

УДК 681.326.7

Методика функционального диагностирования оперативных запоминающих устройств средств обработки информации робототехнических комплексов военного назначения

Козлов Р. Н., Финько О. А.

Актуальность задачи: для достижения высоких показателей надежности оперативных запоминающих устройств, функционирующих в агрессивных условиях и средах, особую актуальность приобретают задачи их технического, в частности функционального, диагностирования. К подобным запоминающим устройствам относятся микросхемы памяти, являющиеся компонентами средств обработки и защиты информации, размещаемых на борту робототехнических комплексов военного назначения (РТК ВН) и эксплуатируемых в условиях воздействий противника или экстремальных средах. Для решения задачи обеспечения требуемых показателей надежности применяются классические методы, заключающиеся во внесении структурно-логической избыточности (дублирование, мажоритарное троирование, методы помехоустойчивого кодирования). При этом существующие методы повышения надежности могут быть не всегда приемлемыми с позиции вносимой аппаратурной избыточности, либо не учитывают всю совокупность деструктивных воздействий. Предлагаемые способы функционального диагностирования оперативных запоминающих устройств (ОЗУ) ориентированы на комбинированный характер воздействий, адаптивны для применения в большинстве используемых средств обработки информации (СОИ) РТК ВН устройств памяти. Возможности применения предлагаемых способов для каждого конкретного типа памяти ограничиваются принятой стратегией записи информации в них и принятой моделью ошибок. **Целью работы** является повышение вероятности правильного декодирования данных, считываемых из ОЗУ, размещаемых на борту РТК ВН, функционирующих в условиях сложного характера деструктивных воздействий. **Новизна** разработанной методики заключается в учете более полной совокупности характеристик деструктивных воздействий и характеризуется увеличением достоверности хранимой в ОЗУ информации. **Результат.** Численные результаты оценки показали, что ввиду двойственного характера ошибок в хранимой информации, применение традиционных способов функционального диагностирования не в полной мере удовлетворяет современным требованиям к надежности ОЗУ СОИ РТК ВН. Результаты сравнительной оценки используемых и предложенных способов контроля ОЗУ показывают преимущество предложенных при заданной модели ошибок. **Практическая значимость** заключается в выборе наилучшего способа контроля устройства памяти с учетом требований к массогабаритным показателям и энергетическим затратам СОИ РТК ВН. Разработанные в рамках методики алгоритмы позволяют не только парировать ошибки, но и выполнять реконфигурацию ОЗУ в случае возникновения отказов в компонентах памяти.

Ключевые слова: функциональное диагностирование, коды коррекции ошибок, оперативные запоминающие устройства, надежность оперативных запоминающих устройств, робототехнические комплексы военного назначения.

Библиографическая ссылка на статью:

Козлов Р. Н., Финько О. А. Методика функционального диагностирования оперативных запоминающих устройств средств обработки информации робототехнических комплексов военного назначения // Системы управления, связи и безопасности. 2018. № 4. С. 249-267. URL: <http://sccs.intelgr.com/archive/2018-04/13-Kozlov.pdf>

Reference for citation:

Kozlov R. N., Finko O. A. Functional diagnostics method of storage devices for military robotic systems. Systems of Control, Communication and Security, 2018, no. 4, pp. 249-267. Available at: <http://sccs.intelgr.com/archive/2018-04/13-Kozlov.pdf> (in Russian).

Актуальность

Современные робототехнические комплексы военного назначения (РТК ВН), в частности с беспилотными летательными аппаратами (БЛА), используются в качестве одного из важнейших средств повышения эффективности применения Вооруженных сил Российской Федерации [1, 2]. Их использование актуально в условиях, когда применение пилотируемых летательных аппаратов неприемлемо или нецелесообразно по каким-либо причинам: повышенный радиационный фон, бактериологическое заражение местности, при продолжительном ведении разведки.

Отсутствие пилота на борту позволило реализовать высокие показатели летно-технических характеристик: продолжительность полета – более суток; высота полета – 20 км; дальность полета – 20000 км [3]. Такие показатели обуславливают перспективность разработки многофункциональных, стратегических РТК ВН с БЛА большой высоты и времени активного существования. Для достижения таких показателей к компонентам перспективных воздушных РТК ВН предъявляются повышенные требования к массогабаритным показателям и энергетическим затратам, а новые условия функционирования, их специфика, связанная с воздействиями противника, перспектива применения новых ядерных энергетически установок, накладывают дополнительные требования к методам обеспечения их надежности.

По мере возникновения новых задач, связанных с увеличением продолжительности активного существования, вопрос проектирования перспективных РТК ВН с БЛА определяет ужесточение требований к надежности их систем. К ним относятся:

- 1) топливная система;
- 2) система электроснабжения;
- 3) система обеспечения посадки;
- 4) пилотажно-навигационная система;
- 5) система приема и обработки сигналов полезной нагрузки;
- 6) система обработки и сбора информации;
- 7) бортовые средства защиты информации;
- 8) блоки полезной нагрузки.

Особенно актуальной является задача обеспечения требуемых показателей надежности компонентов микроэлектроники из-за их повышенной чувствительности к различным деструктивным воздействиям [4-9]. К таким компонентам относятся, прежде всего, запоминающие устройства, являющиеся важным элементом любой системы обработки информации и средств ее защиты, используемых для хранения ключей шифрования, данных о целостности метрик системы, незашифрованных, конфиденциальных данных, а также информации, связанной с непосредственно выполняемыми задачами (хранение фото, видео материалов и т.п.), передаваемой по каналам связи в реальном масштабе времени.

Для обеспечения требуемых показателей надежности оперативные запоминающие устройства (ОЗУ) используют различные методы диагностирования [10]. Выбор метода диагностирования зависит от многих факторов, в частности

от требований и ограничений, накладываемых на тактико-технические характеристики бортовых средств обработки информации (СОИ) РТК ВН, компонентами которых они являются. В свою очередь, технические характеристики СОИ обусловлены спецификой решаемых задач РТК ВН. Для РТК ВН, выполняющих задачи в реальном масштабе времени, эффективность которых в значительной степени зависит от достоверности обрабатываемой информации, а время, затрачиваемое на обработку данных, может быть критичным, наиболее адекватным решением является применение методов *функционального диагностирования*. Методы функционального диагностирования дискретных устройств, действующих в реальном масштабе времени, основаны, в том числе, на применении кодов, контролирующих ошибки.

Традиционно используемые в дискретных устройствах коды, контролирующие ошибки, адаптивны для различных запоминающих устройств и могут быть применимы как для перспективных твердотельных накопителей, так и жестких дисков [11].

Постановка задачи

Эффективность применения корректирующих кодов для обнаружения и исправления ошибок в ОЗУ СОИ РТК ВН зависит от того, насколько корректирующие способности кода согласованы с моделью ошибок в контролируемом устройстве. В алгебраической теории кодирования задачу согласования характера проявления ошибок в дискретных устройствах со свойствами корректирующего кода описывают в терминах метрики подмножеств разрешенных и запрещенных кодовых комбинаций. Определение характеристик кода сводится к поиску подмножества, обладающего подходящей метрикой. Большинство способов помехоустойчивого кодирования, применяемых для контроля ОЗУ, направлены на определенную модель ошибок. Данный факт обуславливает достоверность контролируемой информации при одной модели ошибок и невозможность эффективного контроля при другой. Кроме того, для контроля ОЗУ, выбор корректирующего кода осуществляется не только на основе модели ошибок, но и в соответствии с требуемыми показателями качества (массогабаритные показатели и энергетические затраты).

