С.В. Гаврилов, С.И. Гуров, Т.Д. Жукова, В.С. Рухлов, Д.И. Рыжова, Д.В. Тельпухов

МЕТОДЫ ПОВЫШЕНИЯ СБОЕУСТОЙЧИВОСТИ КОМБИНАЦИОННЫХ ИМС НА ОСНОВЕ ИЗБЫТОЧНОГО КОДИРОВАНИЯ*

Введение

В данной статье рассматривается проблема повышения сбоеустойчивости применительно к комбинационным ИМС. Под сбоем комбинационной схемы понимается факт получения выходного вектора, отличающегося от истинного инверсией некоторых разрядов. В качестве аналогии понятий «отказоустойчивость» и «надёжность» используются термины «*помехоустойчивость*», «*сбоеустойчивость*» и «*помехозащищённость*» ИМС соответственно.

Для обнаружения и возможной последующей коррекции сбоев методами функционального диагностирования, когда ИМС непосредственно реализует предписанный алгоритм, необходимо введение в неё той или иной аппаратной избыточности. В результате ИМС оказывается снабжённой схемами встроенного контроля (СВК). Полученные таким образом схемы называют самопроверяемыми [1, 2]. *Самопроверяемость* есть способность устройства обнаруживать неисправности в процессе функционирования.

Самым простым и наиболее часто используемым на практике способом обеспечения самопроверяемости является универсальный метод горячего аппаратного резервирования основной схемы, т.е. прямое использование *аппаратная избыточности*. Для восстановления информации далее применяется *мажорирование* – процедура коррекции выхода путём сравнения результатов, полученных параллельным путём, и выдача наиболее совпадающих результатов. Почти исключительно используется *троирование* аппаратуры (TMR, Triple Modular Redundancy, тройное модульное резервирование). Очевидно, применение аппаратного резервирования характеризуется значительным проигрышем в площади схемы, но и минимальными временными задержками.

В [14] предложен оригинальный метод обеспечения отказоустойчивости на основе искусственных нейронных сети специального вида (коммутаторных и доменных), использующий резервирование блоков.

* Исследование выполнено за счет грантов Российского научного фонда (проекты №14-19-01036, 16-01-00196)

Временная избыточность связана с возможностью неоднократного повторения определённого вычисления, При этом каждый выходной вектор вычисляется одной и той же схемой несколько раз и далее производится сравнение результатов. Такой подход избавит только от кратковременной самоустраняющейся ошибки и приводит к выигрышу в сложности схемы, но к проигрышу по времени.

Одним из перспективных подходов к решению поставленной задачи является введение избыточности в информационные потоки синтезируемой схемы [1, 3, 8]. Такой тип избыточности будем называть *информационной* (не забывая при этом, что любая избыточность при функциональной диагностике схем в конце концов обеспечивается встроенной дополнительной контролирующей аппаратурой).

В рамках данного подхода наиболее распространённым методом является применение избыточного кодирования выходных векторов комбинационных схем. Ясно, что здесь невозможно применить помехозащищённое кодирование уже вычисленных выходных векторов, поскольку таковые могут быть получены с ошибками. Поэтому дополнительные проверочные разряды кода должны вычисляться одновременно с информационными (предполагается использование разделимых кодов, как наиболее удобных и естественных для данной задачи).

С теоретической точки зрения можно сказать об осуществлении систематического блокового. При таком кодировании считают, что кодовое слово длины $n = k + m$ содержит в себе k информационных и дополнительно ещёm проверочных бит. Для сравнительно коротких кодовых слов кодеры и декодеры могут просто содержать в памяти все возможные варианты, или даже реализовывать их в виде полупроводниковой схемы. Разделимый блоковый код описывают тройкой ров (n, k, d) или, упрощённо, парой (n, k), где d - *кодовое расстояние* (минимальное расстояние между словами кода). Очевидно у кода, исправляющего r ошибок, кодовое расстояние должно быть не менее $2r + 1$. Величину $R = k/n$ называют *скоростью*, а $\frac{m}{n} = 1 - R$ – *избыточностью кода*.

Экспериментальное определение кратностей ошибок

Важной особенностью комбинационных схем является то, что возникающее при сбоях искажение информации вряд ли адекватно описывается в рамках традиционной модели двоичного симметрического канала, которая обычно используется при разработке избыточных кодов. Обоснованными представляются предположения о следующем характере результатов сбоев комбинационных ИС. Во-первых, одиночная неисправность того или иного элемента ИС может привести к кратной ошибке на выходе схемы, в результате чего типичной является ситуация либо вообще отсут-

ствия ошибки (*маскирование*), либо наличия сразу нескольких ошибок на выходе схемы (число ошибок – её *кратность*). Во-вторых, наиболее частыми являются ошибки константного (stuck-at faults) типа.

