На правах рукописи

Мамутова Ольга Вячеславовна

МЕТОДЫ И ИНСТРУМЕНТАЛЬНЫЕ СРЕДСТВА АНАЛИЗА ВЛИЯНИЯ ОДИНОЧНЫХ СБОЕВ В КЭШ-ПАМЯТИ НА РАБОТУ СПЕЦИАЛИЗИРОВАННЫХ ПРОЦЕССОРОВ

Специальность 05.13.05 –
Элементы и устройства вычислительной техники и систем управления

АВТОРЕФЕРАТ

диссертации на соискание ученой степени
кандидата технических наук

Санкт-Петербург – 2017

Работа выполнена на кафедре компьютерных систем и программных технологий в федеральном государственном автономном образовательном учреждении высшего образования «Санкт-Петербургский политехнический университет Петра Великого».

Научный руководитель: кандидат технических наук, доцент
Филиппов Алексей Семенович

Официальные оппоненты: **Мурсаев Александр Хафизович**
доктор технических наук, профессор
кафедры вычислительной техники ФГАОУ ВО
«Санкт-Петербургский государственный
электротехнический университет «ЛЭТИ»
им. В.И.Ульянова (Ленина)»

Суворова Елена Александровна
кандидат технических наук, доцент кафедры
аэрокосмических компьютерных и
программных систем ФГАОУ ВО «Санкт-
Петербургский государственный университет
аэрокосмического приборостроения»

Ведущая организация: АО «**Научно-исследовательский институт точной механики**» (г. Санкт-Петербург)

Защита состоится 30 марта 2017 г. в 16 часов на заседании диссертационного совета Д 212.229.18 при ФГАОУ ВО «Санкт-Петербургский политехнический университет Петра Великого», расположенного по адресу: 195251, Санкт-Петербург, ул. Политехническая, д. 29, – в аудитории 325 девятого учебного корпуса.

С диссертацией можно ознакомиться в библиотеке ФГАОУ ВО «Санкт-Петербургский политехнический университет Петра Великого» и на сайте www.spbstu.ru.

Автореферат разослан «___» _____ 2017 года.

Ученый секретарь
диссертационного совета Д 212.229.18
кандидат технических наук, доцент _____ Васильев Алексей Евгеньевич

1. ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Актуальность темы исследования. Системы на кристалле (СнК) в бортовых приборах авиакосмической техники позволяют обрабатывать большие объемы информации, обеспечивая необходимую производительность при существующих ограничениях по массе и энергопотреблению приборов. Однако высокая степень интеграции делает СнК особо подверженными радиационным эффектам при воздействии ионизирующего излучения космического пространства.

Для современных полупроводниковых компонентов из всех радиационных эффектов наиболее вероятны одиночные сбои, при которых инвертируются значения отдельных битов информации в запоминающих элементах. Ошибки в слове памяти, вызванные одиночными сбоями, исчезают после операции записи в это слово. Однако за время присутствия ошибки в памяти информация с ошибкой может быть считана, что определяет уязвимость вычислительной системы к одиночным сбоям.

Кэш-память процессора может занимать существенную часть площади СнК и предназначена для хранения часто востребованных данных. Распространение ошибки при чтении из кэш-памяти может привести к ложным результатам или нарушению хода исполнения программы. Поэтому исследования, посвященные проблеме влияния одиночных сбоев в кэш-памяти на работу процессоров, являются актуальными.

Степень разработанности темы исследования. Анализ уязвимости вычислительной системы к одиночным сбоям необходим на каждом этапе проектирования для обоснованного выбора параметров узлов системы и верификации реализованных средств борьбы с последствиями ошибок. Подобный анализ включает в себя предсказание характеристик ионизирующего излучения, определение чувствительности микросхемы к одиночным радиационным эффектам, определение параметров потока одиночных сбоев и оценку влияния одиночных сбоев на работу процессора.

Анализу влияния одиночных сбоев в кэш-памяти на вычислительный процесс посвящены работы Р. Велазко и М. Николаидиса (TIMA lab), М. Реботенго (Politecnico di Torino), Л. Энтрены (Univ. Carlos II de Madrid), С. Мукерджи (Intel), А. Эджлали и Х. Асади (Sharif Univ. of Technol.), Б.З. Шмейлина (ИПИ РАН) и др.

Время жизни ошибки в кэш-памяти процессора сопоставимо с временем исполнения задач, поскольку определяется событиями самовосстановления при операциях записи и реализацией обнаружения и исправления с помощью средств борьбы с последствиями сбоев. Поэтому последствия сбоев в кэш-памяти необходимо оценивать с учетом характера вычислительной нагрузки. При этом большинство существующих методов анализа основано на использовании симуляторов архитектуры процессора или

симуляторов устройства на уровне RTL-описания, не позволяющих проводить эксперименты необходимой длительности. Поэтому для современных СнК, цикл проектирования которых постоянно сокращается, требуются более быстрые инструментальные средства анализа.

Целью работы является улучшение качества вычислительных систем в исполнении СнК, используемых в условиях приводящего к одиночным сбоям ионизирующего излучения космического пространства. Для создания необходимых для этого методов и инструментальных средств анализа поставлены следующие **задачи исследования**:

1. Анализ требований к методике проектирования кэш-памяти процессора, направленной на улучшение радиационной стойкости СнК.

2. Разработка комплекса аналитических моделей для быстрой оценки влияния одиночных сбоев в кэш-памяти на работу процессора, предназначенных для ранних этапов проектирования.

3. Анализ влияния одиночных сбоев в массиве строк и таблице тэгов кэш-памяти на работу процессора.

4. Разработка методов и инструментальных средств внесения неисправностей типа «сбой» в кэш-память процессора в СнК для этапа прототипирования на базе программируемых логических интегральных схем (ПЛИС).

