УДК 681.3
doi:10.15217/issn1684-8853.2018.2.18

СПОСОБ ОРГАНИЗАЦИИ АВТОМАТА С ПАМЯТЬЮ С ПОВЫШЕННОЙ УСТОЙЧИВОСТЬЮ К МЯГКИМ ОТКАЗАМ И РЕГИСТРАЦИЕЙ МЯГКИХ ОТКАЗОВ

И. В. Егоров[a], *аспирант, iegorov@kspt.icc.spbstu.ru*
В. Ф. Мелехин[a], *доктор техн. наук, профессор, melekhin@kspt.ftk.spbstu.ru*
[a]*Санкт-Петербургский политехнический университет Петра Великого, Политехническая ул., 29, Санкт-Петербург, 195251, РФ*

Постановка проблемы: *снижение проектной нормы в производстве полупроводниковых структур повышает чувствительность вычислительных устройств к попаданию частиц высоких энергий (в частности, при работе в условиях радиации), что приводит к возникновению мягких отказов — искажению информации при сохранении работоспособности аппаратуры. Проведенные ранее исследования показали, что наибольшее влияние на мягкие отказы оказывают элементы памяти, а комбинационные схемы влияют меньше. Поэтому известные способы повышения надежности, основанные на использовании структурной избыточности, в условиях мягких отказов малоэффективны.* ***Цель:*** *разработка новых технических решений для автомата с памятью, работающего при потоке мягких отказов.* ***Результаты:*** *разработана структура автомата Мура с троированием памяти, мажорированием выходных сигналов памяти и восстановлением информации на каждом такте, обладающая повышенной защитой от ложных импульсов, возникающих в области комбинационных схем и памяти состояний автомата. Разработанная структура также оснащена средствами регистрации количества мягких отказов, произошедших в ходе эксплуатации. Предложена методика расчета характеристик надежности и структурной сложности для разработанной структуры.*

Ключевые слова *— автомат с памятью, комбинационная схема, анализ надежности, оценка сложности аппаратной реализации, синхронизация, мягкие отказы, структурное резервирование, восстанавливаемые системы, вероятность безотказной работы.*

Цитирование: Егоров И. В., Мелехин В. Ф. Способ организации автомата с памятью с повышенной устойчивостью к мягким отказам и регистрацией мягких отказов// Информационно-управляющие системы. 2018. № 2. С. 18–27. doi:10.15217/issn1684-8853.2018.2.18
Citation: Egorov I. V., Melekhin V. F. Organizing a Finite State Machine with Higher Resistance to Soft Failures and Soft Failure Registration. Informatsionno-upravliaiushchie sistemy [Information and Control Systems], 2018, no. 2, pp. 18–27 (In Russian). doi:10.15217/issn1684-8853.2018.2.18

Введение

Под мягким отказом будем понимать явление, при котором в элементе памяти конечного автомата происходит искажение бита данных. Возникновение мягких отказов наиболее характерно при работе устройства в условиях повышенной радиации. Элемент памяти при этом остается работоспособным, что позволяет периодически восстанавливать его состояние путем перезаписи искаженных данных корректными [1].

В опубликованных работах [2–6] анализируются процессы в логических элементах и триггерах, выполненных по технологии КМОП (CMOS Fabrication), протекающие при воздействии радиации. Благодаря известным исследованиям [3, 7–9] установлена функциональная взаимосвязь между вероятностью попадания частицы высокой энергии и возникновением мягкого отказа в цифровом устройстве, а также определены подходы к оценке надежности [2, 10–11] технических систем, учитывающие влияние мягких отказов. На основании этих исследований авторами были получены оценки вероятности возникновения мягкого отказа для различных известных реализаций автомата Мура со структурной избыточностью и восстановлением [5]. Результатом полученных оценок является сравнение различных структур конечного автомата с точки зрения надежности и сложности реализации (количества логических элементов).

В то же время актуальным остается вопрос повышения устойчивости конечного автомата к мягким отказам [12, 13], так как именно это свойство зачастую определяет надежность устройства при воздействии радиации [1].

В текущей работе предлагается схемотехническая реализация автомата Мура, обладающая лучшими (сравнительно с известными структурами [5, 14]) характеристиками надежности при воздействии потока мягких отказов [15]. Данное решение может быть использовано при проектировании отказоустойчивых восстанавливаемых вычислительных систем, работающих в условиях регулярного возникновения мягких отказов [16, 17].

Модель и структура автомата Мура

Модель автомата Мура S представляется следующей математической структурой:

$$S = <A, B, R, \delta, \lambda, r_0>,$$

где A — множество состояний входа (входной алфавит); B — множество состояний выхода (выходной алфавит); R — множество внутренних состояний; $r_0 \in R$ — начальное состояние, в которое автомат приводится сигналом начальной установки; δ: $A \times R \to R$ — функция переходов; λ: $R \to B$ — функция выходов.

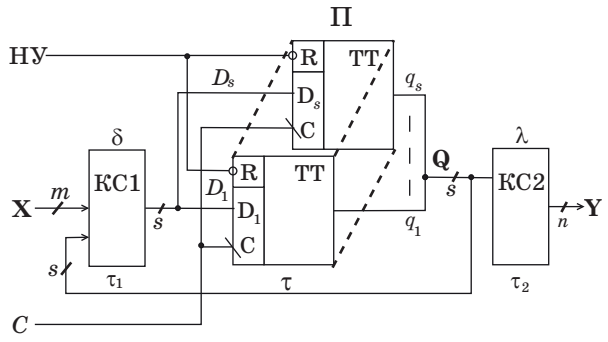
Традиционная структурная схема автомата Мура [4] представлена на рис. 1.

Комбинационная схема *КС*1 реализует функцию переходов δ; *КС*2 реализует функцию выходов λ; для реализации блока памяти *П* автомата использованы триггеры *ТТ* типа *D*, синхронизируемые спадом тактового импульса синхронизации *С*; *НУ* — сигнал начальной установки; связи между блоками соответствуют функциям в автомате Мура: δ: $\{\mathbf{X}\} \times \{\mathbf{Q}\} \to \{\mathbf{Q}\}$; λ: $\{\mathbf{Q}\} \to \{\mathbf{Y}\}$; τ_1, τ_2, τ обозначают задержки в электронных схемах, реализующих блоки *КС*1, *КС*2 и *П* соответственно.

