УДК 681.3
doi:10.15217/issn1684-8853.2016.1.26

АНАЛИЗ ПРОБЛЕМЫ ПОВЫШЕНИЯ РАДИАЦИОННОЙ СТОЙКОСТИ ИНФОРМАЦИОННО-УПРАВЛЯЮЩИХ СИСТЕМ НА ЭТАПЕ ФУНКЦИОНАЛЬНО-ЛОГИЧЕСКОГО ПРОЕКТИРОВАНИЯ

И. В. Егоров[a], *аспирант*
В. Ф. Мелехин[a], *доктор техн. наук, профессор*
[a]*Санкт-Петербургский политехнический университет Петра Великого, Санкт-Петербург, РФ*

Постановка проблемы: *в условиях радиации в элементах вычислительных устройств возникают мягкие отказы, интенсивность которых значительно превышает интенсивность невосстанавливаемых отказов. Меры повышения радиационной стойкости за счет технологии изготовления интегральных схем и схемотехники библиотечных элементов недостаточны. В целях повышения радиационной стойкости актуальна организация периодического восстановления искаженной информации в резервированных структурах устройств. Это требует решения ряда задач, связанных с синтезом и анализом при функционально-логическом проектировании систем.* ***Цель:*** *аналитический обзор опубликованных результатов по рассматриваемой проблеме, выработка концептуальных положений подхода к решению проблемы повышения радиационной стойкости систем на этапе функционально-логического проектирования, постановка задач дальнейших исследований.* ***Результаты:*** *анализ показал, что мягкие информационные отказы, возникающие при радиационных воздействиях, оказывают иное влияние на работу систем по сравнению с невосстанавливаемыми отказами и, как следствие, изменяют структурную значимость элементов разных типов с точки зрения надежности. Определен подход к организации вычислительных процессов и построению резервированных структур выделенных типов блоков системы, основанный на использовании резерва времени для периодического восстановления информации, искаженной под воздействием потока мягких отказов. Сформулированы задачи дальнейших исследований, направленных на разработку методики проектирования информационно-управляющих систем с повышенной радиационной стойкостью.*

Ключевые слова *— радиационные эффекты в полупроводниковых структурах, мягкие отказы, структурное резервирование, восстановление информации в резервированных структурах, восстанавливаемые вычислительные системы.*

Введение

Из работ [1–3], посвященных анализу эффектов в полупроводниковых структурах при действии радиации, известно, что наиболее часто частица высокой энергии, попадая в МОП-транзистор, вызывает ионизацию подзатворной области полупроводника. При этом если транзистор закрыт, в подзатворной области возникает заряд неосновных носителей определенной величины, вызывающий проскакивание соответствующего импульса тока, а на выходе вентиля, в схему которого входит транзистор, появляется кратковременный импульс напряжения (ложный сигнал). Он может возникнуть в вентиле при состоянии как логического нуля, так и логической единицы. Длительность импульса зависит от величины заряда неосновных носителей, а он — от энергии частицы и технологических параметров вентиля. Обычно длительность импульса находится в диапазоне до 1–2 нс. Воздействие таких импульсов на цифровую схему зависит от задержек переключения вентиля и задержек в связях. В свою очередь эти параметры зависят от проектной нормы изготовления интегральных схем (ИС). При микронной и субмикронной технологии производства ИС эти импульсы были неопасны вследствие инерционности элементов. При современной нанотехнологии производства ИС с проектной нормой меньше 0,1 мкм такие наведенные ложные импульсы сравнимы с полезными импульсными сигналами и приводят к искажению информации в СБИС. Рассматриваемые в работе вопросы связаны с особенностями поведения ИС, выполненных по современным технологиям микроэлектроники.

Наиболее опасны рассматриваемые эффекты для транзисторов и вентилей, входящих в состав бистабильной ячейки триггера либо в запоминающий элемент блока памяти. Тогда эффект воздействия частицы приводит к искажению бита информации, которое принято называть «мягким отказом» (soft error). Если вентиль, подвергшийся воздействию, входит в состав логического элемента комбинационной схемы, то возникший ложный сигнал будет распространяться по цепи элементов и может достигнуть триггера и изменить его состояние. Это тоже приводит к сбою, но вероятность возникновения сбоя в этом случае существенно меньше, чем при непосредственном воздействии на триггер. Особенности распространения ложных сигналов по сети элементов требуют отдельного рассмотрения. Группой сотрудников Санкт-Петербургского политехнического университета, в которую входят авторы, выполнен ряд исследований по проблеме повышения

радиационной стойкости информационно-управляющих систем (ИУС).