5. Анализ характеристик функционирования типового RISC процессора при исполнении тестовых программ в присутствии ошибок в кэш-памяти.

6. Разработка рекомендаций по практическому применению результатов исследования.

Научная новизна:

1. Разработаны новые настраиваемые аналитические модели, позволяющие оценивать уязвимость вычислительной системы к одиночным сбоям в кэш-памяти с учетом характера вычислительной нагрузки, организации кэш-памяти, реализуемой для борьбы с ошибками избыточности и потока одиночных сбоев.

2. Разработана новая имитационная модель кэш-памяти, обеспечивающая проверку корректности аналитических моделей.

3. Установлены ранее неизвестные зависимости показателя уязвимости вычислительной системы к одиночным сбоям в кэш-памяти от характеристик вычислительной нагрузки, параметров кэш-памяти, характеристик реализуемой для борьбы с последствиями ошибок избыточности и интенсивности потока одиночных сбоев.

4. Предложен новый метод внесения неисправностей в массивы кэш-памяти физической модели СнК на базе ПЛИС, реализующий автономную эмуляцию сбоев с по-

мощью сети агентов внесения неисправностей под управлением тестируемого процессора. Метод включает в себя инструментальные средства оснащения, сбора и анализа результатов.

5. Сформулированы рекомендации по применению предложенных моделей и методов оценки показателя уязвимости вычислительной системы к одиночным сбоям в кэш-памяти при проектировании СнК.

Теоретическая значимость работы заключается в создании новых аналитических моделей влияния одиночных сбоев в кэш-памяти на работу процессора и выявлении новых закономерностей в функции показателя уязвимости вычислительной системы к одиночным сбоям в кэш-памяти.

Практическая значимость. Разработанные в работе методы и инструментальные средства анализа позволяют на этапе системного проектирования СнК оценивать вероятность информационного отказа процессора из-за одиночных сбоев в кэш-памяти и на этапе прототипирования обеспечивают проверку реализации избыточности для борьбы с их последствиями. Результаты исследования использованы в ООО «ЭсДиСи» при разработке модулей и архитектур бортовых сетей малых спутников, что подтверждается актом о внедрении. Результаты исследования использованы в НИОКР «Развитие центра трансфера технологий FPGA и ASIC Санкт-Петербургского государственного политехнического университета для решения задач Межвузовской лаборатории проектирования мультипроцессорных систем» и «Исследование фундаментальных свойств асинхронных многопроцессорных вычислительных структур в базисе перепрограммируемых логических кластеров». Отдельные результаты исследования использованы в учебном процессе в Санкт-Петербургском политехническом университете Петра Великого при подготовке бакалавров и магистров по направлениям 09.03.01 и 09.04.01 «Информатика и вычислительная техника», что подтверждается актом о внедрении.

Методы исследования. В работе использован комплексный метод исследований, включающий теоретический анализ и проверку полученных результатов в лабораторных условиях. Для теоретических исследований использованы методы системного анализа, теории вероятностей, комбинаторики, теории надежности и теории планирования эксперимента. Для построения моделей уязвимости процессора к одиночным сбоям в кэш-памяти использованы среды Mathematica и Möbius. Физический макет вычислительной системы, позволяющий вносить неисправности в кэш-память процессора, разработан с использованием сред Quartus II и Nios II SBT. Для оценки быстродействия СнК на базе ПЛИС использован временной анализатор TimeQuest. Оценка характеристик ионизирующего излучения выполнена в среде моделирования Crème.

Положения, выносимые на защиту:

1. Метод аналитической оценки влияния одиночных сбоев в кэш-памяти на работу процессора, позволяющий проводить быстрый сравнительный анализ возможных вариантов организации кэш-памяти на ранних этапах проектирования СнК. Аналитические модели влияния одиночных сбоев в кэш-памяти с типовыми параметрами на работу процессора.

2. Результаты теоретических исследований влияния одиночных сбоев в кэш-памяти на работу процессора, полученные на основе разработанных аналитических моделей и позволяющие выполнять обоснованный выбор параметров кэш-памяти процессора на ранних этапах проектирования.

3. Метод внесения неисправностей типа «одиночный сбой» в кэш-память на физической модели СнК на базе ПЛИС, обеспечивающий на этапе прототипирования проверку проектных решений и подтверждение характеристик процессора с кэш-памятью.

4. Рекомендации по использованию предложенных методов и инструментальных средств анализа влияния одиночных сбоев в кэш-памяти на работу процессоров при проектировании кэш-памяти специализированных процессоров в СнК с целью улучшения качества проектных решений.

Достоверность результатов обеспечена обоснованностью использованных теоретических подходов, допущений и ограничений, корректностью постановки задач, применением известных математических методов и подтверждается согласованием результатов теоретических исследований с исследованием на физической модели, а также подтверждается практическим применением результатов исследования.

Апробация результатов работы. Результаты работы доложены на шестнадцати конференциях: конференции «Будущее Российской космонавтики в инновационных разработках молодых специалистов» (г. Королёв, 2009 г.), межрегиональных конференциях «Региональная информатика» (СПб, 2009–2010 гг.), XIII–XVI всероссийских конференциях “Фундаментальные исследования и инновации в национальных исследовательских университетах” (СПб, 2009–2012 гг.), международной научно-практической конференции «XXXIX Неделя науки СПбГПУ» (СПб, 2010 г.), XVI международной научно-практической конференции «Системный анализ в проектировании и управлении» (СПб, 2012 г.), международном семинаре «Verification of Embedded Systems» (СПб, 2013 г.), XX–XXI международных научно-методических конференциях «Высокие интеллектуальные технологии и инновации в национальных исследовательских университетах» (СПб, 2013–2014 гг.), международной конференции «Circuits, Systems and Signal Processing» (СПб, 2014 г.), международной конференции «1st Symposium on Space Edu-

cational Activities» (г. Падуя, 2015 г.), международной конференции «17th Conference of Open Innovations Association (FRUCT)» (г. Ярославль, 2015 г.), VII всероссийской научно-технической конференции «Проблемы разработки перспективных микро- и наноэлектронных систем» (г. Зеленоград, 2016 г.).