Для данной структуры была получена [5] формула, позволяющая оценить вероятность отказа $P_{\text{о.а1}}$ и вероятность безотказной работы $\overline{P}_{\text{о.а1}}$ автомата в течение всего времени выполнения задачи $T_з$ при известной частоте $q_{\text{п.ч.т}}$ попадания заряженных частиц в один из транзисторов конечного автомата: $\overline{P}_{\text{о.а1}} = e^{-(q_{\text{м.о.п}} + q_{\text{м.о.КС1}})T_з}$, где:

— частота $q_{\text{м.о.п}}$ возникновения мягкого отказа автомата по причине попадания заряженной частицы в область П напрямую зависит от числа транзисторов $N_{\text{т.п}}$, входящих в состав блока памяти ($q_{\text{м.о.п}} = N_{\text{т.п}}\, q_{\text{п.ч.т}}$);

— частота $q_{\text{м.о.КС1}}$ возникновения мягкого отказа автомата по причине попадания заряженной частицы в область КС1 рассчитывается по известной методике с учетом внутренней структуры КС1 (удаленности элементов от входов П).



■ ***Рис. 1.*** Структурная схема автомата Мура

■ ***Fig. 1.*** The block diagram of the Moore automaton

Также при расчете $q_{\text{м.о.КС1}}$ учитывается тот факт, что ложный импульс, распространяющийся с выходов КС1, повлечет за собой изменение состояния П (мягкий отказ) только в том случае, если он совпадет по времени с моментом записи данных (спадом синхроимпульса *С*) в один из триггеров П. Этот интервал времени занимает незначительную долю периода синхронизации автомата. Таким образом, с точки зрения надежности КС1 имеет меньшую структурную значимость, нежели П, где ложное изменение состояния любого из триггеров непосредственно приводит к мягкому отказу. Однако КС1 может содержать большее по сравнению с П число логических элементов, что увеличивает вероятность попадания заряженных частиц в ее область и приводит к необходимости разработки механизма борьбы с ложными импульсами на выходах КС1.

Попадание частицы в область КС2 влияния на работу автомата не оказывает, так как эта комбинационная схема не подключена к элементам памяти, следовательно, ложный импульс, угасающий через несколько наносекунд после попадания частицы, не может привести к мягкому отказу.

Структура автомата Мура с троированием, мажорированием и самовосстановлением

Применительно к рассматриваемой задаче построения автомата с повышенной устойчивостью к мягким отказам определим расширение функций автомата дополнительно к основной функции реализации заданного алгоритма:

1) блокирование прохождения мягкого отказа на выход автомата;

2) восстановление состояния отказавшего экземпляра автомата без прерывания выполнения основной функции;

3) выявление, регистрация и подсчет числа мягких отказов в автомате.

Определим подходы к реализации этих функций.

Для блокирования прохождения искаженной информации на выход автомата будем использовать известный способ структурного резервирования — троирование и мажорирование, предложенный для систем с невосстанавливаемыми отказами. С учетом результатов проведенных исследований [5] троирование и мажорирование целесообразно использовать только для блока памяти автомата П.

Мажорирование сигналов на выходах трех экземпляров блока памяти автомата обеспечит восстановление искаженной в случае мягкого отказа информации при очередном переходе автомата.

Для обнаружения мягких отказов в автомате предусмотрим в мажоритаре выходных сигналов

памяти П формирование сигнала «ошибка» *E* (error).

Для регистрации и подсчета числа мягких отказов введем в структуру автомата блок регистрации ошибок (БРО).

Схема автомата Мура с троированием, мажорированием и самовосстановлением, предложенная авторами [15], приведена на рис. 2. Рассмотрим состав схемы и ее отличительные особенности в сравнении с традиционной схемой (см. рис. 1) автомата Мура без структурного резервирования.

Входные сигналы, аналогичные рис. 1:

— **X** — *m*-разрядный вектор входных информационных сигналов;

— *C* — тактовый импульс синхронизации;

— *R* — сигнал сброса (начальной установки).

Дополнительные входные сигналы:

— *ENA* (enable) — сигнал разрешения работы автомата: при *ENA* = 1 работа разрешена; при *ENA* = 0 автомат остановлен, при переходе сигнала *ENA* 0 → 1 автомат продолжит работу с того состояния, в котором был остановлен. Этот сигнал расширяет возможности использования автомата в системе;

— $R_{БРО}$ — сигнал сброса блока регистрации ошибок *БРО*. В восстанавливаемых системах периодически проводится мониторинг состояния блоков (проверка количества отказов, зарегистрированных БРО), в конце каждого цикла мониторинга производится сброс состояния БРО на начальное.

Выходные сигналы автомата:

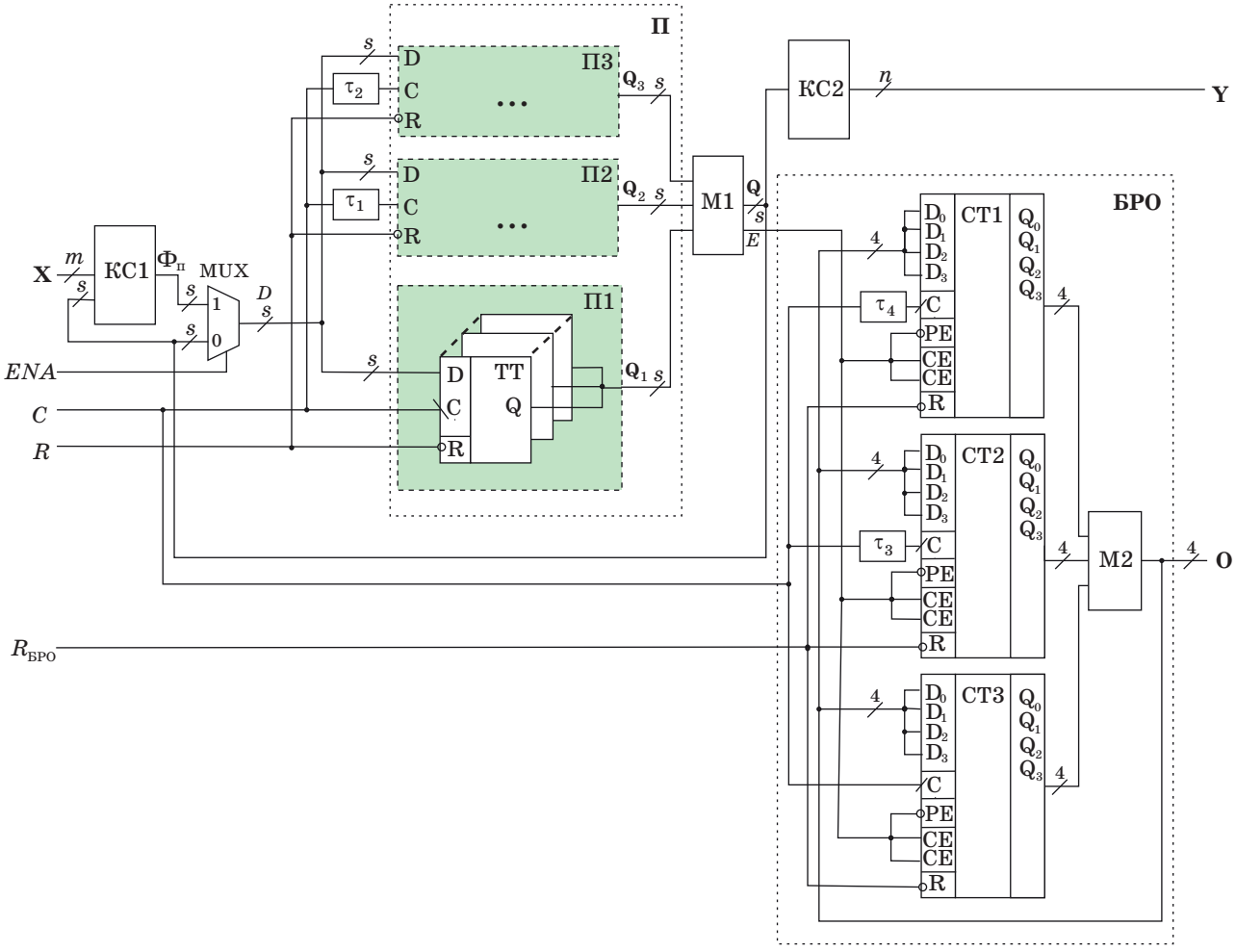
— **Y** — *n*-разрядный вектор информационных выходных сигналов (аналогично сигналам на рис. 1);

— **O** — код числа мягких отказов в автомате за период мониторинга.

Состав и назначение блоков структуры:

— *КС*1 — комбинационная схема, реализующая функцию переходов δ (аналогичная на рис. 1);

— *КС*2 — комбинационная схема, реализующая функцию выходов λ (аналогичная на рис. 1);



■ ***Рис. 2.*** Схема автомата Мура с троированием, мажорированием и самовосстановлением

■ ***Fig. 2.*** The block diagram of the Moore automaton with triple redundancy, majority voting and self-recovery

— *П* — блок памяти автомата, содержащий три экземпляра *П*1, *П*2, *П*3 (каждый аналогичен блоку памяти П на рис. 1);

— *М*1 — блок мажорирования троек соответствующих выходных сигналов блоков *П*1, *П*2, *П*3, дополнительно выявляющий возникновение отказа и формирующий в этом случае выходной сигнал *E*;

— *MUX* — мультиплексор, переключающий на информационные входы блоков памяти *D* сигнал $\Phi_{\text{п}}$ перехода с выходов комбинационной схемы *КС*1 либо сигнал **Q** с выходов блока *М*1;

— *БРО* — блок регистрации ошибок (мягких отказов в автомате);

— *СТ*1, *СТ*2, *СТ*3 — три экземпляра синхронных счетчиков для подсчета числа мягких отказов;

— *М*2 — блок мажорирования сигналов с выходов счетчиков и формирования сигнала **O** — числа мягких отказов за период мониторинга;

— τ_1, τ_2, τ_3, τ_4 — элементы задержки.

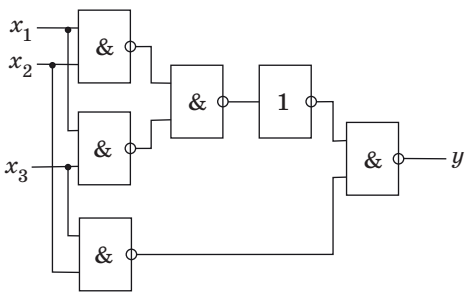
Поясним функции новых (по сравнению с рис. 1) блоков.

Блок мажорирования М1 содержит *s* (*s* — число триггеров в памяти автомата) мажоритарных элементов. Возможная схема, реализующая мажоритарный элемент, представлена на рис. 3.

Помимо этого блок М1 содержит схему, реализующую функцию выявления мягкого отказа:

$$E = (Q_1^1 + Q_1^2 + Q_1^3)(\bar{Q}_1^1 + \bar{Q}_1^2 + \bar{Q}_1^3) + \ldots + \\ + (Q_s^1 + Q_s^2 + Q_s^3)(\bar{Q}_s^1 + \bar{Q}_s^2 + \bar{Q}_s^3).$$

Сигнал *E* поступает на вход БРО. В БРО для подсчета числа мягких отказов (ошибок) используется синхронный счетчик, например, соответствующий стандартному счетчику К1533ИЕ10. Счетчик имеет информационные входы записи ($D_0D_1D_2D_3$), вход *PE* разрешения записи (при *PE* = 0), входы *CE* разрешения прибавления единицы (при *CE* = 1), вход синхронизации *C* и вход сброса *R*. Поскольку в самом счетчике под воздействием радиации могут возникать мягкие отказы, то в БРО применяется троирование счетчика и мажорирование. Блок мажорирования М2 содержит четыре мажоритарных элемента соответственно числу разрядов в счетчике. Выходы блока мажорирования подключены к внешнему выходу **O** автомата и к информационным входам ($D_0D_1D_2D_3$) всех трех счетчиков. Управляющие входы *PE* и *CE* всех трех счетчиков соединены и подключены к выходу *E* блока мажорирования М1. Таким образом, при *E* = 1 в счетчиках по спаду *C* прибавляется 1, при *E* = 0 по спаду *C* записывается код с выхода М2, и каждый такт в счетчиках БРО происходит самовосстановление информации.