Цель данной работы — обобщить опубликованные результаты и обосновать постановку задач дальнейших исследований, решение которых позволит создать методику проектирования (маршрут функционально-логического проектирования) ИУС со структурной, информационной и временной избыточностью, обладающих повышенной радиационной стойкостью. Публикации по новым результатам решения поставленных задач готовятся. В настоящей статье дано общее концептуальное представление о проводимых исследованиях, объединяющее последующие публикации, посвященные частным результатам.

Анализ опубликованных результатов по проблеме повышения радиационной стойкости ИУС на этапе функционально-логического проектирования

В работе [4] выполнен аналитический обзор методов повышения радиационной стойкости, описанных в литературе. Эти методы относятся к технологии изготовления ИС и построению элементов библиотеки, на базе которой производится проектирование схем устройств.

Эффективной в плане повышения радиационной стойкости при изготовлении ИС является технология SOI (кремний на изоляторе), которая создавалась в целях уменьшения паразитных емкостей и, как следствие, повышения быстродействия элементов. Оказалось, что технология SOI позволяет также уменьшить интенсивность потока мягких отказов до 10 раз. Недостатками метода являются значительное удорожание изготовления ИС и количественный характер достигаемого эффекта. Уменьшение толщины кремния (полупроводника) в подзатворном слое транзистора уменьшает величину наводимого в нем заряда неосновных носителей воздействием частицы высокой энергии, но не исключает этот эффект. При этом уменьшается длительность «ложного» импульса, но по мере уменьшения проектной нормы изготовления ИС эффект повышения радиационной стойкости будет снижаться.

На уровне построения библиотеки элементов для повышения радиационной стойкости предложены схемы триггеров с увеличенным числом транзисторов (например, DICE-cells), что, как утверждают авторы этих ячеек, тоже позволяет уменьшить интенсивность мягких отказов в несколько раз. Анализ [4] переключения такого триггера под действием наведенного «ложного» импульса показывает, что и в этом случае эффект имеет количественный характер: для переключения требуется большая длительность импульса.

Таким образом, из проведенного анализа [4] следует, что предложенные методы повышения радиационной стойкости не снимают проблемы. Наряду с ними актуально рассмотреть дополнительные методы повышения радиационной стойкости ИУС на уровне функциональной организации системы и организации вычислительных процессов.

В работе [5] введено понятие восстанавливаемых вычислительных систем при действии потока мягких отказов. В этих системах со структурной и информационной избыточностью наряду с основным вычислительным процессом исполнения прикладной программы организованы вспомогательные процессы периодического контроля и исправления информации в узлах с информационным отказом. Показано, что такая организация позволяет в условиях потока мягких отказов в несколько раз повысить время работоспособного состояния системы со структурным резервированием.

Применительно к задаче повышения надежности все блоки структуры системы делятся на два типа [5]: автоматы с памятью, реализуемой на триггерах (блоки типа 1), и блоки памяти с линейно-адресной организацией (блоки типа 2). В автоматах с памятью для блокирования распространения отказов используется троирование блока и мажорирование сигналов от экземпляров блока. Варианты структурной организации невосстанавливаемых систем со структурным резервированием исследованы в работе [6]. Обоснован способ так называемой «доменной» организации, обеспечивающий независимость блокирования распространения отказов в доменах, а также масштабируемость структурного резервирования. В работе [5] рассматривается структура блоков типа 1, построенная в соответствии со способом доменной организации. Как будет показано в следующем разделе, для проектирования восстанавливаемых систем целесообразна модификация подхода к структурному резервированию блоков типа автомата с памятью, подверженных потоку мягких отказов, по отношению к невосстанавливаемым системам.

В работе [7] предложена математическая модель для анализа надежности функциональных узлов цифровых СБИС со структурным резервированием и периодическим восстановлением работоспособного состояния. Исследуется поведение узлов типа конечного автомата с памятью, в которых используется структурное резервирование по способу, разработанному для невосстанавливаемых систем. Показано, что при периодах восстановления, меньших среднего интервала возникновения мягкого отказа, интервал работоспособного состояния блока восстанавливаемой системы увеличивается в несколько раз.