Публикации. По материалам диссертационного исследования опубликовано двадцать три печатные работы, в том числе шесть – в изданиях, включенных в перечень рецензируемых научных изданий ВАК.

Личный вклад автора. Все научно-технические результаты, выносимые на защиту, получены автором самостоятельно. Постановка задачи выполнена совместно с научным руководителем к.т.н., доц. каф. КСПТ Филипповым А.С. Автоматизация оснащения СнК средствами внесения неисправностей в память выполнена совместно с асп. каф. КСПТ Ненашевым О.В.

Структура и объем диссертации. Диссертация состоит из введения, четырех глав, заключения, библиографии, включающей 150 наименований, и десяти приложений. Работа изложена на 165 страницах, содержит 116 страниц основного текста, включая 24 рисунка и 16 таблиц.

2. ОСНОВНОЕ СОДЕРЖАНИЕ РАБОТЫ

Во введении обоснована актуальность темы, определены цели и задачи работы, сформулированы выносимые на защиту положения.

В первой главе проведен анализ проблемы одиночных сбоев, возникающей при проектировании специализированных вычислительных систем; описаны модели и методы, применяемые на разных этапах проектирования.

Описаны подходы к определению параметров потока одиночных сбоев как исходных данных при проектировании архитектуры устройства. Выполнен аналитический обзор синтезируемых процессорных ядер и определены настраиваемые параметры кэш-памяти. Показан жизненный цикл ошибки, вызываемой в кэш-памяти одиночным сбоем, и механизмы многоуровневого реагирования вычислительной системы на такую ошибку. Проведен обзор методов борьбы с ошибками в памяти. Показаны особенности борьбы с ошибками в кэш-памяти процессора. Определены требования к инструментальным средствам анализа при платформенно-ориентированном подходе к проектированию. Дано определение показателя уязвимости как критерия оценки чувствительности вычислительной системы к одиночным сбоям в кэш-памяти. Проведен анализ существующих методов и результатов оценки показателя уязвимости.

При платформенно-ориентированном проектировании основные усилия разработчика по сужению пространства возможных решений сосредоточены на этапе сис-

темного проектирования, после завершения которого выполняется быстрый переход к прототипированию с использованием ПЛИС. Основным требованием к методам анализа уязвимости вычислительной системы к одиночным сбоям в кэш-памяти является сокращение времени оценки.

На ранних этапах проектирования для исследования функционирования вычислительной системы используются методы аналитической оценки. Однако для оценки показателя уязвимости существующие аналитические модели требуют предварительной обработки данных симулятора с целью определения характеристик вычислительной нагрузки.

Для этапа прототипирования на базе ПЛИС необходимы методы внесения неисправностей, которые обеспечивают необходимую скорость оценки. Однако для реализации экспериментов по внесению неисправностей в кэш-память существующие методы требуют значительной дополнительной площади кристалла или ограничены в применении архитектурой ПЛИС.

Таким образом, необходимость учета характера вычислительной нагрузки значительно ограничивает скорость оценки показателя уязвимости вычислительной системы к одиночным сбоям в кэш-памяти. Поэтому с целью быстрой оценки показателя уязвимости в данной работе предлагается новый аналитический подход для ранних этапов проектирования и новый метод внесения неисправностей для этапа прототипирования на базе ПЛИС.

Во второй главе представлен аналитический подход к оценке показателя уязвимости вычислительной системы к одиночным сбоям в кэш-памяти, который позволяет выбрать параметры кэш-памяти на начальном этапе проектирования СнК.

Определено, что информационный отказ возникает при чтении из кэш-памяти значения с ошибкой, которая не может быть исправлена. Если при этом ошибка может быть обнаружена, то информационный отказ будет обнаружен и может быть исправлен за счет избыточности на следующем уровне системы. В случае невозможности обнаружения, ошибка распространится вверх или вниз по иерархии памяти, т.е. приведет к необнаруженному информационному отказу.

Целью функционирования вычислительной системы задано безотказное исполнение программы в условиях появления одиночных сбоев в кэш-памяти. Тогда кэш-память можно рассматривать как изолированный узел вычислительной системы, представленный набором аналитических зависимостей (накопления ошибок, быстродействия кэш-памяти, поведения программы и реакции системы на ошибку), как показано на рисунке 1.

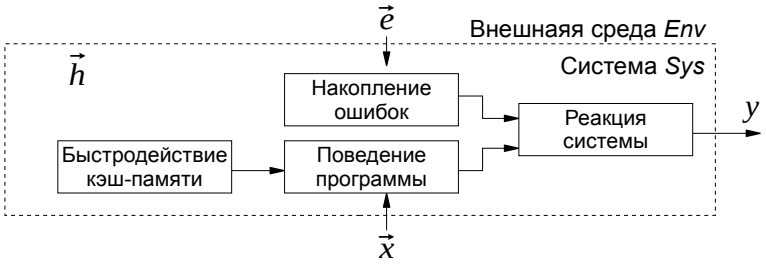

Рисунок 1. Блочная модель для оценки уязвимости вычислительной системы к одиночным сбоям в кэш-памяти

Таким образом, кэш-память рассматривается как динамическая система *Sys* в условиях воздействий внешней среды *Env* во времени *t*. Собственные параметры $\vec{h}$ системы *Sys* включают параметры реализованной для борьбы с последствиями ошибок избыточности и параметры кэш-памяти. Входные воздействия $\vec{x}$ задают характер потока обращений процессора в кэш-память. Воздействия внешней среды $\vec{e}$ характеризуют процесс накопления ошибок в кэш-памяти. В качестве выходной переменной *y* выступает показатель уязвимости – вероятность информационного отказа после появления одиночного сбоя в кэш-памяти.