Для проверки первого предположения были проведено исследование кратности возникающей ошибки на выходе комбинационных бенчмарк-схем набора ISCAS'85 [9] при возникновении одиночной ошибки некоторого элемента схемы. В различных экспериментах было протестировано от 10 до 15 схем.

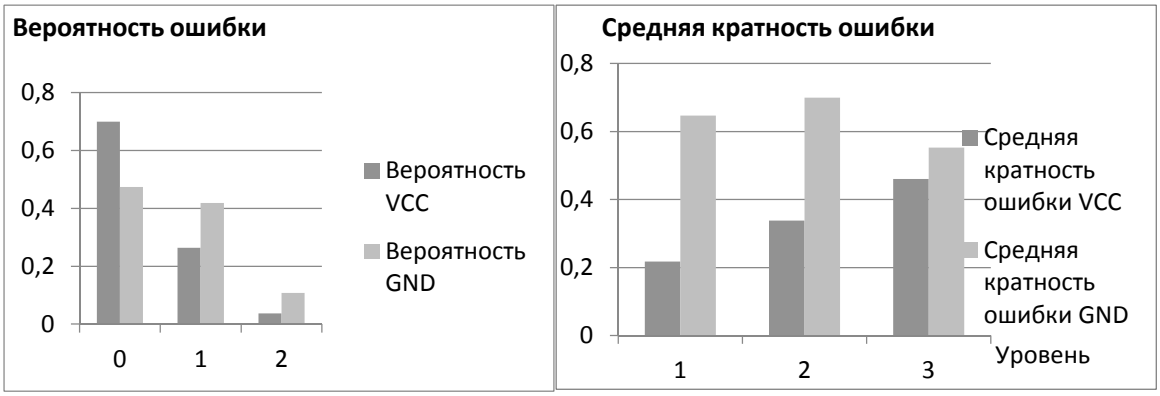
Исследования влияния ошибки инвертирования на выходе какого-либо элемента комбинационной схемы проводились следующим образом.

1. Сравнивались выходы комбинационных схем – исправной и с ошибкой.

2. На входы каждой из схем подались одинаковые случайные значения и подсчитывалось количество несовпадающих значений на выходах схем.

3. Для каждой схемы было проведено 20 тыс. симуляций с различными значениями на входе схемы и с ошибкой в различных узлах.

В результате была подсчитана частота возникновения ошибок определённой кратности на выходах для каждого набора входных данных.



а) б)

Рис 1. Схема C17. Константная ошибка: замыкание выхода элемента схемы на питание и землю.

а) зависимость вероятности выходной ошибки от её кратности;

б) средняя кратность в зависимости от уровня её возникновения.

Также исследовалось влияние места возникновения сбоя в схеме на кратность ошибки на выходе. Для этого аналогичным описанным выше образом было оценено математическое ожидание кратности ошибки для каждого уровня схемы.

Полученные данные позволяют сделать следующие выводы:

1) вероятность маскирования одиночной ошибки инвертирования высока и составляет 60-80%;
2) вероятность ошибки, вообще говоря, падает с её кратностью, однако вероятность ошибки кратности более 2 составляет не менее 10%;
3) наиболее чувствительны к ошибкам либо средние уровни схем, либо сразу и первые, и последние.

Также моделировалось влияние одиночных константных ошибок (замыкание выхода какого-либо элемента на землю GND, или шину питания VCC) на выходы комбинационной схемы.

Исследование проводилось по следующей схеме.

1. Сравнивались выходы исследуемой исправной схемы и её вариант с константной ошибкой обоих типов.
2. На входы каждой из схем подавались одинаковые случайные значения и подсчитывалось количество несовпадающих значений выходных векторов. Для каждой схемы было сделано 40 000 запусков (по 20 000 запусков для каждого типа ошибки) с различными значениями на входе схемы и с ошибкой в различных узлах схемы.
3. Для каждого набора входных данных подсчитывалась относительная частота возникновения ошибок определенной кратности на выходах. Ниже приведены некоторые типичные вероятностные распределения кратности ошибки на выходе, в зависимости от типа ошибки.
4. Также исследовалось влияние локализации ошибки на её кратность в выходном векторе. Для этого аналогичным образом было оценено среднее значение кратности ошибки для каждого уровня схемы.
5. Кроме того для ряда схем были исследованы их мажорированные версии.

По результатам моделирования можно сделать вывод об увеличении возможной кратности константной ошибки по сравнению со случаем ошибки инвертирования.

Для части схем ISCAS’85 было реализовано тройное модульное резервирование схемы с добавлением мажоритарного элемента, состоящего из четырех двухвходовым элементов: трёх логических «И» и двух логических «ИЛИ». Мажоритарный элемент добавляет минимум три дополнительных уровня в каждую схему. Исследование выполнено аналогично

описанной выше методике. Для сравнения, в диаграммы добавлены представленные выше данные схем без применения методов кратного резервирования.