Этот результат доказывает, что организация периодического восстановления информации, искаженной под действием мягких отказов, весьма эффективна. Кроме того, результат наглядно демонстрирует сильную зависимость показателей надежности от временной избыточности блоков, т. е. от того, какую часть времени блок используется для реализации основного вычислительного процесса, а какую — для вспомогательного процесса контроля и восстановления информации. В связи с этим для анализа надежности восстанавливаемых ИУС, подверженных потоку мягких отказов, необходимо учитывать не только структуру системы, отражающую состав и связи блоков, но и организацию вычислительных процессов, в которой существенную роль играют системное и прикладное программное обеспечение (ПО).

Изменения в подходе к проблеме повышения надежности ИУС при потоке мягких отказов, вызванных действием радиации

Прежде всего, ответим на вопрос: «Почему проблему обеспечения работоспособности системы при воздействии потока мягких отказов можно выделить в самостоятельную проблему повышения надежности системы?»

Как уже отмечалось, при воздействии радиации на современные ИС мягкие отказы возникают существенно чаще (в сотни раз), чем невосстанавливаемые отказы элементов. Для вычислительного процесса мягкий отказ, проявляющийся в искажении запомненной в текущий момент информации, — это такой же отказ, как и невосстанавливаемый отказ элемента, который также проявляется в искажении информации. Поэтому для блокирования распространения мягкого отказа и обеспечения выполнения вычислительного процесса применяются те же методы повышения надежности, что и в случае невосстанавливаемых отказов элементов. Кратность резервирования при введении структурной избыточности ограничена увеличением сложности реализации системы. Из этого следует, что при действии радиации отказ резервированной системы с большой вероятностью произойдет из-за мягких отказов. Таким образом, можно поставить задачу повышения надежности системы при действии потока мягких отказов на таком интервале времени, когда невосстанавливаемые отказы элементов маловероятны. Получив эффективные способы обеспечения работоспособности системы в условиях только мягких отказов, далее можно рассматривать и более общую задачу с учетом невосстанавливаемых отказов.

Еще одним аргументом актуальности рассмотрения работы системы при потоке мягких отказов является возможность сбора статистики о мягких отказах в блоке и прогнозирование критического увеличения потока отказов для своевременного выхода действующей системы из рабочего режима с целью предотвратить аварию. Возможность восстановления состояния элемента после мягкого отказа во много раз увеличивает интервал работоспособного состояния резервированной системы. Поэтому, регистрируя каждый случай выявленного мягкого отказа в блоке, можно собирать и обрабатывать статистику отказов. При отсутствии периодических восстановлений информации в блоках такая возможность отсутствовала.

Ограничиваясь рассмотрением только потока мягких отказов, уточним понятие «отказ». Как и в классической теории надежности вычислительных систем, отказ связан с нарушением работоспособности на нижнем уровне организации вычислительного процесса, т. е. с аппаратурой. Отказ проявляется в искажении информации, представленной сигналами в аппаратуре.

В классической теории надежности справедливо считается, что отказ любого логического элемента, будь то элемент комбинационной схемы или памяти, вызывает искажение информации, представленной хранением или распространением сигналов по сети. Поэтому применительно к показателям надежности речь об информации не идет, а рассматривается исправность элементов, объединенных в сеть.

При возникновении мягких отказов под воздействием радиации ситуация иная. Если воздействие оказано на логический элемент комбинационной схемы, то на выходе может возникнуть ложный импульс, что влечет изменение соответствующего бита информации. Но этот ложный сигнал существует всего 1–2 нс, после чего опять восстановится тот же сигнал, который был до воздействия. Таким образом, можно считать, что логические элементы комбинационных схем не подвержены мягким отказам. Однако их влияние необходимо учитывать при оценке надежности памяти, так как они являются источником потока кратковременных ложных импульсов, поступающих на вход запоминающего элемента. Воздействие радиации непосредственно на элементы памяти вызывает поток мягких отказов, так как искажает хранимую информацию, т. е. изменяет состояния системы.

Итак, мягкие отказы возникают только в элементах памяти. В элементах комбинационных схем через 1–2 нс наступает самовосстановление. Это существенно влияет на подход к структурному резервированию блоков 1-го типа и требует отдельного рассмотрения. В частности, отказ от троирования мажоритаров существенно упрощает связи между блоками и снимает ограничения, связанные с доменной организацией структур.

Отличия построения блоков 2-го типа (блоков памяти) в восстанавливаемых системах обусловлены следующими дополнительными требованиями к их функциональности.