Унифицированный принцип работы кэш-памяти позволяет представить реакцию системы на появление ошибки в строке кэш-памяти или записи таблицы тэгов логическими индуктивными моделями в виде деревьев событий, где исходным событием является обращение процессора к слову с ошибкой. Реакция системы зависит от типа обращения к кэш-памяти (чтение/запись, промах/попадание) и стратегий записи и загрузки. Кроме того, для таблицы тэгов учитывается расположение ошибок в записи, определяющее вероятности ложного промаха, ложного попадания, множественного попадания, ложной обратной записи и ложного отсутствия обратной записи. Первым барьером защиты от ошибок выступает введенная в кэш-память избыточность. Вторым барьером выступает механизм самовосстановления кэш-памяти, когда в ходе исполнения программы в слово с ошибкой записываются новые данные. Вероятные исходы включают самовосстановление, маскирование, исправление, обнаруженный информационный отказ и необнаруженный информационный отказ.

Определение вероятностей исходов в соответствии с полученными деревьями событий позволяет получить аналитическое представление функций реакции системы на ошибки в таблице тэгов и в массиве слов для выбранных параметров кэш-памяти.

Использование известных законов для формализации остальных компонентов модели (процесс накопления ошибок, быстродействие кэш-памяти и поведение программы) позволяет получить искомую аналитическую модель.

При этом процесс накопления ошибок определяется временем t между одиночными сбоями в одной ячейке памяти с плотностью распределения

$$f_{err}(t) = \lambda e^{-\lambda t}, \quad (1)$$

где λ – интенсивность потока одиночных сбоев в слове кэш-памяти.

Поведение программы представлено набором функций: функцией локальности обращений, вероятностями записи и промаха и функцией среднего времени между обращениями в память.

Для характеристики локальности обращений выбрана модель независимых обращений, где распределение адреса обращения представлено как

$$P_A = \left\{ p_A(n) \mid n \in [0; N-1], \sum_{n=0}^{N-1} p_A(n) = 1 \right\}, \quad (2)$$

где N – размер кэш-памяти.

Для представления вероятности промаха используется степенная зависимость

$$p_{miss}(N) = \beta (N+1)^{-\alpha}, \quad (3)$$

где α и β характеризуют локальность исполняемой программы.

Быстродействие кэш-памяти определяется средним временем между обращениями процессора к памяти:

$$t_0 = t_{hit}(N, r) + t_{miss} \cdot p_{miss}(N) + t_{wait}, \quad (4)$$

где $t_{hit}(N,r)$ – время обращения в кэш-память при кэш-попадании в зависимости от размера кэш-памяти N и характеристик избыточности r, t_{miss} – среднее дополнительное время обращения при кэш-промахе, определяемое в основном временем доступа к памяти следующего уровня иерархии и задаваемое в качестве собственного параметра разрабатываемой модели, t_{wait} – среднее время до следующего обращения.

Предложен следующий алгоритм получения аналитического выражения показателя уязвимости:

1. В терминах процесса накопления ошибок и реакции системы на ошибки определить последовательность событий, приводящих к информационному отказу.

2. Определить вероятности для каждого события из этой последовательности. Считая обращения в память независимыми событиями, определить вероятность реализации последовательности событий как произведение их вероятностей.

3. Перейти от модели дискретных событий к модели в непрерывном времени для обеспечения скорости аналитических вычислений.

4. Выполнить необходимое интегрирование полученного выражения по времени для получения выражения показателя уязвимости.

В третьей главе представлен пример использования предложенного аналитического подхода к оценке влияния одиночных сбоев в кэш-памяти на работу процессоров и рекомендации по проектированию кэш-памяти процессора в СнК на базе ПЛИС.

Рассмотрена кэш-память, защищенная кодом с исправлением одиночных и обнаружением двойных ошибок (SECDED). Представлены результаты выполнения алгоритма для получения частного аналитического выражения показателя уязвимости к одиночным сбоям в слове массива строк.

1. Определена последовательность событий, приводящая к обнаруживаемому информационному отказу. Пусть ошибка появилась в слове *n* строки кэш-памяти. Тогда информационный отказ возможен на *i*-ом обращении после появления второй ошибки в слове на *j*-ом обращении, если после появления первой ошибки (*i*–1 обращений) не произошло самовосстановление и после появления второй ошибки сам информационный отказ не произошел ранее (*i*–*j* обращений). Последовательность событий, приводящая к не обнаруживаемому информационному отказу, определяется аналогично.

2. Тогда вероятность информационного отказа на *i*-ом обращении после появления повторной ошибки на *j*-ом обращении определяется выражением

$$\begin{aligned} &p\left(x=i, err=j\right) = p_A\left(n\right)\cdot p_{word\_fail} \times \\ &\times\left[1-p_A\left(n\right)\cdot p_{word\_recover} - p_{block}\left(n\right)\cdot p^{CE}_{block\_recover}\right]^{j-1} \times \\ &\times\left[1-p_A\left(n\right)\cdot p_{word\_fail} - p_A\left(n\right)\cdot p_{word\_recover} - p_{block}\left(n\right)\cdot p^{DE}_{block\_recover}\right]^{i-j}, \end{aligned} \tag{5}$$

где вероятность информационного отказа p_{word_fail}, вероятность самовосстановления для слова $p_{word\_recover}$, и вероятности самовосстановления для строки при исправляемых и обнаруживаемых ошибках $p^{CE}_{block\_recover}$, $p^{DE}_{block\_recover}$ определяются как вероятности исходов с помощью деревьев событий.