Таким образом, для ОЗУ, функционирующих в составе бортовых СОИ, в том числе средств защиты информации РТК ВН с БЛА, выполняющих задачи в условиях сложного характера деструктивных воздействий, проявляющихся в виде ошибок различной кратности (множественные ошибки, «вспышки» ошибок и т. п.), необходимо разработать методику функционального диагностирования, определяющую выбор наиболее приемлемого способа кодового контроля, при котором будут соблюдаться необходимые требования к массогабаритным показателям и энергетическим затратам РТК ВН.

Модель ошибок

Модель ошибок разработана с учетом условий функционирования РТК ВН и описывает взаимосвязь элементов модели, раскрывающей влияние различных факторов на достоверность хранимой информации в ОЗУ. Условия

функционирования определяются деструктивными воздействиями и их совокупностью, реализующими угрозы достоверности информации.

Повышение требований к тактико-техническим характеристикам современных СОИ РТК ВН требует применения ОЗУ большой информационной емкости, низкого уровня энергопотребления и малых массогабаритных показателей с одной стороны, а с другой – обладающих стойкостью к деструктивным воздействиям ионизирующих излучений и воздействию перспективного вооружения, основанного на новых физических принципах (СВЧ, электромагнитное, лазерное и др. оружие). Увеличение информационной емкости предопределяет переход на субмикронные технологические нормы и удовлетворяет требованию к уменьшению массогабаритных показателей и энергетических затрат, но и обуславливает снижение стойкости к указанным деструктивным воздействиям.

Проведенные исследования элементов микроэлектроники с топологическими нормами проектирования от 0,5 мкм до 0,18 мкм, работающих под воздействием атмосферных нейтронов, выявили, что основными эффектами воздействия являются одиночные сбои и тиристорные эффекты [12]. С учетом того, что поток атмосферных нейтронов в 3,5 раза больше на высоте 1,5 км и в 300 раз больше на высоте 10-12 км, чем на уровне моря, с ростом высоты активного существования РТК ВН рост числа сбоев увеличивается [13].

На рис. 1 представлена зависимость характеристик ошибок в данных, хранимых в ОЗУ, от требований, предъявляемых к перспективным РТК ВН с БЛА.

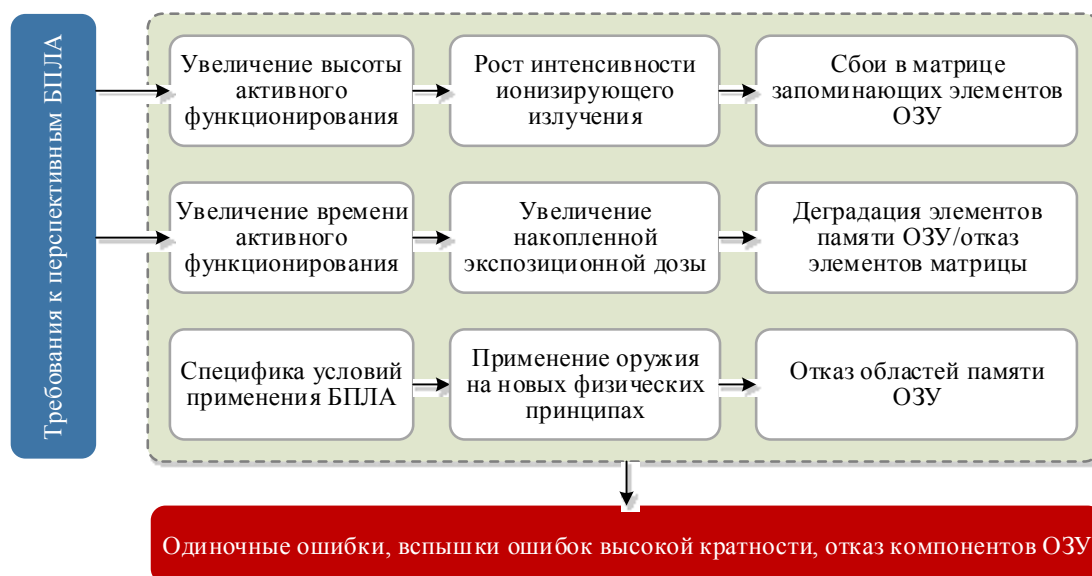


Рис. 1. Характеристика ошибок в зависимости от условий функционирования ОЗУ СОИ РТК ВН

Имеем, что на комплекс оказываются преднамеренные и непреднамеренные деструктивные воздействия, а также ряд факторов, обуславливающих их влияние на надежность ОЗУ (см. рис. 2). Воздействия могут быть как комплексными, так и отдельными.

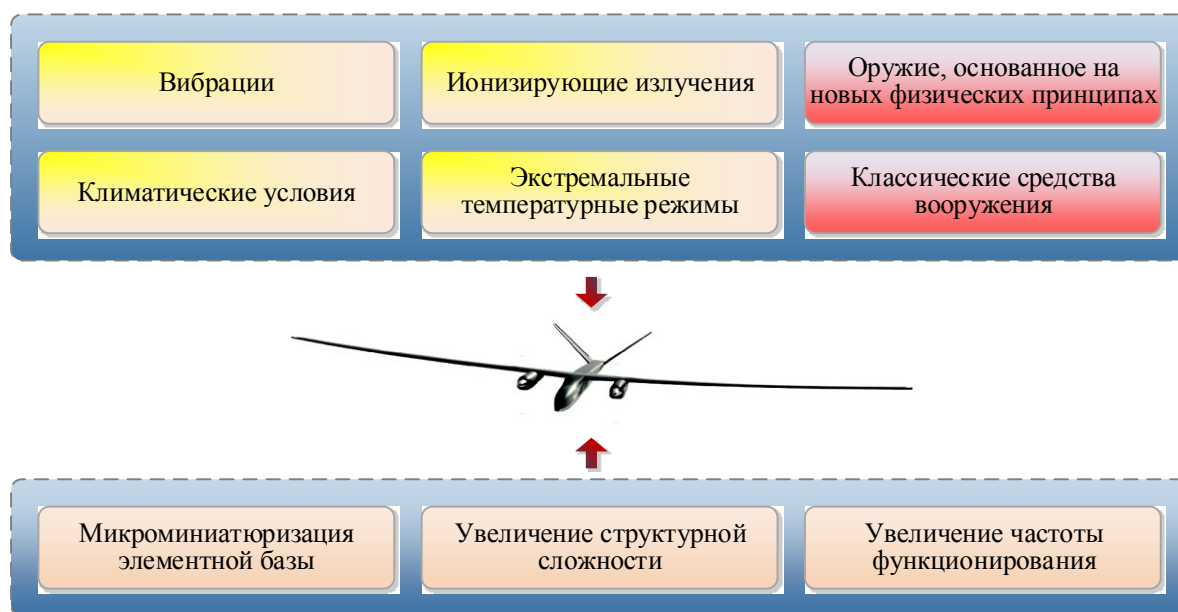


Рис. 2. Деструктивные воздействия и факторы, обуславливающие их влияние на ОЗУ СОИ РТК ВН

Примем допущения о том, что в силу различного характера причинно-следственных связей возникновения ошибок в данных, хранящихся в ОЗУ СОИ РТК ВН, следует классифицировать два типа ошибок:

1) *ошибки первого типа* – ошибки, вызванные воздействием на матрицу запоминающих элементов; будем считать, что они носят традиционный характер и проявляются на битовом уровне в виде одиночных ошибок и ошибок малой кратности согласно биномиальному закону распределения вероятностей (рис. 3, синий контур);

2) *ошибки второго типа* – ошибки, вызванные деструктивными воздействиями на компоненты схемы обрамления; ошибки этого типа имеют характер близкий к равновероятному и проявляются в виде пакетирующихся «вспышек» ошибок на битовом уровне (рис. 3, красный контур).