— Для обнаружения отказов и периодического восстановления информации необходимо организовать в фоновом режиме в дополнение к основному процессу выполнения прикладной программы процесс циклического чтения всех ячеек, контроля, регистрации и исправления ошибок. Взаимодействие основного и фонового процессов следует осуществлять на аппаратном уровне с использованием способа построения двухпортовой памяти.

— Период восстановления информации при мягких отказах существенно влияет на показатели надежности. Поэтому при необходимости в целях повышения надежности накопитель памяти можно разделить на несколько банков, в каждом из которых вспомогательный процесс чтения контроля и восстановления информации должен протекать параллельно.

— В блоках памяти целесообразно предусмотреть средства регистрации ошибок и формирования сообщений, передаваемых на верхний уровень организации.

Это позволит определить текущий уровень деградации системы по частоте возникновения сбоев и заблаговременно вывести систему из эксплуатации.

Интенсивность отказов блоков со структурным резервированием, подверженных потоку «мягких» отказов, пропорциональна периоду восстановления информации [7]. Это очень сильная зависимость. Поэтому временной ресурс блоков, не используемый основным процессом, необходимо употреблять для контроля и восстановления. В связи с этим для анализа надежности восстанавливаемой системы необходимо рассматривать не только структуру (состав блоков и связи), что соответствует статическому состоянию системы, но и процессы в системе, отражающие ее динамическое поведение. Чем меньше период восстановления, тем устойчивее система к воздействию «мягких» отказов. Но уменьшению периода восстановления препятствует тот факт, что блок, требующий восстановления, может быть в текущий момент времени задействован основным вычислительным процессом. Следовательно, при проектировании отказоустойчивых систем и при анализе их надежности необходимо иметь информацию о том, в какие моменты требуется доступ вычислительного процесса к аппаратным ресурсам.

Это выходит за рамки традиционных подходов к анализу надежности и классических моделей надежности, оперирующих лишь информацией о возникновении случайных событий — отказов аппаратных элементов системы.

Возникает задача интеграции сведений о протекании основного вычислительного процесса и встроенных средствах периодического восстановления в процедуру анализа надежности. Попытка моделирования программных компонентов по аналогии с аппаратными блоками в традиционных моделях надежности не позволяет добиться положительных результатов, поскольку:

— поведение программы определяется детерминированным алгоритмом, а не описывается законами распределения случайных событий, используемых в классических моделях надежности;

— в предлагаемом подходе ПО необходимо анализировать именно с точки зрения использования им аппаратных ресурсов, а не с позиции источника возникновения/распространения отказов, как это делается в большинстве моделей надежности.

Моделирование процессов периодического восстановления также связано с рядом проблем. Основная их причина в том, что события восстановления происходят периодически (обусловлены детерминированным процессом), что нарушает требование использования потока случайных событий, характерное для большинства классических моделей надежности. По этой причине применение таких моделей может привести к возникновению значительной погрешности в оценке. Данное ограничение затрудняет построение адекватной модели надежности. Но если аппаратная составляющая системы спроектирована в виде сети восстанавливаемых функциональных блоков, то оценка влияния ПО на надежность может быть сведена к определению периодичности обращения вычислительного процесса к конкретному аппаратному ресурсу. Используя знания об алгоритме программы, для каждого блока можно оценить резерв времени, который может быть использован в целях восстановления данного блока. Этот подход позволяет учесть влияние ПО еще до построения модели надежности. Для этого нужно:

— по алгоритму программы определить, к каким функциональным ресурсам происходит обращение в конкретные моменты времени;

— связать функциональный ресурс с соответствующим аппаратным блоком в структуре, определив тем самым моменты времени, когда данный блок доступен для процесса восстановления;

— для блока задать характеристики восстановления: в простейшем случае — выбрать минимально допустимый период восстановления исходя из сведений о доступности блока.

После определения периода восстановления для каждого восстанавливаемого блока в системе можно «забыть» о влиянии ПО и далее оценивать надежность чисто аппаратной системы с учетом полученных характеристик.

Подход к проектированию восстанавливаемых ИУС с учетом требований к надежности

На основании предложенного выше подхода к оценке влияния ПО на надежность восстанавливаемых систем предлагается разделить процесс проектирования отказоустойчивой системы на следующие этапы.

1. Оценка допустимых периодов восстановления в резервированных функциональных блоках.