■ ***Рис. 3.*** Структурная схема мажоритарного элемента
■ ***Fig. 3.*** The block diagram of the majority voter

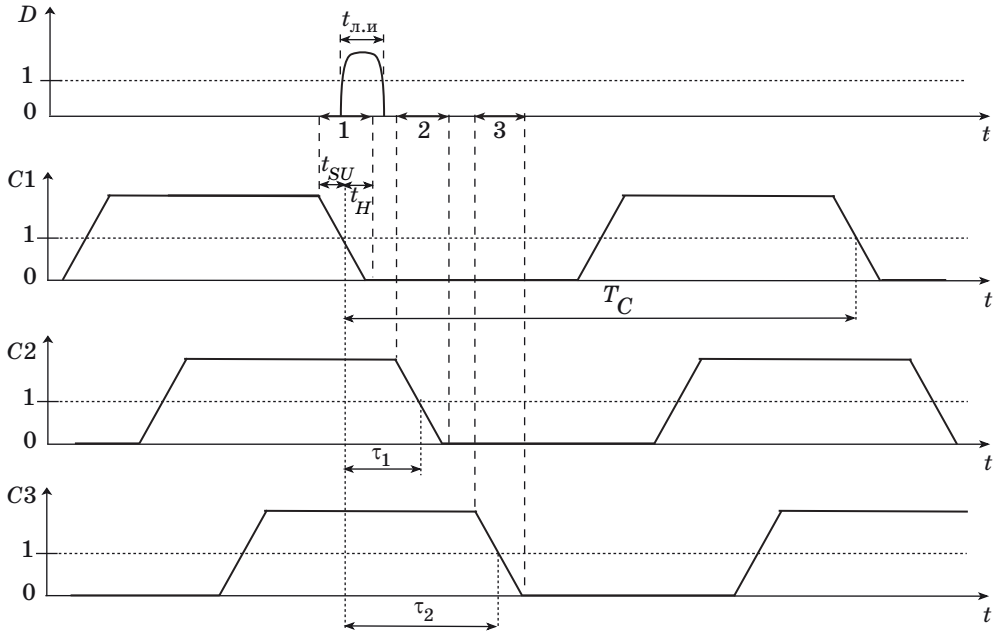
При работе автомата в режиме реализации алгоритма каждый такт выполняется переход в новое состояние (в некоторых случаях переход выполняется в старое состояние путем его подтверждения). В случае возникновения отказа в одном из экземпляров памяти он не проявляется на выходе **Q** мажоритара, и на информационные входы элементов П каждый такт поступает верная информация. Таким образом, каждый такт осуществляется самовосстановление данных в П.

В некоторых случаях в системах организуется работа автомата в стартстопном режиме. Для этого используется сигнал *ENA*, вырабатываемый управляющим блоком системы. Режим временной приостановки работы автомата может быть достаточно длительным. За это время в памяти автомата также могут возникать мягкие отказы. С целью организовать самовосстановление памяти автомата в этом режиме выходные сигналы **Q** с выхода блока М1 поступают не только на входы комбинационной схемы КС1, но и на вход мультиплексора *MUX*. При этом если *ENA* = 0, каждый такт происходит самовосстановление памяти П.

Для уменьшения влияния ложных сигналов на выходах КС1, подключенных к информационным входам триггеров памяти автомата, предложен следующий способ. Как было отмечено [5], ложный импульс, поступающий на информационный вход триггера, может изменить его состояние, если этот импульс попадает в интервал $\tau = t_{SU} + t_H$ (t_{SU} — время предустановки триггера, t_H — время удержания триггера), на практике составляющий около 10 % от периода T_C тактовых сигналов. В троированной схеме памяти автомата П (см. рис. 2) в цепь передачи синхроимпульсов *C* введены элементы задержки: $\tau_1 = \tau$ для экземпляра памяти П2 и $\tau_2 = 2\tau$ для экземпляра П3. Благодаря этому переключение всех триггеров в П2 происходит по сравнению с П1 с задержкой τ, а в П3 — с задержкой 2τ.

Принцип использования задержек τ_1 и τ_2 проиллюстрирован на рис. 4, где:

— *D* — сигнал на информационных входах *D* триггеров блока памяти П (см. рис. 2);



■ ***Рис. 4.*** Принцип уменьшения влияния ложных сигналов на выходах КС1
■ ***Fig. 4.*** The principle of the minimization of spurious pulses on CS1 outputs

— *C*1, *C*2, *C*3 — входы синхронизации *C* экземпляров блока памяти П1, П2, П3 соответственно (см. рис. 2);

— T_C — период синхронизации триггеров.

На входы *D* поступает кратковременный ложный импульс длительностью $t_{л.и}$. Для каждого экземпляра блока памяти (П1, П2, П3) существует временной интервал (*1*, *2* и *3* соответственно) длительностью $t_{SU} + t_H$, в течение которого сигнал на входе *D* влияет на состояние триггеров данного экземпляра. Эти интервалы между собой не пересекаются из-за внесенных задержек τ_1, τ_2. Таким образом, ложный импульс, попадающий только в интервал *1* (как изображено на рис. 4), вызывает мягкий отказ в П1, но не оказывает влияние на П2 и П3. А поскольку выходы троированного блока памяти П подключены к мажоритару М1, мягкий отказ в одном из экземпляров блока памяти не вызывает искажение выходного вектора **Q**. Таким образом, распространение мягкого отказа заблокировано.