Учитывая специфику выполняемых задач и условия функционирования РТК ВН [14], определим требования к выбору способа кодового контроля ОЗУ СОИ РТК ВН:

1) необходимо учесть различные модели ошибок, определяемые как преднамеренными и непреднамеренными воздействиями, так и их совокупностями;

2) необходимо обеспечить гибкость задействования аппаратных и энергетических затрат ОЗУ в условиях изменяющихся требований к надежности и другим характеристикам ОЗУ в различных условиях обстановки.

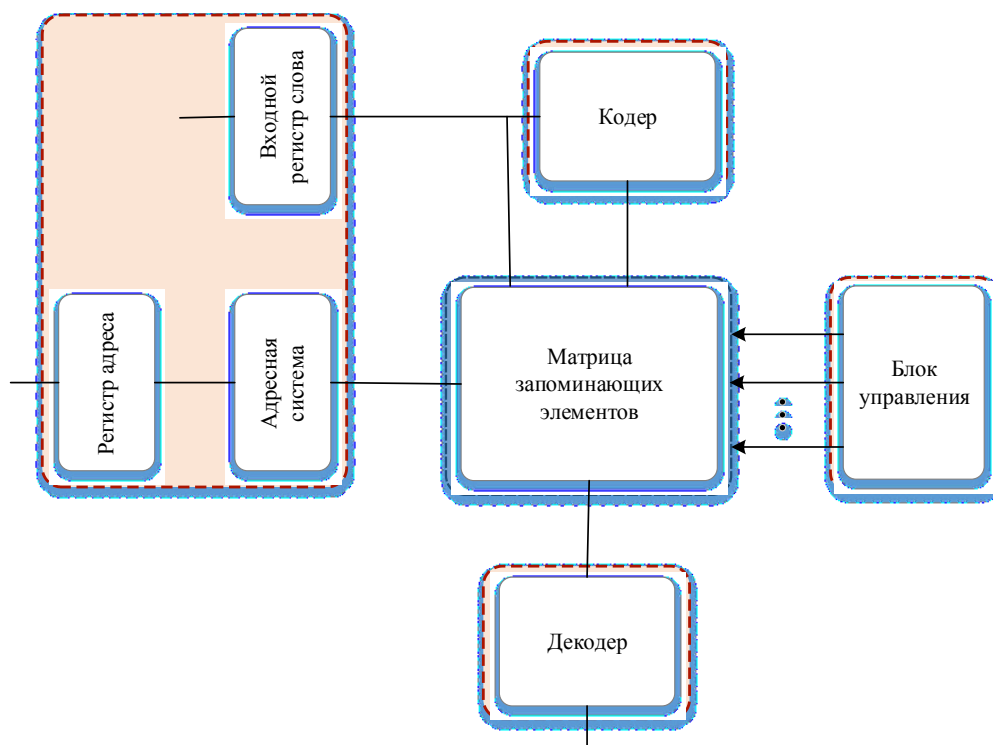


Рис. 3. Типовая структура локальной области памяти ОЗУ

Контроль ОЗУ СОИ РТК ВН на основе R-кодов полиномиальной модулярной арифметики

Под полиномиальным R-кодом будем понимать модулярный код, полученный по расширенной системе оснований (модулей) – полиномов $p_1(z), p_2, \dots$, где под основаниями системы понимаются задающие классы эквивалентности полиномы такие, что

$$\gcd(p_i(z), p_j(z)) = 1; \quad i, j = 1, 2, \dots, n; \quad i \neq j.$$

Устройство памяти представляет собой массив локальных областей памяти, где $B_i(z)$ ($i=1, 2, \dots, n$) – полиномы информационных сообщений, трактуемые как вычеты модулярного полиномиального кода по системе оснований R-кода $p_1(z), p_2, \dots$, где $\deg p_1(z) = \deg p_2(z) = \dots = \deg p_n(z)$. ОЗУ функционирует в условиях сложных деструктивных воздействий в составе СОИ РТК с БЛА.

Для заданной модели ошибок определим способ кодового контроля, при котором реализуется обнаружение и исправление множественных ошибок в одной или нескольких локальных областях памяти. Математический аппарат модулярной арифметики позволяет выполнять реконфигурацию ОЗУ в случае отказа соответствующих областей памяти. Кроме того, в условиях комплексирования деструктивных воздействий применение такой кодовых конструкций, основанных на модулярных кодах, позволяет, как корректировать ошибки, так и преодолевать отказы компонентов ОЗУ.

Рассмотрим алгоритм расширения R-кода. Для этого, внесем в имеющуюся систему оснований r избыточных оснований, таким образом, чтобы выполнялось:

$$\deg p_n(z) > \deg p_{n+1}(z) > \dots > \deg p_{n+r}(z);$$

построим систему полиномиальных ортогональных базисов $\beta_1(z), \beta_2(z), \dots$, а также определим рабочий диапазон системы как $\deg P(z) = \sum_{i=1}^n \deg p_i(z)$, где $P(z) = \prod_{i=1}^n p_i(z)$.

Алгоритм 1.1: Алгоритм кодирования R-кодом

Data: $B_1(z), B_2(z), \dots, p_{n+1}(z), \dots, z$; $\beta_1(z), \beta_2(z), \dots$

Result: $B_{n+1}(z), \dots, z$

while $j=1, \dots$ **do**

$$B_{n+j}(z) = \left| \sum_{i=1}^n B_i(z) \beta_i(z) \right|_{P(z)} \Big|_{p_{n+j}(z)} = \left| \begin{bmatrix} B_1(z) \\ B_2(z) \\ \vdots \\ B_n(z) \end{bmatrix} \times \begin{bmatrix} \beta_1(z) \\ \beta_2(z) \\ \vdots \\ \beta_n(z) \end{bmatrix} \right|_{P(z)} \Big|_{p_{n+j}(z)}$$

end

Print: $B_{n+1}(z), \dots, z$

Теперь рассмотрим алгоритм кодирования полученных вычетов R-кода двоичным циклическим кодом; $g(z)$ – порождающий полином циклического кода; u – число избыточных символов циклического кода.

Алгоритм 1.2: Алгоритм кодирования циклическим кодом

Data: $\mathbf{B}_i(z) = \langle b_{i,0} + b_{i,1}z^1 + \dots + b_{i,k-1}z^{k-1} \rangle$, $g(z)$

Result: $\mathbf{H}_i(z)$

for $i=1, 2, \dots, n+r$ **do**

$\mathbf{H}_i(z) = g(z) \times \mathbf{B}_i(z)$;

end

Print: $\mathbf{H}_i(z) = \langle h_{i,0} + h_{i,1}z^1 + \dots + h_{i,k-1}z^{k-1} + h_{i,k+u-1}z^{k+u-1} \rangle$

Полученные кодовые слова записываются в локальные области памяти. Символ «*» означает вероятностный характер обнаружения ошибки.