3. Переходя к непрерывному времени, можно определить вероятность отказа в момент времени $T_i = it_0$ следующим образом:

$$\begin{aligned} &p\left(T_i, T_j\right) = p_A\left(n\right)\cdot p_{word\_fail}\cdot e^{-\left(p_A(n)\cdot p_{word\_recover} + p_{block}(n)\cdot p^{CE}_{block\_recover}\right)T_j/t_0} \times \\ &\times e^{-\left(p_A(n)\cdot p_{word\_fail} + p_A(n)\cdot p_{word\_recover} + p_{block}(n)\cdot p^{DE}_{block\_recover}\right)\left(T_i - T_j\right)/t_0}. \end{aligned} \tag{6}$$

4. Проводя усреднение по вероятности появления повторной ошибки и интегрируя полученное выражение по времени, получаем выражение показателя уязвимости *VF* – вероятности того, что появившаяся в слове *n* ошибка приведет к обнаруживаемому информационному отказу за время наблюдения *t*.

В результате значение показателя уязвимости может быть получено аналитически из выражения:

$$VF(t,n) = \frac{1}{t_0} \int_0^t \int_0^{Ti} f_{err}(T_j)\, p(T_i, T_j)\, dT_j dT_i. \quad (7)$$

Выражение показателя уязвимости к одиночным сбоям в записи таблицы тэгов получается аналогично.

Разработаны аналитические модели для оценки показателя уязвимости при реализации типичных способов введения избыточности в кэш-память. Для проверки правильности получаемых моделей дополнительно разработана имитационная модель, которая, однако, не может быть рекомендована как средство проектирования из-за низкой скорости получения статистически значимых результатов.

Примеры зависимости показателя уязвимости от размера кэш-памяти без помехоустойчивого кодирования, полученные для значений из таблицы 1, показаны на рисунках 2 и 3. Примеры зависимостей в случае защиты кэш-памяти SECDED кодом представлены на рисунке 4. В ходе исследования выделены следующие закономерности в функции показателя уязвимости.

При длительности времени наблюдения, когда вероятность обращения к записи с ошибкой близка к единице, во всех случаях показатель уязвимости практически не зависит от времени наблюдения.

При одиночном сбое в записи таблицы тэгов без помехоустойчивого кодирования исходы делятся преимущественно между самовосстановлением и распространением ошибки в память верхнего уровня в соотношении, определяемом вероятностью промаха и вероятностью записи. При этом вероятность распространения ошибки в память нижнего уровня мала. Поэтому сквозная запись оказывается эффективным барьером, исключающим распространение ошибок в память верхнего уровня (рисунок 2).

При одиночном сбое в слове массива строк без помехоустойчивого кодирования значение показателя уязвимости определяется вероятностью промаха и стремится к величине $(1 - p_{write})$ (рисунок 3).

В случае применения SECDED кода существует диапазон значений интенсивности λ, когда значение показателя уязвимости меняется пропорционально изменению значения λ.

При этом при одиночных сбоях в записи таблицы тэгов, для кэш-памяти со сквозной записью показатель уязвимости равен нулю, а для кэш-памяти с обратной записью показатель уязвимости определяется степенью ассоциативности и вероятностями промаха и записи (рисунок 4, *а*).

Таблица 1

Исходные данные при оценке показателя уязвимости

Параметр модели	Значение
Размер адресного пространства, байт	2^{32}
Размер строки кэш-памяти, *block_size*, байт	16
Число наборов (степень ассоциативности)	1
Вероятность записи, p_{write}	0,3
Параметры функции p_{miss}, α и β соответственно	0,5 и 2
Интенсивность одиночных сбоев, λ, 1/с	10^{-6}
Среднее время обращения при кэш-промахе, t_{miss}, с	10^{-7}
Среднее время до следующего обращения, t_{wait}, с	0
Период просеивания, с	5
Время наблюдения, *t*, с	1000

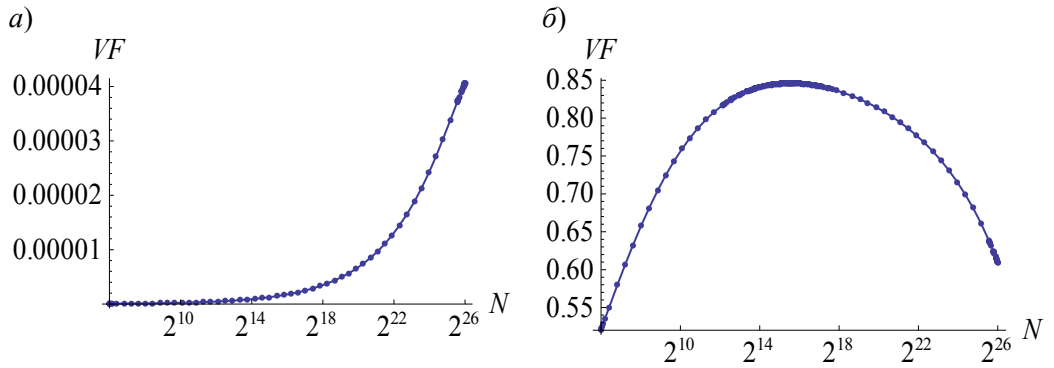

Рисунок 2. Показатель уязвимости к одиночному сбою в записи таблицы тэгов в зависимости от размера кэш-памяти: при стратегиях сквозной (*а*) и обратной записи (*б*) (без помехоустойчивого кодирования таблицы тэгов)

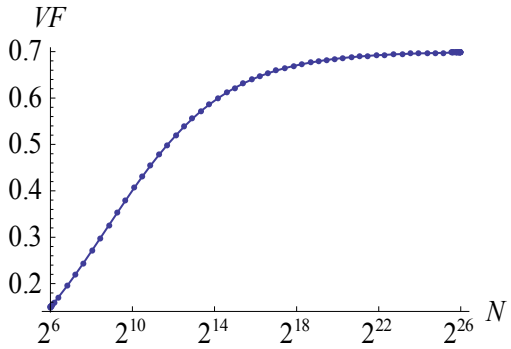

Рисунок 3. Показатель уязвимости к одиночному сбою в слове массива строк в зависимости от размера кэш-памяти (без помехоустойчивого кодирования массива строк)