Искажение состояния троированной памяти может произойти только в том случае, если в течение одного такта ложный сигнал на входах *D* захватит минимум два интервала длительностью $t_{SU} + t_H$, отмеченных выше. Назовем это сложное событие возникновением неисправленного отказа в памяти из-за ложных сигналов на входе *D*. Оценим вероятность $P_{н.о\ D}$ этого события и эффективность предложенного способа как

$$P_{н.о\ D} = \left(P_{л.с\ D} \frac{\tau}{T_C} \right)^2,$$

где $P_{л.с\ D} \frac{\tau}{T_C}$ — вероятность появления ложного сигнала на информационном входе *D* в течение одного такта и попадания его в интервал τ при спаде импульса *C*.

Ясно, что $\left(P_{л.с\ D} \frac{\tau}{T_C} \right)^2 \ll 1$. Поэтому воздействие ложных импульсов на входе *D* на работу автомата практически исключается. Из этого следует, что данный способ намного эффективнее известных, изложенных в работах [18–20] и рассмотренных в статье [5].

Аналогичный способ введения задержек ($\tau_3 = \tau$, $\tau_4 = 2\tau$) в цепь передачи синхроимпульсов предлагается использовать и в блоке БРО.

Анализ надежности и сложности реализации автомата Мура с троированием, мажорированием и самовосстановлением

По аналогии с исследованием, проведенным в работе [5], оценим вероятность сохранения автоматом работоспособности в течение времени $T_з$ решения задачи и сложность реализации структуры автомата (выраженную в числе логических элементов). Считается, что все отказы в элементах автомата являются мягкими (восстанавливаемыми), возникающими по причине попадания заряженных частиц в транзисторы автомата с некоторой известной интенсивностью $q_{п.ч.т}$. Работоспособность автомата считается утрачен-

ной, если на выход автомата Y (см. рис. 2) поступают искаженные данные.

Оценку проведем для частного примера конечного автомата [5], где известны:

— сложность реализации исходного блока памяти П: $C_{\text{П}} = 30$;

— сложность реализации комбинационной схемы КС1: $C_{\text{КС1}} = 54$;

— сложность реализации комбинационной схемы КС2: $C_{\text{КС2}} = 88$;

— сложность реализации одноразрядного мажоритара: $C_{\text{М}} = 6$;

— сложность реализации одноразрядного мультиплексора 2 в 1: $C_{MUX} = 4$;

— количество бит в блоке памяти П: $s = 3$;

— интенсивность появления ложных импульсов на выходах КС1: $3{,}4q_{\text{п.ч.т}}$;

— интенсивность появления ложных импульсов на выходах одноразрядного мультиплексора 2 в 1: $1{,}25q_{\text{п.ч.т}}$;

— отношение суммарного времени предустановки и удержания триггера к длительности периода синхронизации, выраженное коэффициентом $K = 0{,}15$.

При оценке не будем рассматривать БРО (см. рис. 2), так как он реализует дополнительную функцию, не связанную с решением основной задачи автоматом. С учетом этого исследуемая структура состоит из комбинационных схем КС1, КС2, троированной памяти состояния автомата (сложности $C_{\text{П}}$), мажорирующего элемента разрядности $s = 3$ (сложности $C_{\text{М}}$) и мультиплексора (сложности C_{MUX}) на две шины разрядности s. Общая сложность структуры

$$C_{\text{а}} = C_{\text{КС1}} + C_{\text{КС2}} + 3C_{\text{П}} + s \times C_{\text{М}} + s \times C_{MUX} = \\ = 54 + 4 + 3 \times 30 + 3 \times 6 + 3 \times 4 = 178.$$

Для оценки надежности структуры проанализируем, в результате чего может исказиться выходной сигнал автомата. Основной причиной являются мягкие отказы в элементах памяти, которые приведут к потере работоспособности, если за один такт работы автомата в одинаковых битах двух различных экземпляров памяти П произойдет мягкий отказ. В противном случае побитный мажоритар М1 по цепи обратной связи передаст корректные данные на входы П1, П2, П3, и на следующем такте состояние памяти будет автоматически восстановлено. Для получения оценки вероятности отказа в памяти ограничимся рассмотрением ситуаций, когда за такт работы автомата возникает от нуля до трех отказов (остальными случаями пренебрежем, так как вероятность их возникновения на несколько порядков меньше). Тогда, обозначив событие мягкого отказа бита памяти за $A_{\text{П}i,j}$, а событие отсутствия мягкого отказа за $\overline{A_{\text{П}i,j}}$ (где i — номер экземпляра памяти, j — порядковый номер бита памяти в экземпляре), рассмотрим возможные комбинации событий, которые приведут к отказу блока памяти.

В условиях текущей задачи каждый блок памяти содержит три информационных бита ($s = 3$). В случае отсутствия искаженных бит памяти либо при наличии только одного искаженного бита отказа рассматриваемой структуры не происходит. При наличии двух искаженных бит к отказу приведут следующие комбинации: $A_{\text{П}1,1}A_{\text{П}2,1}$, $A_{\text{П}1,1}A_{\text{П}3,1}$, $A_{\text{П}2,1}A_{\text{П}3,1}$, $A_{\text{П}1,2}A_{\text{П}2,2}$, $A_{\text{П}1,2}A_{\text{П}3,2}$, $A_{\text{П}2,2}A_{\text{П}3,2}$, $A_{\text{П}1,3}A_{\text{П}2,3}$, $A_{\text{П}2,3}A_{\text{П}3,3}$, $A_{\text{П}1,3}A_{\text{П}3,3}$. Итого девять комбинаций для случая двух искаженных бит. При наличии трех искаженных бит к отказу приводят 57 возможных комбинаций событий.