Алгоритм 1.3: Алгоритм декодирования циклического кода

Data: $\mathbf{H}_i^*(z) = \langle h_{i,0}^* + h_{i,1}^*z^1 + \dots + h_{i,k-1}^*z^{k-1} + h_{i,k+u-1}^*z^{k+u-1} \rangle$; $i=1, 2, \dots, n+r$

Result: $S_{B_i(z)}(z)$

for $1 \leq i \leq n+r$ **do**

$B_i^*(z) = \frac{H_i^*(z)}{g(z)}$;

end

Print: $S_{B_1(z)}(z), \dots, S_{B_{n+r}(z)}(z)$

Получим некоторое количество ненулевых синдромов ошибки. Если количество ненулевых синдромов меньше или равно количеству r , то выполним восстановление кодового слова с заданной вероятностью посредством реконфигурации [15] структуры ОЗУ. Рассмотрим алгоритм декодирования R-кода (символ «**» означает вероятностный характер исправления ошибки).

Алгоритм 1.4: Алгоритм декодирования R-кода (реконфигурация ОЗУ, частный случай исправления однократной ошибки)

Data: $B_i^*(z)$; $S_{B_i(z)}(z)$; $\beta_1(z), \beta_2(z), \dots, \beta_n(z), \dots$; z

Result: $B_i^{**}(z)$

while $1 \leq i \leq (n+r)$ **do**

$$B_i^{**}(z) = \left| \sum_{\substack{i=1,2,\dots,n+r \\ i \neq c_1, c_2, \dots, c_j}} B_i^{*(c_1, c_2, \dots, c_j)}(z) \beta_i(z) \right|_{P^{(c_1, c_2, \dots, c_j)}(z)} \Big|_{p_i(z)}, \text{ where}$$

$$P^{(c_1, c_2, \dots, c_j)}(z) = \prod_{\substack{i=1,2,\dots,n+r \\ i \neq c_1, c_2, \dots, c_j}} p_i(z)$$

if $i = 1, 2, \dots, n+r$, $i \neq c_1, c_2, \dots, c_j$ **then**

$$B^{*(c_1, c_2, \dots, c_j)}(z) = \frac{q_i^{(c_1, c_2, \dots, c_j)}(z) P_i^{(c_1, c_2, \dots, c_j)}(z)}{m_i(z)}$$

else $i = c_1, c_2, \dots, c_j$ **then**

$$B^{*(c_1, c_2, \dots, c_j)}(z) = 0$$

end

end

Print: $A_i^{**}(z) = a_{i,0}^* + a_{i,1}^* z^1 + \dots + a_{i,k-2}^* z^{k-2} + a_{i,k-1}^* z^{k-1}$

Таким образом, предложенный алгоритм кодового контроля удовлетворяет предложенной модели ошибок, сочетает в себе гибкость к аппаратным затратам в условиях отказов локальных областей памяти, обеспечивает контроль пакетирующихся ошибок в кодовых словах локальных областей памяти.

Каскадный контроль ОЗУ СОИ РТК ВН,

основанный на манипуляциях с систематическими циклическими кодами

Алгоритм предполагает наличие двух ступеней кодирования. Код первой ступени определяется как обнаруживающий ошибки, второй – исправляющий.

Аналогично имеем массив локальных областей памяти. В связи со спецификой выполняемых задач на используемые компоненты воздушных РТК ВН накладываются ограничения к их массогабаритным показателям и энергетически характеристикам. В данных условиях к кодовой конструкции предъявим

требования к минимизации структурно-логической избыточности при требуемых показателях к корректирующим способностям.

В ОЗУ записывается $i=1,2,\dots$ кодовых слов $B_i(z)$, каждое из которых подвергается процедуре кодирования систематическим циклическим кодом. При этом, $g(z)$ – порождающий полином кода, $z^{\deg g(z)}$ – одночлен степени равной степени $g(z)$.

Алгоритм 2.1: Первая ступень кодирования

Data: $A_i(z)$, $z^{\deg g(z)}$, $g(z)$

Result: $B_i(z)$

for $1 \leq i \leq n$ **do**

$$\frac{A_i(z)z^{\deg g(z)}}{g(z)}$$

if operation is ready **then**

do $A_i(z) + \frac{A_i(z)}{g(z)}$

end

end

Print: $B_i(z) = \langle b_{i,0} + b_{i,1}z^1 + \dots \quad z^{k-2} + b_{i,k-1}z^{k-1} + b_{i,k+u-1}z^{k+u-1} \rangle$

Ввиду высокой обнаруживающей способности ряда линейных кодов [16-18] будем их использовать на первой ступени в качестве «индикатора» ошибок для выполнения коррекции ошибок кодом второй ступени.

Получим набор кодовых слов систематического циклического кода:

$$\left\{ \begin{aligned} B_1(z) &= \left(a_{1,0} + a_{1,1}z^1 + a_{1,2}z^2 + \dots \quad \dots \quad z^{k-2} + a_{1,k-1}z^{k-1} \right) z^{\deg g(z)} + \\ &\quad + \frac{\left(a_{1,0} + a_{1,1}z^1 + a_{1,2}z^2 + \dots \quad \dots \quad z^{k-2} + a_{1,k-1}z^{k-1} \right) z^{\deg g(z)}}{g(z)}, \\ B_2(z) &= \left(a_{2,0} + a_{2,1}z^1 + a_{2,2}z^2 + \dots \quad \dots \quad z^{k-2} + a_{2,k-1}z^{k-1} \right) z^{\deg g(z)} + \\ &\quad + \frac{\left(a_{2,0} + a_{2,1}z^1 + a_{2,2}z^2 + \dots \quad \dots \quad z^{k-2} + a_{2,k-1}z^{k-1} \right) z^{\deg g(z)}}{g(z)}, \\ &\dots \dots \dots \\ B_n(z) &= \left(a_{n,0} + a_{n,1}z^1 + a_{n,2}z^2 + \dots \quad \dots \quad z^{k-2} + a_{n,k-1}z^{k-1} \right) z^{\deg g(z)} + \\ &\quad + \frac{\left(a_{n,0} + a_{n,1}z^1 + a_{n,2}z^2 + \dots \quad \dots \quad z^{k-2} + a_{n,k-1}z^{k-1} \right) z^{\deg g(z)}}{g(z)}, \end{aligned} \right.$$

Определим алгоритм кодирования второй ступени.

Алгоритм 2.2: Вторая ступень кодирования

Data: $B_1(z), B_2(z), \dots$

Result: $B_{n+1}(z)$

for $i = 1, 2, \dots, n$ **do**

$$B_{n+1}(z) = \sum_{i=1}^n \left(b_{i,0} + b_{i,1}z^1 + \dots + b_{i,k-1}z^{k-1} \right) z^{\deg g(z)} + \sum_{i=1}^n \frac{\left(b_{i,0} + b_{i,1}z^1 + b_{i,2}z^2 + \dots + b_{i,k-1}z^{k-1} \right) z^{\deg g(z)}}{g(z)}$$

end

Print:

$$B_{n+1}(z) = \left\langle b_{n+1,0} + b_{n+1,1}z^1 + \dots + b_{n+1,k-2}z^{k-2} + b_{n+1,k-1}z^{k-1} + b_{n+1,k+u-1}z^{k+u-1} \right\rangle$$

Пусть в результате деструктивного воздействия в одной из локальных областей памяти произошла ошибка с вектором $E_i(z)$. Процедура обнаружения заключается в делении кодового слова $B_i^*(z)$ на порождающий полином $g(z)$. Остаток от деления является синдромом $S_{B_i(z)}(z)$ ошибки $E_i(z)$. Здесь и далее «*» – означает вероятностный характер обнаружения ошибки.

