системы. Для синтеза системы-прототипа используется инструментальная ЭВМ и три высоконадежных платы, включающих в себя СБИС ПЛ Stratix фирмы Altera. Для контроля надежности платы связываются друг с другом по LVDS-интерфейсу. В качестве вычислительного ядра системы используется готовый процессорный модуль Nios, применяемый в системах на кристалле.

В **разделе 5.2** производится синтез структуры системы-прототипа с использованием разработанного подхода. На рис. 10 приведен пример структуры узла домена. Здесь доменный коммутатор – устройство, принимающее данные от трех узлов домена и сравнивающее их друг с другом. На основании сравнения производится диагностика состояния отдельных устройств системы.

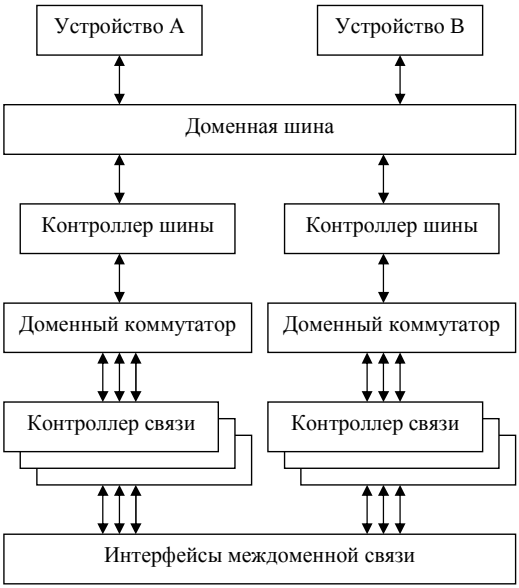

Рис. 10. Функциональная схема узла домена.

В **разделе 5.3** сформулированы основные требования к новым устройствам, входящим в состав системы прототипа: доменной шине, доменному коммутатору, контроллеру связи. В **разделе 5.4** рассмотрены основные проблемы доменной организации: проблема синхронизации вычислений, проблема конфигурации и реконфигурации системы. Предложены пути их решения.

В **заключении** формулируются основные результаты работы и направления дальнейших исследований.

ОСНОВНЫЕ РЕЗУЛЬТАТЫ

1. Предложена модель для представления структур ИУССН, позволяющая анализировать процессы распространения отказов и выявлять условия, необходимые для обеспечения надежности и безопасности. Модель построена в виде динамического типизированного графа (ДТГ), имеющего вершины, принадлежащие различным классам и типам, помеченные символом состояния вершины из определенного множества возможных состояний. Разработана система правил построения и модификации ДТГ, позволяющая решать задачу синтеза структуры ИУССН.
2. Определено отношение порядка по комбинированному критерию надежности, безопасности и стоимости на множестве ДТГ. Доказано, что ДТГ из множества максимальных элементов могут быть разбиты на непересекающиеся узлы доменов – ациклические связные подграфы без однотипных вершин, связанные друг с другом начальными и концевыми вершинами и обладающие возможностью сдерживать процессы распространения отказов.
3. В множестве доменных структур выделен класс новых структур – масштабируемые структуры с резервированием, позволяющие повышать уровень надежности без изменения используемых блоков.
4. Разработана программа расчета вероятности безотказной работы системы по ДТГ. Рассчитаны функциональные зависимости показателей надежности системы от параметров доменной структуры. Определены основные правила разбиения системы на домены. На основе данных результатов разработана методика синтеза ИУССН с доменной структурой.
5. Разработана структура прототипа ИУССН и определены функциональные спецификации к ее блокам. Обоснован функциональный состав системы-прототипа, предназначенной для экспериментальной проверки теоретических положений по синтезу структур ИУССН.

ПУБЛИКАЦИИ ПО ТЕМЕ ДИССЕРТАЦИИ

1. Глухих М.И. Оптимизация структуры информационно-управляющей системы специального назначения по критерию надежности // Научно-технические ведомости СПбГТУ. – 2006. №4. – С. 39-44.
2. Глухих М.И. Формализация представления отказоустойчивых систем при проектировании структуры системы // Информационно-управляющие системы. – 2005. №3. – С. 27-35.
3. Глухих М.И. Расчет показателей надежности по модели структуры вычислительной системы // Вычислительные, измерительные и управляющие системы: Сборник научных трудов / под ред. Ю.Б. Сениченкова. – СПб.: СПбГПУ, 2005. – С. 57-64.
4. Глухих М.И., Мелехин В.Ф. Методика синтеза и анализа высоконадежных схем // Материалы VIII всероссийской конференции «Фундаментальные исследования в технических университетах». – СПб.: СПбГПУ, 2004. – С. 145.
5. Глухих М.И., Максименко С.Л., Мелехин В.Ф. Методология и инструментальные средства создания специализированных процессоров // XXIX неделя науки СПбГТУ. Часть V: Материалы межвузовской научной конференции. – СПб.: СПбГТУ, 2000. – С. 36-38.
6. Глухих М.И., Мелехин В.Ф. Разработка и исследование специализированного процессора для отказоустойчивой системы // XXX юбилейная неделя науки СПбГТУ. Часть VII: Материалы межвузовской научной конференции. – СПб.: СПбГТУ, 2001. – С. 152.