Общую вероятность возникновения отказа в памяти автомата оценим как сумму вероятностей возникновения рассмотренных несовместных комбинаций событий одновременного отказа двух или трех бит в блоке памяти:

$$P_{\text{м.о.а}} = 9(P_{\text{м.о.бита}})^2(1 - P_{\text{м.о.бита}})^7 + \\ + 57(P_{\text{м.о.бита}})^3(1 - P_{\text{м.о.бита}})^6. \qquad (1)$$

Определим зависимость вероятности искажения бита данных в памяти $P_{\text{м.о.бита}}$ в (1) от интенсивности $q_{\text{п.ч.т}}$ попадания заряженной частицы в транзистор автомата. Причин, вследствие которых может возникнуть искажение, две. Первая — попадание заряженной частицы непосредственно в область памяти. Так как один бит памяти реализуется триггером, состоящим из пяти транзисторов, интенсивность возникновения этого события равна $5q_{\text{п.ч.т}}$. Вторая причина — запись искаженной информации вследствие попадания заряженной частицы в элементы КС1 или MUX, подключенные к соответствующему биту памяти. Исходя из расчетов, произведенных в работе [5], интенсивность появления ложных импульсов на выходах КС1 равна $3{,}4q_{\text{п.ч.т}}$, а на выходах мультиплексора — $1{,}25q_{\text{п.ч.т}}$. Для оценки интенсивности появления ложных импульсов, оказывающих влияние на П, эти величины необходимо умножить на коэффициент $K = 0{,}15$, так как элементы КС1 и MUX влияют на работу памяти только в момент спада синхроимпульса. Суммарная интенсивность искажений одного бита данных соответственно равна $5q_{\text{п.ч.т}} + 0{,}15(3{,}4q_{\text{п.ч.т}} + 1{,}25q_{\text{п.ч.т}}) = 5{,}7q_{\text{п.ч.т}}$. Исходя из этого вероятность искажения бита памяти $P_{\text{м.о.бита}}$ в течение одного такта синхронизации T_C автомата выражается через интенсивность попадания заряженной частицы в транзистор $q_{\text{п.ч.т}}$ следующим образом:

$$P_{\text{м.о.бита}} = 1 - e^{-5{,}7q_{\text{п.ч.т}}T_C}. \qquad (2)$$

Подставив выражение (2) в (1), оценим вероятность отказа всей структуры в течение одного такта работы автомата:

$$P_{\text{о.а}} = 9e^{-39,9q_{\text{п.ч.т}}T_C}(1 - e^{-5,7q_{\text{п.ч.т}}T_C})^2 + \\ + 57e^{-34,2q_{\text{п.ч.т}}T_C}(1 - e^{-5,7q_{\text{п.ч.т}}T_C})^3 = \\ = -48e^{-51,3q_{\text{п.ч.т}}T_C} + 153e^{-45,6q_{\text{п.ч.т}}T_C} - \\ - 162e^{-39,9q_{\text{п.ч.т}}T_C} + 57e^{-34,2q_{\text{п.ч.т}}T_C}.$$

Поскольку в начале каждого такта происходит восстановление состояния системы, вероятность безотказной работы автомата $\overline{P_{\text{о.а}}}(n)$ в течение n последовательных тактов вычисляется как произведение вероятностей безотказной работы в течение каждого такта:

$$\overline{P_{\text{о.а}}}(n) = (1 - P_{\text{о.а}})^n = (1 + 48e^{-51,3q_{\text{п.ч.т}}T_C} - \\ - 153e^{-45,6q_{\text{п.ч.т}}T_C} + 162e^{-39,9q_{\text{п.ч.т}}T_C} - \\ - 57e^{-34,2q_{\text{п.ч.т}}T_C})^n.$$

Оценка полученных результатов

В работе [5] была произведена оценка вероятности безотказной работы различных отказоустойчивых структур автомата Мура при следующих условиях:

— интенсивность попадания заряженных частиц в один транзистор: $q_{\text{п.ч.т}} = 0{,}0005$;

— общее время, необходимое для полного решения задачи: $T_{\text{з}} = 100$;

— время одного рабочего цикла автомата: $T_{\text{ц}} = 10$;

— время одного такта работы автомата: $T_C = 1$.

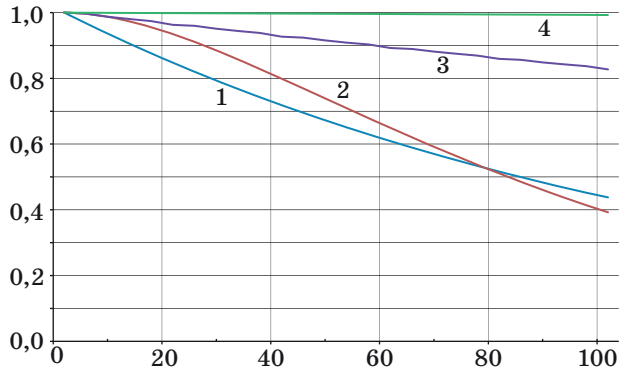
Для структуры, предложенной в данной работе (структура *4*), построим график функции вероятности безотказной работы (3) на интервале $T_{\text{з}}$ ($n = 100$ тактов) и сравним ее с результатами, полученными для известных структур (рис. 5):

— структура *1* — автомат без структурного резервирования (см. рис. 1);

— структура *2* — автомат с троированными блоками и троированными входными мажоритарами без периодического восстановления информации;

— структура *3* — автомат с троированными блоками и троированными входными мажоритарами и периодическим восстановлением информации. Восстановление искаженного состояния происходит за счет формирования сигнала начальной установки в конце каждого цикла работы автомата (период восстановления соответствует длительности цикла алгоритма работы автомата).

Ось абсцисс обозначает текущее время t решения задачи. По оси ординат расположена вероятность нахождения автомата в работоспособном состоянии (1 — гарантированно работоспособен, 0 — гарантированно неработоспособен).



■ ***Рис. 5***. Функции работоспособности анализируемых структур

■ ***Fig. 5***. The reliability function of the analyzed structures

■ Сложность реализации анализируемых структур

■ The structural complexity of the analyzed structures

Структура	Сложность реализации (количество логических элементов)
1	88
2	336
3	336
4	178

Итоговая вероятность успешного решения задачи для предложенной структуры *4* равна 0,99. Аналогичная величина, рассчитанная для структуры *3* (показавшей в статье [5] лучшие характеристики надежности), равна 0,84, что наглядно демонстрирует преимущество предложенной структуры при работе в условиях мягких отказов. Это превосходство обеспечивается меньшим по сравнению со структурой *3* периодом восстановления — оно происходит на каждом такте, а не только по окончании цикла работы алгоритма.

При этом предложенная структура также имеет по сравнению со структурой *3* меньшую сложность реализации (таблица).