Алгоритм 2.3: Декодирование кода первой ступени

Data: $B_1(z), B_2(z), \dots, B_{n+1}(z); g(z)$

Result: $S_{B_i(z)}(z)$

for $i = 1, 2, \dots$ **do**

$$S_{B_i(z)}(z) = \frac{B_i(z)}{g(z)}$$

if $S_{B_i(z)}(z) \neq 0$ **then**

$A_i(z)$ – error

end

end

Print: $S_{B_i(z)}(z)$

После локализации места ошибки построим алгоритм ее коррекции, «**» – означает вероятностный характер исправления ошибки.

Алгоритм 2.4: Коррекция ошибок кодом второй ступени

Data: $B_1(z), B_2(z), \dots, B_{n+1}(z); g(z)$

Result: $B_i^{**}(z)$

for $i = 1, 2, \dots, n$ **do**

$$B_i^{**}(z) = \sum_{i=1; i \neq j}^{n+1} B_i(z),$$

j -е кодовое слово с $S_{B_i(z)}(z) \neq 0$.

end

Print: $B_i^{**}(z) = \langle b_{i,0}^{**} + b_{i,1}^{**}z^1 + \dots + b_{i,k-1}^{**}z^{k-1} + b_{i,k+u-1}^{**}z^{k+u-1} \rangle$

Информационные кодовые слова $A_i^{**}(z)$ образуются из многочленов $B_i^*(z)$, $B_i^{**}(z)$ путем исключения одночленов степени меньшей $z^{\deg(z)}$ и делением получившегося полинома $A_i^*(z)z^{\deg g(z)}$ на $z^{\deg(z)}$.

Таким образом, разработанный способ каскадного кодирования информации в ОЗУ СОИ РТК ВН, при минимальной структурно-логической избыточности и заданной модели ошибок, позволяет:

- приравнять количество обнаруживаемых ошибок кодом первой ступени к исправляемым ошибкам кодом второй ступени;
- исправлять любые ошибки в рамках одной локальной области памяти.

Структура методики функционального диагностирования ОЗУ СОИ РТК ВН с БЛА

Структура методики, представленная на рис. 4, определяет выбор способа кодового контроля для заданных условий. Определяющими факторами для выбора способа контроля являются:

- 1) условия функционирования воздушных РТК (высота и продолжительность полета, вероятность появления внешних преднамеренных или непреднамеренных деструктивных воздействий и их совокупности, применение ядерной энергетической установки и пр.);
- 2) характер возникающих ошибок (вызванных отказами или сбоями, кратностью их возникновения);
- 3) требования к показателям качества РТК ВН (надежность, массогабаритные показатели, энергетические затраты).

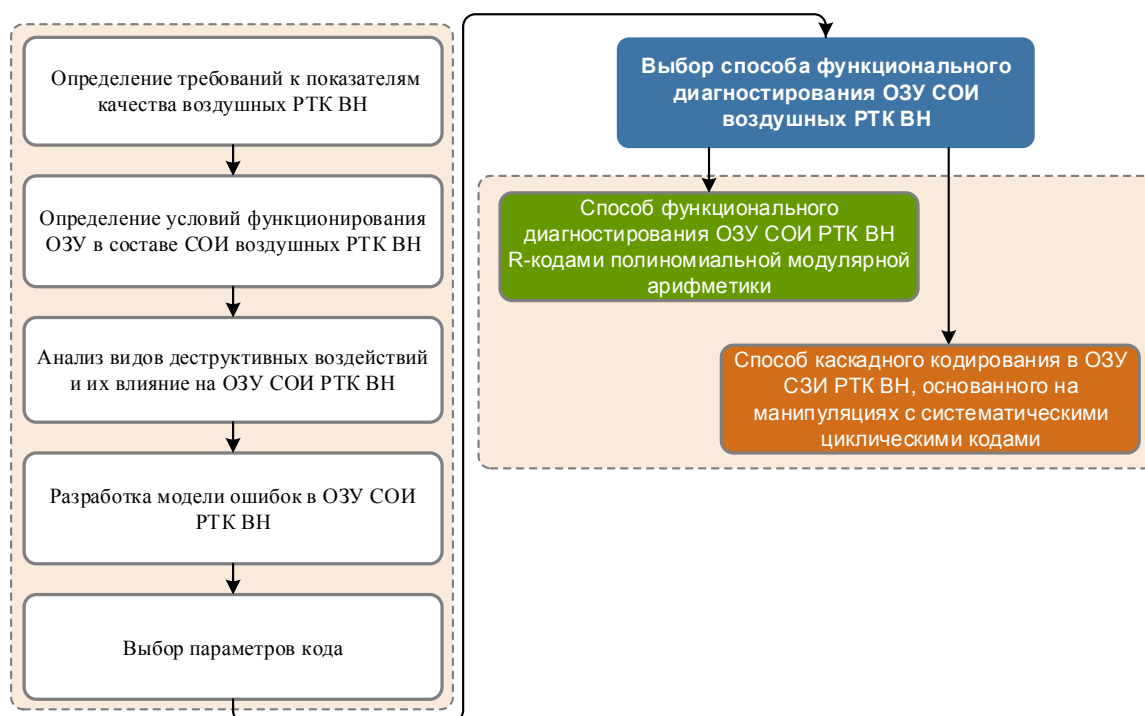


Рис. 4. Структура методики функционального диагностирования ОЗУ СОИ воздушных РТК ВН

Оценка достоверности информации, извлекаемой из ОЗУ СОИ РТК ВН

Достоверность извлекаемой из ОЗУ информации будем характеризовать вероятностью правильного декодирования кодового слова.

Примем следующие обозначения кратности ошибки:

1) под кратностью ошибки в кодовой комбинации первой ступени кодирования понимается количество $q_{\text{first stage}}$ искаженных двоичных букв одного кодового слова;

2) под кратностью ошибки на второй ступени кодирования понимается количество $q_{\text{second stage}}$ искаженных двоичных кодовых слов второй ступени кодирования;

Пусть $p_{\text{bit error}}^{(\text{type 1})}$ и $p_{\text{bit error}}^{(\text{type 2})}$ – вероятности возникновения *ошибок первого и второго типа* соответственно в одной двоичной букве кодового слова первой ступени; ошибки первого и второго типа могут возникать в локальной области памяти одновременно, являются совместными и независимыми событиями.