2. Анализ надежности каждого функционального блока с учетом оцененных периодов восстановления. Для корректной оценки на этом этапе необходимо учитывать протекание детерминированных процессов восстановления в блоке, поэтому традиционные методы оценки надежности могут оказаться неприменимыми либо приводить к большим погрешностям в результатах. Для решения этой проблемы при оценке надежности блока предлагается использовать имитационные модели вместо традиционных аналитических. Имитационная модель позволяет более точно отразить специфику протекания детерминированных процессов, что на текущем этапе может привести к более точной оценке. Результатом данного этапа является оцененная вероятность отказа (вероятностная функция работоспособности) каждого восстанавливаемого блока. Так как внутренние отказы блока не распространяются в сети, на следующем этапе можно абстрагироваться от структуры блока и представлять его в виде «черного ящика» с предрассчитанной вероятностной функцией работоспособности.

3. Оценка надежности системы на основании оценок надежности блоков с учетом всех аппаратных элементов: самих функциональных блоков, а также источников питания, интерфейсных модулей, оперативной памяти, ПЗУ, процессора и т. д.

Последний этап может быть осуществлен традиционными методами анализа надежности: логико-вероятностными методами, использованием марковской модели, структурной схемой надежности и т. д. — либо с помощью имитационных моделей.

Целями проведения последнего этапа анализа являются:

— определение общих характеристик надежности системы: среднего времени наработки до отказа, вероятностной функции работоспособности;

— определение структурного вклада отдельных элементов системы в ее общую надежность.

Если по результатам анализа требования к надежности не удовлетворяются, то:

— либо осуществляется реорганизация вычислительного процесса в целях уменьшения периодов восстановления блоков;

— либо применяются методы структурного или информационного резервирования к блокам, оказывающим наибольшее влияние на надежность;

— либо реализуются более трудозатратные способы повышения надежности: резервирование на более низком уровне структурного разбиения, изменение технологии производства и т. д.

Перепроектирование осуществляется до тех пор, пока требования к надежности не будут удовлетворены.

Заключение

В результате проведенного анализа установлено, что обеспечение защиты от «мягких» отказов позволяет значительно увеличить надежность вычислительных систем, эксплуатируемых в условиях повышенной радиации. Выявлено, что эффективной является реализация механизмов защиты как на аппаратном уровне, так и на уровне организации вычислительного процесса путем выделения резерва времени, используемого для периодического восстановления искаженной информации.

Предложен подход к проектированию отказоустойчивых систем, основанный на анализе надежности отдельных функциональных блоков с учетом встроенных в них механизмов самовосстановления, по результатам которого производится оценка надежности всей системы и выбор структуры, обеспечивающей выполнение требований к производительности системы и к характеристикам надежности.

Выявлен ряд задач, требующих дополнительных исследований:

— разработка имитационной модели для оценки показателей надежности восстанавливаемых ИУС и определение условий применения аналитических и имитационной модели в процессе проектирования;

— исследование вариантов функциональной организации блоков типа автомата с памятью со структурным резервированием и периодическим восстановлением для ИУС с повышенной радиационной стойкостью;

— анализ вариантов функциональной организации блоков памяти с информационной избыточностью и периодическим восстановлением для ИУС с повышенной радиационной стойкостью;

— создание методики проектирования ИУС с повышенной радиационной стойкостью и разработка инструментальных средств для их синтеза.

Литература

1. **Edmonds L. D., Barnes C. E., Scheick L. Z.** An Introduction to Space Radiation Effects on Microelectronics. — JPL publication 00-06, 2000. — 83 p. http://snebulos.mit.edu/projects/reference/NASA-Generic/JPL-00-06.pdf (дата обращения: 05.12.2015).
2. **Gaillard R.** Single Event Effects Mechanisms and Classification // Frontiers in Electronic Testing. 2011. Vol. 41. P. 27–54.
3. **Amusan O. A.,** et al. Single Event Upsets in Deep-Submicrometer Technologies due to Charge Sharing / O. A. Amusan, L. W. Massengill, M. P. Baze, A. L. Sternberg, A. F. Witulski, B. L. Bhuva, J. D. Black // IEEE Transactions on Device and Materials Reliability. 2008. Vol. 8. N 3. P. 582–589.
4. **Максименко С. Л., Мелехин В. Ф., Филиппов А. С.** Анализ проблемы построения радиационно-стойких информационно-управляющих систем // Информационно-управляющие системы. 2012. № 2(57). С. 18–25.
5. **Максименко С. Л., Мамутова О. В., Филиппов А. С., Мелехин В. Ф.** Методология проектирования восстанавливаемых встраиваемых вычислительных систем // Университетский научный журнал. 2014. № 8. С. 144–153.
6. **Глухих М. И.** Разработка методов синтеза информационно-управляющих систем специального назначения со структурным резервированием: автореф. дис. ... канд. техн. наук. — СПб.: СПбПУ, 2006. — 173 с.
7. **Максименко С. Л., Мелехин В. Ф.** Анализ надежности функциональных узлов цифровых СБИС со структурным резервированием и периодическим восстановлением работоспособного состояния // Информационно-управляющие системы. 2013. № 2(63). С. 18–23.