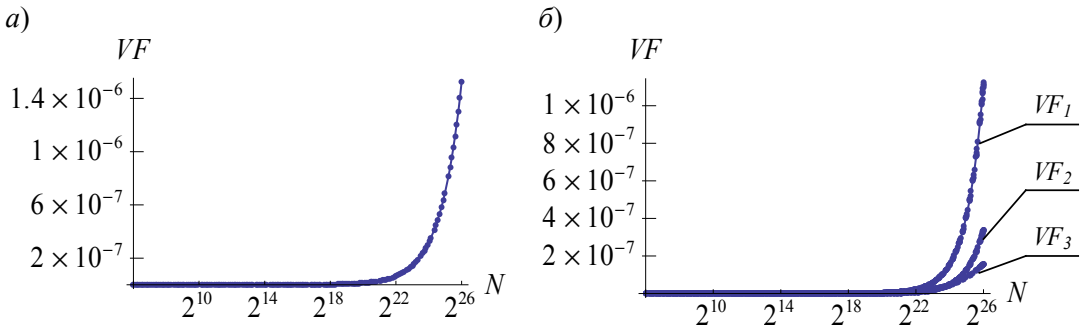

Рисунок 4. Показатель уязвимости к одиночному сбою в записи таблицы тэгов с SECDED кодированием в кэш-памяти с обратной записью (*а*) и в слове массива строк с SECDED кодированием (*б*): только с маскированием (*VF*1), с исправлением (*VF*2) и с просеиванием (*VF*3)

При одиночных сбоях в слове массива строк (см. рисунок 4, *б*) реализация исправления ошибок (*VF*2) вместо маскирования (*VF*1) не приводит к существенному дополнительному уменьшению значения показателя уязвимости. Более того, кривая зависимости показателя уязвимости при реализации просеивания (*VF*3) для реализуемых периодов просеивания приближается к кривой *VF*2.

Дополнительно решена задача оценки быстродействия и аппаратных затрат для определения эффективности типовых способов введения избыточности в кэш-память процессора. Для этого разработаны модификации процессора mor1kx, позволяющие использовать бит паритета и помехоустойчивое кодирование в массивах памяти. Анализ выполнен для реализации процессора на базе ПЛИС семейства Cyclone V с блоками памяти типа M10K. Проведенный анализ, дополненный результатами исследования функции показателя уязвимости, позволил сформулировать следующие рекомендации по реализации избыточности в кэш-памяти:

- Для массивов памяти следует использовать метод чередования, когда логически смежные биты информации хранятся в физически не смежных ячейках памяти. Это не только обеспечивает эффективность помехоустойчивого кодирования в случае многократных сбоев, но и позволяет упростить оценку показателя уязвимости.
- Для массивов памяти следует использовать как минимум бит четности. Это дает возможность определять появление информационных отказов без значительного увеличения аппаратных затрат или существенной потери быстродействия.
- В случае, когда для проектируемой системы допустимо соответствующее увеличение объема кэш-памяти памяти и потеря быстродействия до 50%, для массивов памяти следует использовать SECDED кодирование. Это приводит к существенному уменьшению величины показателя уязвимости, даже без реализации исправления или просеивания ошибок.

Таким образом, предложенный аналитический подход позволяет оценивать зависимость показателя уязвимости от любого параметра модели для кэш-памяти произвольного уровня. Такая быстрая оценка может быть использования для обоснованного выбора параметров кэш-памяти процессора на ранних этапах проектирования.

В четвертой главе представлено решение задачи создания экспериментального окружения для внесения неисправностей в кэш-память на базе ПЛИС. Предложен подход к автономному внесению неисправностей, основанный на использовании сети агентов внесения неисправностей под управлением встроенного процессора, предназначенный для проверки проектных решений и подтверждения характеристик кэш-памяти на этапе прототипирования.

Агентом внесения неисправностей выступает блок-саботажник, который получает от процессора команды с маской и адресом слова в памяти. При получении команды саботажник отключает память от основного интерфейса и выполняет процедуру чтение–изменение–запись для инверсии требуемых битов. Реализация такого саботажника для простой двухпортовой 32-разрядной памяти размером 512 байт на базе микросхемы ПЛИС семейства Cyclone V потребовала 114 логических блоков и 76 регистров.

Реализованный метод автономного внесения неисправностей в кэш-память заключается в использовании процессора в роли как контроллера внесения неисправностей, так и генератора вычислительной нагрузки, монитора эксперимента и устройства первичного анализа экспериментальных данных. Таким образом, программное обеспечение процессора делится на управляющую программу, реализующую эксперимент, и тестируемую программу. Независимость исполнения двух программ обеспечивается разделением памяти и контекстов управляющей и тестируемой программ.

Дополнительные аппаратные затраты при реализации предлагаемого метода внесения неисправностей определяются числом добавляемых в устройство саботажников и разрядностью двух таймеров для контроля хода эксперимента. При этом управляющая программа в случае недостаточности ресурсов внутрикристальной памяти может быть размещена во внешней памяти.

Оснащение СнК агентами внесения неисправностей выполняется на уровне RTL-описания. Проблему трудоемкости ручного оснащения предлагается решать путем автоматизации с помощью средства реинжиниринга PHRT. Создаваемая в PHRT гибридная модель устройства содержит одновременно исходное высокоуровневое описание системы и результаты его синтеза. Это позволяет автоматизировать все этапы оснащения: разделение системы на интересующие исследователя части, поиск синтезированных блоков памяти, добавление саботажников, а также организацию новых связей между элементами системы в плоском пространстве сигналов.