Таким образом, вероятность $P_{\text{correct detection}}^{(\text{complex type})}$ правильного обнаружения ошибок комбинированного характера определяется суммой вероятностей $P_{\text{correct detection}}^{(\text{type 1})}$ и $P_{\text{correct detection}}^{(\text{type 2})}$ – правильного обнаружения ошибок первого и второго типа соответственно:

$$P_{\text{correct detection}}^{(\text{complex type})} = P_{\text{correct detection}}^{(\text{type 1})} + P_{\text{correct detection}}^{(\text{type 2})} - P_{\text{correct detection}}^{(\text{type 1})} P_{\text{correct detection}}^{(\text{type 2})}, \quad (1)$$

где:

$$P_{\text{correct detection}}^{(\text{type 1})} = 1 - \sum_{q_{\text{first stage}}=d_{\min}}^{k+u} \frac{\Gamma(k+u) p_{\text{bit error}}^{(\text{type 1}) q_{\text{first stage}}} (1 - p_{\text{bit error}}^{(\text{type 1})})^{k+u-q_{\text{first stage}}}}{\Gamma(q_{\text{first stage}}) \Gamma(k+u-q_{\text{first stage}})}; \quad (2)$$

$$P_{\text{correct detection}}^{(\text{type 2})} = \frac{p_{\text{bit error}}^{(\text{type 2})}}{2^{k+u}} \left(1 - \sum_{q_{\text{first stage}}=d_{\min}}^{k+u} \frac{\Gamma(k+u)}{\Gamma(q_{\text{first stage}}) \Gamma(k+u-q_{\text{first stage}})} \right). \quad (3)$$

где $\Gamma(\cdot)$ – гамма-функция; u – количество избыточных двоичных символов циклического кода.

Ввиду того, что рассматриваемый двухступенчатый код исправляет все ошибки обнаруживаемой кратности кодом первой ступени, в пределах одной локальной области памяти, его корректирующие способности будем характеризовать обнаруживающей способностью кода первой ступени. Таким образом, из выражений (1)-(3), с учетом связи минимального кодового расстояния с количеством обнаруживаемых ошибок, получим выражение для расчета вероятности правильного исправления ошибок на уровне локальных областей памяти при двухступенчатом кодовом контроле:

$$P_{\text{correct correction two-step code}}^{(\text{complex type})} = 1 - \sum_{q_{\text{second stage}}=2}^{n+1} \frac{\Gamma(n+1)}{\Gamma(q_{\text{second stage}}) \Gamma(n+1-q_{\text{second stage}})} P_{\text{correct detection}}^{(\text{complex type}) q_{\text{second stage}}} \times \left(1 - P_{\text{correct detection}}^{(\text{complex type})} \right)^{n-q_{\text{second stage}}+1}.$$

$$P_{\text{correct correction two-step code}}^{(\text{complex type})} = 1 - \sum_{q_{\text{second stage}}=2}^{n+1} \frac{\Gamma(n+1)}{\Gamma(q_{\text{second stage}}) \Gamma(n+1-q_{\text{second stage}})} P_{\text{correct detection}}^{(\text{complex type}) q_{\text{second stage}}} \times \left(1 - P_{\text{correct detection}}^{(\text{complex type})} \right)^{n-q_{\text{second stage}}+1}.$$

Для определения наиболее эффективного способа контроля информации в ОЗУ для рассматриваемого характера ошибок, задаваемого выражением (1), сравним вероятность правильного декодирования кодового слова при двуступенчатом кодовом контроле и вероятностью правильного декодирования кодового слова с помощью классического линейного кода.

Выражения (2) и (3) примут вид:

$$P_{\text{correct correction LC}}^{(\text{type 1})} =$$

$$= 1 - \sum_{q_{\text{first stage}}=\left\lceil \frac{d_{\min}-1}{2} \right\rceil+1}^{k+u} \frac{\Gamma(k+u) p_{\text{bit error}}^{(\text{type 1}) q_{\text{first stage}}} (1 - p_{\text{bit error}}^{(\text{type 1})})^{k+u-q_{\text{first stage}}}}{\Gamma(q_{\text{first stage}}) \Gamma(k+u-q_{\text{first stage}})},$$

$$P_{\text{correct correction LC}}^{(\text{type 2})} =$$

$$= \frac{p_{\text{bit error}}^{(\text{type 2})}}{2^{k+u}} \left(1 - \sum_{q_{\text{first stage}}=\left\lceil \frac{d_{\min}-1}{2} \right\rceil+1}^{k+u} \frac{\Gamma(k+u)}{\Gamma(q_{\text{first stage}}) \Gamma(k+u-q_{\text{first stage}})} \right).$$

где $\lceil a \rceil$ – наименьшее целое число $\geq a$.

Вероятность правильного декодирования линейным кодом (LC) ошибок комплексного типа определяется:

$$P_{\text{correct correction LC}}^{(\text{complex type})} = \sum_{q_{\text{second stage}}=0}^n \frac{\Gamma(n)}{\Gamma(q_{\text{second stage}})\Gamma(n-q_{\text{second stage}})} \times \left(P_{\text{correct correction LC}}^{(\text{type 1})} + P_{\text{correct correction LC}}^{(\text{type 2})} - P_{\text{correct correction LC}}^{(\text{type 1})} \times P_{\text{correct correction LC}}^{(\text{type 2})} \right)^{q_{\text{second stage}}} \times \left(1 - \left(P_{\text{correct correction LC}}^{(\text{type 1})} + P_{\text{correct correction LC}}^{(\text{type 2})} - P_{\text{correct correction LC}}^{(\text{type 1})} \times P_{\text{correct correction LC}}^{(\text{type 2})} \right) \right)^{n-q_{\text{second stage}}}$$

На рис. 5 представлено сравнение вероятностей возникновения ошибки в ОЗУ СОИ РТК ВН при контроле двухступенчатым кодом и при контроле линейным кодом, при равных условиях по вводимой кодовой избыточности; $P^{(1)}$ – вероятность правильного декодирования при контроле линейным кодом, $P^{(2)}$ – вероятность правильного декодирования при контроле двухступенчатым кодом.

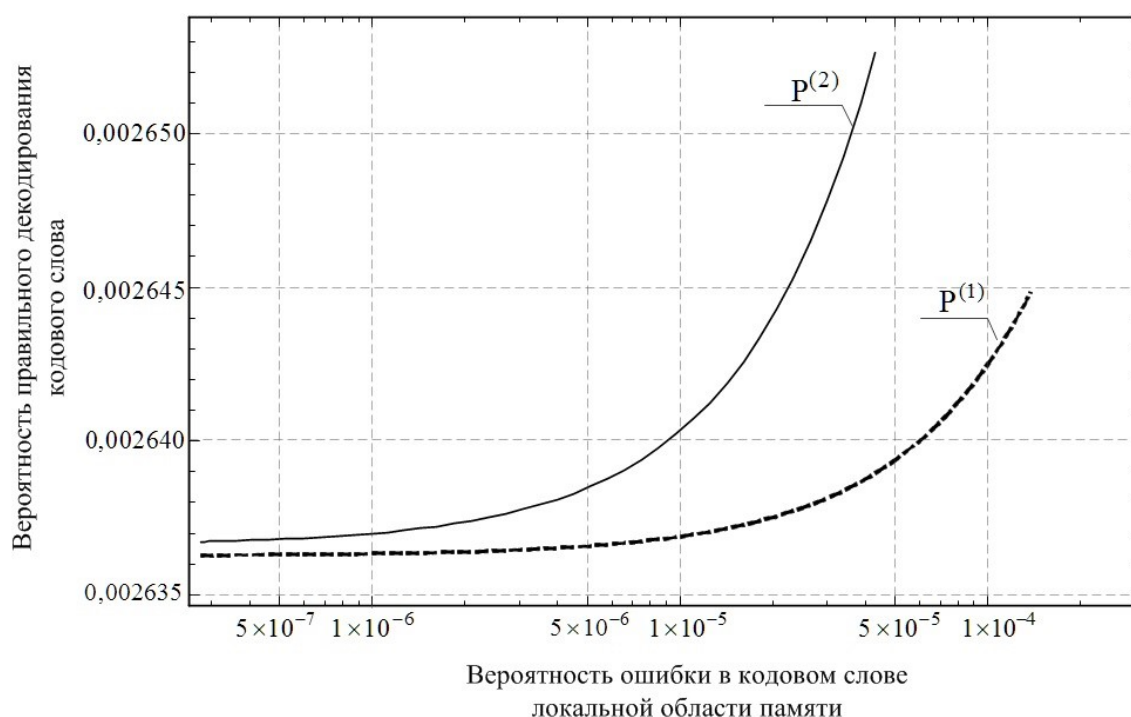


Рис. 5. Зависимости вероятностей правильного декодирования кодового слова, считываемого из ОЗУ, от вероятности возникновения ошибки в этом кодовом слове в процессе его хранения в условиях рассматриваемого характера ошибок