Оценивая сложность реализации, помимо количества логических элементов также полезно учитывать и количество линий связи между структурными блоками. В структурах *2* и *3* это количество троекратно увеличено по сравнению с исходной структурой *1* (по причине полного троирования автомата). В структуре *4* троирован только блок памяти, поэтому избыточные линии связи отсутствуют.

Заключение

На основе анализа проведенных ранее исследований определены направления разработки схемотехнических решений для конечного автомата с памятью, работающего в условиях потока мягких отказов.

Разработана структура автомата Мура с троированием памяти, мажорированием выходных сигналов памяти и восстановлением информации в каждом такте (см. рис. 2), которая обладает повышенной защитой от ложных импульсов, возникающих по причине попадания частиц высокой энергии в области комбинационных схем и памяти состояний автомата, а также оснащена средствами регистрации количества мягких отказов, произошедших в ходе эксплуатации.

Для разработанной структуры на примере показана методика расчета, позволяющая при известной радиационной обстановке (интенсивности попадания частиц высокой энергии в транзисторы) оценить вероятность работоспособности автомата в заданном интервале времени.

Получены оценки надежности и структурной сложности для примера разработанной структуры. Сравнение полученных оценок с аналогичными, рассчитанными для известных отказоустойчивых реализаций автомата Мура, показало превосходство предложенной структуры как с точки зрения надежности при воздействии потока мягких отказов, так и структурной сложности.

Предложенная структура позволяет также реализовать дополнительные функции детектирования отказов, возникающих в автомате. Следовательно, становится возможным непосредственно в ходе работы автомата оценивать степень его деградации и при выходе за границы безопасной эксплуатации осуществлять аварийную остановку устройства.

Литература

1. **Егоров И. В., Мелехин В. Ф.** Анализ проблемы повышения радиационной стойкости информационно-управляющих систем на этапе функционально-логического проектирования // Информационно-управляющие системы. 2016. № 1. С. 26–31. doi:10.15217/issn1684-8853.2016.1.26
2. **Егоров И. В., Мелехин В. Ф.** Методы и средства анализа надежности структурных блоков с резервированием и периодическим восстановлением информации на различных этапах проектирования вычислительных систем // Информационно-управляющие системы. 2016. № 2. С. 26–34. doi:10.15217/issn1684-8853.2016.2.26
3. **Егоров И. В., Мелехин В. Ф.** Анализ процессов в конечном автомате при воздействии радиации. Оценка вероятности искажения информации // Информационно-управляющие системы. 2016. № 3. С. 24–33. doi:10.15217/issn1684-8853.2016.3.24
4. **Kaeslin H.** Digital Integrated Circuit Design. From VLSI Architectures to CMOS Fabrication. — Cambridge University Press, 2008. http://www.roletech.net/books/DigitalIntegratedCircuit.pdf (дата обращения: 10.04.2016).
5. **Егоров И. В., Мелехин В. Ф.** Анализ показателей надежности и сложности реализации различных вариантов структур автомата с памятью при потоке мягких отказов // Информационно-управляющие системы. 2017. № 3. С. 34–46. doi:10.15217/issn1684-8853.2017.3.34
6. **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).
7. **James R. Schwank, Marty R. Shaneyfelt, Paul E. Dodd.** Radiation Hardness Assurance Testing of Microelectronic Devices and Integrated Circuits: Radiation Environments, Physical Mechanisms, and Foundations for Hardness Assurance // IEEE Transactions on Nuclear Science. 2013. Vol. 60. N 3. P. 2074–2100.
8. **Hass K. J., Ambles J. W.** Single Event Transients in Deep Submicron CMOS // 42nd Midwest Symp. on Circuits and Systems. 2000. Vol. 1. P. 122–125.
9. **Benedetto J. M.,** et al. Variation of Digital SET Pulse Widths and the Implications for Single Event Hardening of Advanced CMOS Processes // IEEE Transactions on Nuclear Science. 2005. Vol. 52. P. 2114–2119.
10. **Jacob A. Abraham, Daniel P. Siewiorek.** An Algorithm for the Accurate Reliability Evaluation of Triple Modular Redundancy Networks // IEEE Transactions on Computers. 1974. Vol. C-23. N 7. P. 682–692.
11. **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. С. 18–23.
12. **Gaillard R.** Single Event Effects Mechanisms and Classification // Frontiers in Electronic Testing. 2011. Vol. 41. P. 27–54.
13. **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. N 3. P. 582–589.
14. **Мурога С.** Системное проектирование сверхбольших интегральных схем. Кн. 1. — М.: Мир, 1985. — 288 с.

15. Пат. 174640 RU, МПК G06F 11/07 (2006.01). Отказоустойчивый цифровой преобразователь информации для управления дискретными процессами / И. В. Егоров (RU), В. Ф. Мелехин (RU). — № 174640/25–08; заявл. 14.06.2017; опубл. 24.10.2017, Бюл. № 30. — 7 с.
16. **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.
17. **Максименко С. Л., Мелехин В. Ф., Филиппов А. С.** Анализ проблемы построения радиационно-стойких информационно-управляющих систем // Информационно-управляющие системы. 2012. № 2. С. 18–25.
18. **Eaton P., Benedetto J., Mavis D., Avery K., Sibley M., Gadlage M., Turflinger T.** Single Event Transient Pulsewidth Measurements Using a Variable Temporal Latch Technique // IEEE Transactions on Nuclear Science. Dec. 2004. Vol. 51. N 6. P. 3365–3368.
19. **Rollins N., Wirthlin M., Caffrey M., Graham P.** Evaluating TMR Techniques in the Presence of Single Event Upsets // Proc. of the 6th Annual Intern. Conf. on Military and Aerospace Programmable Logic Devices (MAPLD), Washington, D.C. Sept. 2003. http://scholarsarchive.byu.edu/cgi/viewcontent.cgi?article = 2047&context = facpub (дата обращения: 05.08.2016).
20. **She Xiaoxuan, Samudrala P. K.** Selective Triple Modular Redundancy for Single Event Upset (SEU) Mitigation // Adaptive Hardware and Systems: NASA/ESA Conf. 2009. P. 344–350.