Преимущество предложенного подхода к внесению неисправностей на базе ПЛИС заключается в эффективном использовании ресурсов внутрикристальной памяти и независимости от архитектуры ПЛИС. Кроме того, предложенный подход может быть использован не только для кэш-памяти, но и для других блоков памяти СнК.

Разработан стенд для проведения экспериментов по внесению неисправностей в кэш-память процессора niosII с RISC-архитектурой. Разработанная управляющая программа включает следующие процедуры: инициализация эксперимента, эталонный запуск тестируемой программы, запуск серии экспериментов, переключение контекста между управляющей и тестируемой программами, внесение неисправностей, а также

контроль корректного исполнения тестируемой программы. Объем памяти управляющей программы составляет 130 КБ.

Разработан набор синтетических тестовых программ, позволяющих с помощью созданного экспериментального окружения проверить адекватность разработанных аналитических моделей уязвимости процессора к одиночным сбоям в кэш-памяти. Для исследования выбрана кэш-память данных фиксированного размера, для которой в разработанных тестовых программах обеспечивается близкое к равномерному распределение адресов обращений. Характеристики исполнения тестовых программ (вероятности промаха и записи) получены с помощью разработанных средств профилирования и использованы при оценке показателя уязвимости с помощью аналитической модели.

Для каждой тестовой программы выполнена серия из тысячи экспериментов. Полученные результаты оценки представлены в таблице 2.

Таблица 2

Сравнение аналитической и экспериментальной оценок показателя уязвимости кэш-памяти данных

Характеристика	Синтетический тест				
	1	2	3	4	5
Вероятность промаха, p_{miss}	0,043	0,251	0,333	0,416	0,498
Вероятность записи, p_{write}	0,332	0,332	0,373	0,426	0,329
Экспериментальная оценка показателя уязвимости, *VF*	0,657	0,513	0,386	0,339	0,294
Аналитическая оценка показателя уязвимости, *VF*	0,631	0,486	0,403	0,337	0,281

Максимальное расхождение результатов оценки составило 5,6%, среднее – 3,8%. Расхождение результатов оценки показателя уязвимости, получаемых в результате аналитической оценки и в результате эксперимента по внесению неисправностей, объясняется статистической погрешностью экспериментальной оценки и погрешностью генератора случайных чисел, использованного для формирования адресов вносимых сбоев. Малое расхождение результатов оценки показателя уязвимости показывает корректность предложенного подхода к аналитической оценке, что дает основание рекомендовать данный подход для практического применения.

В **Заключении** описано место предложенных методов и инструментальных средств в ходе проектирования кэш-памяти процессора СнК при платформенно-ориентированном подходе:

1. Подход к аналитической оценке показателя уязвимости вычислительной системы к одиночным сбоям в кэш-памяти предназначен для использования на ранних этапах проектирования и обеспечивает возможность обоснованного выбора архитектуры проектируемой системы.

2. Метод и инструментальные средства внесения неисправностей в кэш-память процессора на базе ПЛИС дополняют существующие методы внесения неисправностей

в отдельные триггеры СнК, обеспечивая проверку реализации средств борьбы с последствиями ошибок в кэш-памяти, а также уточнение оценки показателя уязвимости.

3. Метод и инструментальные средства внесения неисправностей в кэш-память процессора на базе ПЛИС также могут быть использованы для характеризации программ с целью определения поправочных коэффициентов, необходимых для анализа и интерпретации результатов физических испытаний.

3. ОСНОВНЫЕ РЕЗУЛЬТАТЫ РАБОТЫ

1. Проведен анализ методов и подходов к проектированию систем на кристалле с кэш-памятью для работы в условиях одиночных сбоев. Выявлена необходимость разработки аналитических моделей для быстрой оценки уязвимости вычислительной системы к одиночным сбоям в кэш-памяти.

2. Предложен не использующий симулятор процессора подход к аналитической оценке показателя уязвимости вычислительной системы к одиночным сбоям в кэш-памяти. Данный подход позволил разработать аналитические модели для оценки показателя уязвимости вычислительной системы к одиночным сбоям в кэш-памяти с типовыми параметрами.

3. На основе предложенного подхода к аналитической оценке и результатов временного анализа сформулированы рекомендации по выбору параметров кэш-памяти по совокупному показателю «уязвимость-производительность» на начальных этапах системного проектирования для типового RISC-процессора на базе ПЛИС.

4. Предложен, разработан и реализован в виде программно-аппаратного комплекса метод внесения неисправностей типа «одиночный сбой» в блоки памяти на базе ПЛИС, позволяющий выполнять проверку реализованных методов повышения надежности и обеспечивающий эффективное использование ресурсов кристалла при сохранении высокой скорости проведения экспериментов.

5. Выполнена проверка адекватности разработанных аналитических моделей с использованием предложенного метода внесения неисправностей. Максимальное расхождение результатов проверки на физической модели относительно аналитической оценки составило единицы процентов, что говорит об адекватности разработанных аналитических моделей.

6. Сформулированы рекомендации по использованию предложенных в работе методов и средств в современных маршрутах проектирования, обеспечивающие высокую скорость и качество проектирования.

7. Предложенные в работе методы и инструментальные средства практически апробированы при разработке универсальных модулей бортовых приборов малых космических аппаратов.