Заключение

Показано, что ОЗУ СОИ РТК ВН, функционируют в сложных изменяющихся во времени условиях обстановки, характеризующихся комплексом непреднамеренных и преднамеренных деструктивных воздействий. Применение методов функционального диагностирования, основанных на применении какого-либо одного класса избыточных кодов, контролирующих ошибки, не позволяет решить общую проблему контроля ошибок, имеющих комплексный характер проявления и происхождения.

Например, двоичные циклические коды, хорошо зарекомендовавшие себя для коррекции одиночных ошибок и ошибок невысокой кратности, обеспечивающие хорошие показатели по избыточности вводимого контрольного оборудования, бесполезны в условиях появления пачек ошибок и отказах оборудования. Напротив, коды, такие как коды Рида-Соломона, прекрасно подходят для коррекции байтовых и других пакетирующихся ошибок. Но при этом, при тех же затратах оборудования, которые могли бы потребоваться при применении двоичных линейных кодов, с достаточно высокой степенью избыточности, демонстрируют явный проигрыш для модели массовых одиночных ошибок и ошибок невысокой кратности.

Предложено два способа двухступенчатого кодирования, основанных на интеграции линейных (циклических) двоичных кодов и многозначных кодов модулярной арифметики. Первый способ ориентирован на модель ошибок, предусматривающую значительный уровень пакетирующихся ошибок по отношению к одиночным ошибкам и ошибкам малой кратности. Второй способ наоборот – ориентирован на массовые ошибки невысокой кратности. Он позволяет обнаруживать и исправлять пакетирующиеся ошибки и, при этом, обеспечивает невысокие затраты контрольного оборудования.

Направлением дальнейших исследований является разработка и совершенствование алгоритмов и схемотехнических решений кодирования и декодирования данных, так как их характеристики существенно определяют показатели скорости функционирования ОЗУ.

Литература

1. Шеремет И. Б., Рудианов Н. А., Рябов А. В., Хрущев В. С. Проблемы развития роботизированного вооружения сухопутных войск // Известия ЮФУ. Технические науки. 2013. № 3. С. 21-24.
2. Рубцов И. В. Вопросы состояния и перспективы развития отечественной наземной робототехники военного и специального назначения // Известия ЮФУ. Технические науки. 2013. № 3. С. 14-21.
3. Каримов А. Х. Возможность авиационных беспилотных систем следующего поколения // Труды МАИ. 2011. № 47. С 1-11.
4. Коршунов Ф. П., Гатальский Г. В., Иванов Г. М. Радиационные эффекты в полупроводниковых приборах. – М: Наука и Техника. 1978. – 232 с.
5. Вавилов В. С., Ухин Н. А. Радиационные дефекты в полупроводниках и полупроводниковых приборах. – М.: Атомиздат. 1969. – 312 с.

6. Taizhi Liu, Chang-Chih Chen, Woongrae Kim, Linda Milor. Comprehensive reliability and aging analysis on SRAMs within microprocessor systems // Microelectronics Reliability. August–September 2015. Vol. 55. № 9–10. P. 1290-1296.
7. Герасимов Ю. М., Григорьев Н. Г., Гусев В. В., Кобыляцкий А. В., Петричкович Я. Я. Радиационно-стойкие КМОП СБИС ОЗУ по технологии объемного кремния // Проблемы разработки перспективных микро- и наноэлектронных систем (МЭС). 2014. № 3. С. 171-176
8. Стенин В. Я., Черкасов И. Г. Влияние топологии субмикронных КМОП ячеек памяти DICE на чувствительность ОЗУ к воздействию отдельных ядерных частиц // Микроэлектроника. 2011. № 3(40). С. 184-190.
9. Кузьмин М., Бузмаков А. Промышленная флэш-память // Компоненты и технологии. 2009. № 10(99). С. 33-38.
10. Щербаков Н. С. Достоверность работы цифровых устройств. – М.: Машиностроение. 1989. – 224 с.
11. Kees A. Schouhamer Immink. Codes for mass data storage systems. Second Edition. – Shannon Foundation Publishers, Institute for Experimental Mathematics, University of Essen-Duisburg, Essen, Germany, 2004. – 349 p.
12. Бетелин В. Б., Баранов С. В., Бобков С. Г., Краснюк А. А., Осипенко П. Н., Стенин В. Я., Черкасов И. Г., Чумаков А. И., Яненко А. В. Перспективы использования субмикронных КМПОМ СБИС в сбоеустойчивой аппаратуре, работающей при воздействии атмосферных нейтронов // Микроэлектроника. 2009. № 1 (38). С. 48-52.
13. Mittal S., Vetter J. S. A Survey of Techniques for Modeling and Improving Reliability of Computing Systems. IEEE Transactions on Parallel & Distributed Systems // 2016. №4(27). P. 1226-1238. doi:10.1109/TPDS.2015.2426179.
14. Макаренко С. И. Робототехнические комплексы военного назначения – современное состояние и перспективы развития // Системы управления, связи и безопасности. 2016. № 2. С. 73-132.
15. Финько О. А. Контроль и реконфигурация аналого-цифровых устройств, функционирующих в системе остаточных классов // Электронное моделирование. 2000. № 4 (22). С. 92-103.
16. Fujiwara E. Code Design for Dependable Systems: Theory and Practical Applications. – Hoboken, New Jersey: John Wiley and Sons, Inc., 2006. – 720 p.
17. Котов П. А. Выбор кодов для систем передачи информации дискретными сигналами. – Л.: Военная Краснознаменная академия связи, 1966. – 193 с.
18. Березюк Н. Н., Андрущенко А. Г., Мощицкий С. С. Кодирование информации (двоичные коды). – Харьков: Высшая школа, 1978. – 252 с.

References

1. Sheremet I. B., Rudianov N. A., Ryabov A. V., Khrushev V. S. Justification of Combat and Support a Family of Robots to Fight in. *Izvestiya SFedU. Engineering Sciences*, 2013, no. 3, pp. 21-24 (in Russian).