UDC 681.3
doi:10.15217/issn1684-8853.2018.2.18

Organizing a Finite State Machine with Higher Resistance to Soft Failures and Soft Failure Registration

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, Politekhnicheskaia St., 195251, Saint-Petersburg, Russian Federation

Introduction: Up-to-date design rules used in computer engineering make hardware unreliable when working under radiation. A hit of a charged particle causes a «soft failure», i.e. a situation when the hardware is still usable but the information transmitted through it or stored in it is corrupted. Some research revealed that soft failures occur more often in memory units than in combinational circuits. This is why the known engineering solutions like structural redundancy are not efficient enough in the case of soft failures. **Purpose:** Developing new circuitry solutions for a finite state machine experiencing a flow of soft failures. **Results:** The developed structure of a Moore automaton with triple redundancy of its internal memory, double redundancy of its output signals and self-recovery on each synchronization clock period has a higher resistance to soft errors which can occur in its combinational circuits or internal memory. The structure also contains tools to count the soft failures during its functioning. A technique is proposed to estimate the reliability and structural complexity of the developed structure.

Keywords — Finite State Machine, Combinational Circuit, Reliability Analysis, Hardware Complexity Estimation, Synchronization, Soft Failures, Structural Redundancy, Recoverable System, Probability of Non-Failure.

Citation: Egorov I. V., Melekhin V. F. Organizing a Finite State Machine with Higher Resistance to Soft Failures and Soft Failure Registration. *Informatsionno-upravliaiushchie sistemy* [Information and Control Systems], 2018, no. 2, pp. 18–27 (In Russian). doi:10.15217/issn1684-8853.2018.2.18

References

1. Egorov I. V., Melekhin V. F. Analysis of Radiation Resistance Improvement Issue for Information and Control Systems at the Stage of Functional and Logical Design. *Informatsionno-upravliaiushchie sistemy* [Information and Control Systems], 2016, no. 1, pp. 26–31 (In Russian). doi:10.15217/issn1684-8853.2016.1.26
2. Egorov I. V., Melekhin V. F. Methods and Tools for Structural Block Reliability Analysis with Reservation and Periodic Information Recovery at Various Stages of Computing System Design. *Informatsionno-upravliaiushchie sistemy* [Information and Control Systems], 2016, no. 2, pp. 26–34 (In Russian). doi:10.15217/issn1684-8853.2016.2.26
3. Egorov I. V., Melekhin V. F. Analysis of Processes in a Finite State Machine under Radiation. Probabilistic Assessment of Information Distortion. *Informatsionno-upravliaiushchie sistemy* [Information and Control Systems], 2016, no. 3, pp. 23–33 (In Russian). doi:10.15217/issn1684-8853.2016.3.23
4. Kaeslin H. *Digital Integrated Circuit Design. From VLSI Architectures to CMOS Fabrication*. Cambridge University Press, 2008. Available at: http://www.roletech.net/books/DigitalIntegratedCircuit.pdf (accessed 10 April 2016).
5. Egorov I. V., Melekhin V. F. Analysis of Reliability Characteristics for Various Structures of a Finite State Machine Working in Case of Soft-Failure Flow. *Informatsionno-upravliaiushchie sistemy* [Information and Control Systems], 2017, no. 3, pp. 34–46 (In Russian). doi:10.15217/issn1684-8853.2017.3.34
6. 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).
7. James R. Schwank, Marty R. Shaneyfelt, Paul E. Dodd. Radiation Hardness Assurance Testing of Microelectronic Devices and Integrated Circuits: Radiation Environments, Physical Mechanisms, and Foundations for Hardness Assurance. *IEEE Transactions on Nuclear Science*, 2013, vol. 60, no. 3, pp. 2074–2100.
8. Hass K. J., Ambles J. W. Single Event Transients in Deep Submicron CMOS. *42nd Midwest Symp. on Circuits and Systems*, 2000, vol. 1, pp. 122–125.

9. Benedetto J. M., et al. Variation of Digital SET Pulse Widths and the Implications for Single Event Hardening of Advanced CMOS Processes. *IEEE Transactions on Nuclear Science*, 2005, vol. 52, pp. 2114–2119.
10. Jacob A. Abraham, Daniel P. Siewiorek. An Algorithm for the Accurate Reliability Evaluation of Triple Modular Redundancy Networks. *IEEE Transactions on Computers*, 1974, vol. C-23, no. 7, pp. 682–692.
11. 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, pp. 18–23 (In Russian).
12. Gaillard R. Single Event Effects Mechanisms and Classification. *Frontiers in Electronic Testing*, 2011, vol. 41, pp. 27–54.
13. 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.
14. Muroga S. *Sistemnoe proektirovanie sverkhbol'shikh integral'nykh skhem. Kn. 1* [System Design of Very-Large-Scale Integrated Circuits. Book 1]. Moscow, Mir Publ., 1985. 288 p. (In Russian).
15. Egorov I. V., Melekhin V. F., et al. *Otkazoustojchivyj cifrovoj preobrazovatel' informacii dlja upravlenija diskretnymi processami* [The Failure-Safe Information Digitizer for Management of Discrete Processes]. Patent RU, no. 174640, 2017.
16. 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).
17. 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, pp. 18–25 (In Russian).
18. Eaton P., Benedetto J., Mavis D., Avery K., Sibley M., Gadlage M., Turflinger T. Single Event Transient Pulsewidth Measurements Using a Variable Temporal Latch Technique. *IEEE Transactions on Nuclear Science*, Dec. 2004, vol. 8, no. 6, pp. 3365–3368.
19. Rollins N., Wirthlin M., Caffrey M., Graham P. Evaluating TMR Techniques in the Presence of Single Event Upset. *Proc. of the 6th Annual Intern. Conf. on Military and Aerospace Programmable Logic Devices (MAPLD)*, Washington, D.C., Sept. 2003. Available at: http://scholarsarchive.byu.edu/cgi/viewcontent.cgi?article = 2047&context = facpub (accessed 05 August 2016).
20. She Xiaoxuan, Samudrala P. K. Selective Triple Modular Redundancy for Single Event Upset (SEU) Mitigation. *NASA/ESA Conf. "Adaptive Hardware and Systems"*, 2009, pp. 344–350.