ПУБЛИКАЦИИ ПО ТЕМЕ ДИССЕРТАЦИИ

Публикации в изданиях из перечня ВАК:

1. **Мамутова О.В.**, Филиппов А.С. Разработка модели иерархической оперативной памяти вычислительной системы // Научно-технические ведомости СПбГПУ. 2011. т. 128. № 4.С. 75–81.
2. **Mamoutova O.V.** Processor-Driven Emulated Upset-Like Fault Injection for Memory Validation // Университетский научный журнал = Humanities & Science University Journal. 2013. No. 5. Pp. 185–194.
3. Maximenko S.L., **Mamoutova O.V.**, Filippov A.S., Melekhin V.F. Design Methodology for Embedded Systems with Built-in Self-Recovery // Университетский научный журнал = Humanities & Science University Journal. 2014. No. 8. Pp. 144–153.
4. **Мамутова О.В.**, Ненашев О.В., Филиппов А.С. Автоматизация низкоуровневого оснащения системы на кристалле средствами эмуляции внесения сбоев в память // Известия высших учебных заведений. Электроника. 2015. т. 20. № 1. С. 50–57.
5. **Мамутова О.В.** Аналитические модели надежности кэш-памяти // Информационные технологии и вычислительные системы. 2015. № 4. С. 13–21.
6. **Мамутова О.В.** Оценка надежности при одиночных сбоях в кэш-памяти в маршруте проектирования системы на кристалле / О. В. Мамутова // Проблемы разработки перспективных микро- и наноэлектронных систем. 2016. № 3. С. 166–171.

Публикации в прочих изданиях:

7. **Мамутова О.В.**, Филиппов А.С. Решение задачи организации памяти в высоконадежной системе // Материалы XIII Всероссийской конф. “Фундаментальные исследования и инновации в национальных исследовательских университетах”. СПб: Изд-во Политехн. ун-та, 2009. С. 194–195.
8. **Мамутова О.В.** Вопросы организации памяти в высоконадежной системе // Материалы VI Санкт-Петербургской межрегиональной конференции «Информационная безопасность регионов России (ИБРР-2009)». СПб: СПОИСУ, 2009. С. 64.
9. **Мамутова О.В.** Вопросы организации памяти в высоконадежной системе // Сборник материалов «Будущее Российской космонавтики в инновационных разработках молодых специалистов». Королев: НОУ «ИПК Машприбор», 2009. С. 51–52.
10. **Мамутова О.В.**, Филиппов А.С. К вопросу организации иерархической памяти в высоконадежной вычислительной системе // Материалы XIV Всероссийской конф. “Фундаментальные исследования и инновации в национальных исследовательских университетах”. СПбГПУ, 2010. С. 136–137.
11. **Мамутова О.В.**, Филиппов А.С. Имитационная модель иерархической оперативной памяти в вычислительной системе // Материалы международной научно-практической конференции XXXIX Неделя науки СПбГПУ. СПб: Изд-во Политехн. ун-та, 2010. С. 20–21.
12. **Мамутова О.В.** Моделирование иерархической оперативной памяти в высоконадежной вычислительной системе // Труды конференции «Региональная информатика». СПб: СПОИСУ, 2010. С. 186–187.
13. **Мамутова О.В.** Моделирование иерархической оперативной памяти в высоконадежной вычислительной системе // Труды конф. Региональная информатика. Секция Информационные технологии в критических инфраструктурах. СПб: СПОИСУ, 2011. С. 47–51.
14. **Мамутова О.В.**, Филиппов А.С. Исследование свойств иерархической оперативной памяти вычислительной системы с помощью имитационной модели // Материалы XV Всероссийской конф. “Фундаментальные исследования и инновации в национальных исследовательских университетах.” СПб: Изд-во Политехн. ун-та, 2011. С. 75–76.

15. **Мамутова О.В.**, Филиппов А.С. Исходные данные при оценке вычислительных систем с кэш-памятью по критерию надежность-производительность // Материалы Всероссийской научно-методической конф. “Фундаментальные исследования и инновации в национальных исследовательских университетах.” СПб: Изд-во Политехн. ун-та, 2012. С. 89–92.

16. **Мамутова О.В.**, Филиппов А.С. Вопросы системного проектирования высоконадежных вычислительных систем с иерархической памятью в условиях неполных исходных данных // Сборник трудов XVI Междунар. науч.-практ. конф. Системный анализ в проектировании и управлении. СПб: Изд-во Политехн. университета, 2012. С. 107–112.

17. **Мамутова О.В.**, Филиппов А.С. Технические средства лабораторных исследований в аппаратном цикле дисциплин по направлению «Информатика и вычислительная техника» // Материалы XX Международной научно-методической конференции «Высокие интеллектуальные технологии и инновации в национальных исследовательских университетах», Т. 3 Интеллектуальные технологии формирования профессиональных компетенций, СПбГПУ, 2013, С. 54-56.

18. **Mamoutova O.V.** Processor-Driven Emulated Upset-Like Fault Injection for Memory Validation // Proceedings of the International Workshop on Verification of Embedded Systems 2013. Saint-Petersburg, Russia, 2013. Pp. 14–10.

19. Певцов И.В., **Мамутова О.В.** Адаптивное просеивание памяти в высоконадежных системах // Неделя науки СПбГПУ: материалы научно-практической конференции с международным участием. СПб: Изд-во Политехн. ун-та, 2014. С. 36–38.

20. **Мамутова О.В.**, Филиппов А.С. Инструментальные средства тестирования надежности встраиваемых систем // Материалы международной научно-методической конференции «Высокие интеллектуальные технологии и инновации в национальных исследовательских университетах». СПб: Изд-во Политехн. ун-та, 2014. С. 103–106.

21. **Mamoutova O.V.**, Nenashev O.V., Filippov A.S. In-circuit Emulation of Memory Fault Injection // Proceedings of the 2014 International Conference on Circuits, Systems and Signal Processing. Recent Advances in Electrical Engineering Series. Saint-Petersburg, 2014. Pp. 105–107.

22. **Mamoutova O.**, Fedotov A., Filippov A., Antonov A. Platform-based embedded solution for small satellite’s onboard computing. // Proc. 17th Conference of Open Innovations Association (FRUCT), IEEE, 2015. Pp. 116–121. (Scopus)

23. **Mamoutova O.V.**, Antonov A.A. On design for reliability of electronics in nanosatellite // Proceedings of 1st Symposium on Space Educational Activities. Padova, 2015.