UDC 681.3
doi:10.15217/issn1684-8853.2016.1.26

Analysis of Radiation Resistance Improvement Issue for Information and Control Systems at the Stage of Functional and Logical Design

Egorov I. V.[a], Post-Graduate Student, iegorov@kspt.icc.spbstu.ru
Melekhin V. F.[a], Dr. Sc., Tech., Professor, melekhin@kspt.ftk.spbstu.ru
[a]Peter the Great St.Petersburg Polytechnic University, 29, Polytechnicheskaya St., 195251, Saint-Petersburg, Russian Federation

Introduction: Under radiation, "soft failures" can occur in elements of computing devices. Their intensity is much higher than the intensity of nonrecoverable failures. To improve the radiation resistance, it is not enough to change the IC manufacturing technology or the circuitry of the standard libraries. The distorted information in the redundant structures of the devices should be repeatedly restored. To provide that, we have to solve a number of synthesis and analysis problems during the functional and logical design of the systems. **Purpose:** The paper gives an analytical overview of the published results on the problem, proposes a conceptual approach to radiation resistance improvement at the stage of functional and logical design, and poses problems for further research. **Results:** The analysis showed that soft information failures under radiation have a different impact on the system compared to nonrecoverable failures. Consequently, they change the structural importance of elements of different types in terms of reliability. An approach is proposed to the organization of computing processes and to the construction of redundant structures of allocated types of system blocks, based on using a time reserve for periodic recovery of the information distorted by the impact of a soft failure stream. The further research should be focused on developing a design technique for information and control systems with improved radiation resistance.

Keywords — Radiation Effects in Semiconductors, Soft Failures, Structural Reservation, Recovery of Information in Redundant Structures, Recoverable Computing Systems.

References

1. Edmonds L. D., Barnes C. E., Scheick L. Z. *An Introduction to Space Radiation Effects on Microelectronics*. JPL publication, 2000, no. 00-06. 83 p. Available at: http://snebulos.mit.edu/projects/reference/NASA-Generic/JPL-00-06.pdf (accessed 05 December 2015).
2. Gaillard R. Single Event Effects Mechanisms and Classification. *Frontiers in Electronic Testing*, 2011, vol. 41, pp. 27–54.
3. Amusan O. A., Massengill L. W., Baze M. P., Sternberg A. L., Witulski A. F., Bhuva B. L, Black J. D. Single Event Upsets in Deep-Submicrometer Technologies due to Charge Sharing. *IEEE Transactions on Device and Materials Reliability*, 2008, vol. 8, no. 3, pp. 582–589.
4. Maximenko S. L., Melekhin V. F., Filippov A. S. Analysis of the Problem of Radiation-Tolerant Information and Control-Systems Implementation. *Informatsionno-upravliaiushchie sistemy* [Information and Control Systems], 2012, no. 2(57), pp. 18–25 (In Russian).
5. Maximenko S. L., Filippov A. S., Melekhin V. F., Mamoutova O. V. Design Methodology for Embedded Systems with Built-in Self-Recovery. *Universitetskii nauchnyi zhurnal*, 2014, no. 8, pp. 144–153 (In Russian).
6. Glukhikh M. I. *Razrabotka metodov sinteza informatsionno-upravliaiushchikh sistem spetsial'nogo naznacheniia so strukturnym rezervirovaniem*. Dis. kand. tehn. nauk. [Development of Methods of Synthesis of Special Purpose Control Information Systems with Structural Reservation. PhD tech. sci. diss.]. Saint-Petersburg, Sankt-Peterburgskii politekhnicheskii universitet Publ., 2006. 173 p. (In Russian).
7. Maximenko S. L., Melekhin V. F. Analysis of Reliability of Functional Nodes of Digital VLSI Circuits with Structural Redundancy and Periodic Operational State Recovery. *Informatsionno-upravliaiushchie sistemy* [Information and Control Systems], 2013, no. 2(63), pp. 18–23 (In Russian).