2. Rubtsov I. V. Current situation and perspective of development for ground military and special robotics. *Izvestiya SFedU. Engineering Sciences*, 2013, no. 3, pp. 14-21 (in Russian).
3. Karimov A. H. Vozmozhnost' aviacionnyh bespilotnyh sistem sleduyushchego pokoleniya [The possibility of next-generation unmanned aircraft systems]. *Trudy MAI*, 2011, no. 47, pp. 1-11 (in Russian).
4. Korshunov F. P., Gatal'skij G. V., Ivanov G. M. *Radiacionnye ehffekty v poluprovodnikovyyh priborah* [Radiation Effects in Semiconductor Devices]. Moscow, Nauka i Tekhnika Publ., 1978. 232 p. (in Russian).
5. Vavilov V. S., Uhin N. A. *Radiacionnye defekty v poluprovodnikah i poluprovodnikovyyh priborah* [Radiation Defects in Semiconductors and Semiconductor Devices]. Moscow, Atomizdat Publ., 1969. 312 p. (in Russian).
6. Taizhi Liu, Chang-Chih Chen, Woongrae Kim, Linda Milor. Comprehensive reliability and aging analysis on SRAMs within microprocessor systems. *Microelectronics Reliability*, August–September 2015, vol. 55, no. 9–10, pp. 1290-1296.
7. Gerasimov Y.M., Grigoryev N.G., Goussev V.V. Kobyl'yatskiy A.V. Petrichkovich Ya. Ya., Petrichkovich Y. Y. Radiation-hardened CMOS VLSI SRAM in bulk technology. *Problems of advanced micro- and nanoelectronic systems development (MES)*, 2014, no 3, pp. 171-176 (in Russian).
8. Stenin V. Y., Cherkasov I. G. Memory-cell layout as a factor in the single-event-upset susceptibility of submicron dice CMOS SRAM. *Russian Microelectronics*, 2011, vol. 40. no 3. pp. 170-175 (in Russian).
9. Kuz'min M., Buzmakov A. Promyshlennaya flehsh-pamyat' [Industrial flash memory]. *Komponenty i tekhnologii*, 2009, vol. 99, no 10, pp. 33-38 (in Russian).
10. Sherbakov N. S. *Dostovernost' raboty cifrovyyh ustroystv* [Reliability of Digital Devices]. Moscow, Mashinostroenie Publishers, 1989. 224 p. (in Russian).
11. Kees A. Schouhamer Immink. *Codes for mass data storage systems*. Second Edition. Shannon Foundation Publishers, Institute for Experimental Mathematics, University of Essen-Duisburg, Essen, Germany, 2004. 349 p.
12. Betelin V. B., Bobkov S. G., Krasnyuk A. A., Osipenko P. N., Stenin V. Ya., Cherkasov I.G., Baranov S. V., Chumakov A. I., Yanenko A. V. Prospects for using submicron CMOS VLSI in fault-tolerant equipment operating under exposure to atmospheric neutrons. *Russian Microelectronics*, 2009, vol. 38, no. 1, pp. 43-47 (in Russian).
13. Mittal S., Vetter J. S. A Survey of Techniques for Modeling and Improving Reliability of Computing Systems. *IEEE Transactions on Parallel & Distributed Systems*, 2016, vol. 27, no. 4, pp. 1226-1238. doi:10.1109/TPDS.2015.2426179.
14. Makarenko S. I. Military Robots – the Current State and Prospects of Improvement. *Systems of Control, Communication and Security*, 2016, no. 2, pp. 73-132. (in Russian).
15. Finko O. A. *Check and Reconfiguration of Analog-to-Digital Devices Operating in the System of Residual Classes*. Engineering Simulation, 2001, vol. 18, pp. 531-543.

16. Fujiwara E. *Code Design for Dependable Systems: Theory and Practical Applications*. John Wiley and Sons, Inc., Hoboken, New Jersey, 2006, 720 p.
17. Kotov P. A. *Vybor kodov dlya sistem peredachi informacii diskretnymi signalami* [Selection of codes for data transmission systems with discrete signals]. Leningrad, Voennaya Krasnoznamennaya akademiya svyazi, 1966, 193 p. (in Russian).
18. Berezyuk N. N., Andrushchenko A. G., Moshchickij S. S. *Kodirovanie informacii (dvoichnye kody)* [Information encoding (binary codes)]. Har'kov, Vysshaya shkola Publ., 1978. 252 p. (in Russian).

Статья поступила 9 ноября 2018 г.

Информация об авторах

Козлов Роман Николаевич – соискатель ученой степени кандидата технических наук. Адъюнкт специальной кафедры. Краснодарское высшее военное училище им. генерала армии С. М. Штеменко. Область научных интересов: защита информации, функциональное диагностирование цифровых устройств. E-mail: kozlovroman2016@yandex.ru

Финько Олег Анатольевич – доктор технических наук, профессор. Академический советник. Российская академия ракетных и артиллерийских наук. Область научных интересов: информационная безопасность и параллельные вычисления в алгебраических структурах, функциональный контроль и обеспечение отказоустойчивости средств обработки информации, контроль целостности и имитозащита данных. E-mail: ofinko@yandex.ru

Адрес: 350035, Россия, г. Краснодар, ул. Красина, д. 4.

Functional diagnostics method of storage devices for military robotic systems

R. N. Kozlov, O. A. Finko

*The main **relevance of the research topic** is devoted to the technical, especially functional diagnosis of the random access memory (RAM) devices used at the destructive conditions for achieving high scales of its reliability. Such storage devices include memory chips which are the part of information processing and protection means placed on-board robotic systems for military use in case of the enemy influence or extreme environments. The classic methods of inserting of structural and logical redundancy (like duplication, majority triplication, methods of noise proof coding) are used for required indices providing. Likewise, the existing methods of improving of the reliability neither always match to the point of inserted machine redundancy, nor consider a total combination of destructive influence. Considered ways of the functional diagnosis of RAM suppose a combining influence resistance and adaptive usage availability operated by the great majority of information processing tools made for the storage devices of the robotic systems for military use. The correct application of the considered methods can be limited with the agreed strategy of information recording and agreed error scheme of each memory type. The **aim of the study** is improvement of the probability of correct decoding of the data received from on-board RAM of the robotic systems for military use which deals with the complicated destructive influence. **Scientific novelty** of the researched method lies in consideration of the wide analysis of destructive influence characteristics and provides growth of RAM data reability. As a*

*result, the evaluation rate gives the ground to state that the usage of classic methods of functional diagnosis does not completely match to the modern requirements of safety for RAM storage devices of the robotic systems for military use. The results of the comparative evaluation based on the used and offered methods of control of RAM data show the offered ones' profit while using of the default error model. **The practical significance** is contained in availability of choosing the best way of the memory device control depending on requirements for weight and size indicators and power consumption of the storage devices of the robotic systems for military use. The algorithms developed within the method let prevent the errors along with reconfigure RAM in case of memory components failures occur.*

Key words: functional diagnosis, error correction codes, random access memory devices, reliability of the random access memory devices, the robotic systems for military use.

Information about Authors

Roman Nikolaevich Kozlov – postgraduate student of special Department. Krasnodar higher military school named after general of army S. M. Shtemenko. Field of research: information security, the functional diagnosing of digital devices. E-mail: kozlovroman2016@yandex.ru

Oleg Anatolyevich Finko – doctor of engineering, professor. Academic Advisor. Russian Academy of Rocket and Artillery Sciences. Field of research: information security and parallel computing in algebraic structures, functional control and fault tolerance of information processing, integrity control and data protection. E-mail: ofinko@yandex.ru

Address: Russia, 350035, Krasnodar, Krasina street, 4.