Для большей наглядности диаграммы разделены по типу ошибки (замыкание на линию питания, и замыкание на линию земли соответственно).

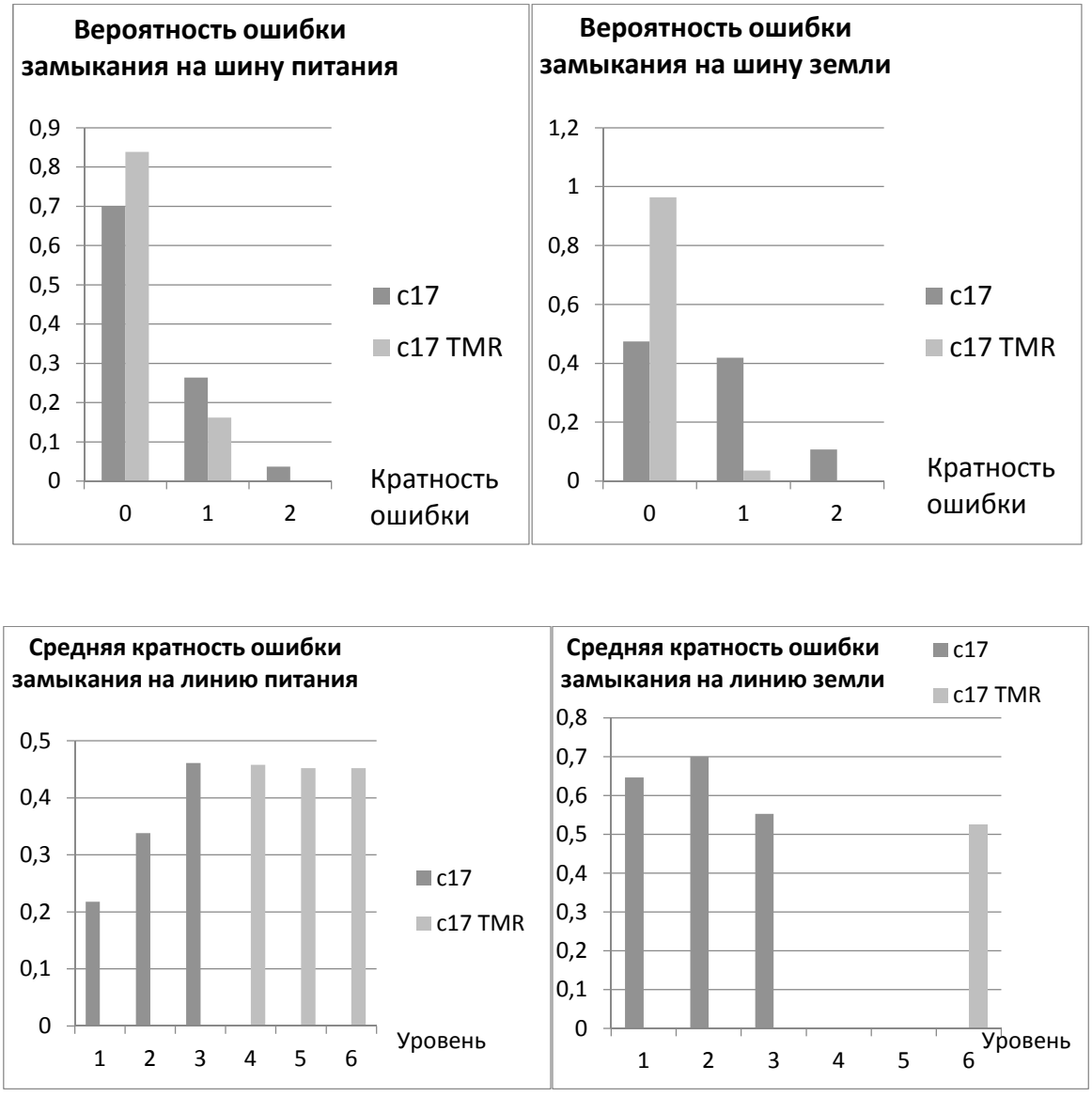


Рис 2. Схема C17. Константная ошибка: замыкание выхода элемента схемы на питание и землю. Зависимости от кратности ошибки и уровня её возникновения с аппаратным троирование и без.

Можно видеть, что использование TMR без специальных мер защиты контрольных схем малоэффективно.

Сбоеустойчивость: парирование избыточными кодами

Ясно, что при использовании избыточного кодирования для обеспечения сбоеустойчивости комбинационных схем требования к качеству используемых кодов (избыточность при данном числе обнаруживаемых/исправляемых ошибок) не являются слишком жёсткими. При этом имеющиеся технологические и схемные решения позволяют обеспечить существенно более высокий уровень помехозащищённости кодирующей схемы по сравнению с основной, что позволяет считать работу данной схемы безошибочной [1, 8, 11, 13]. Данные решения обосновываются тем, что длина вектора проверочных бит значительно короче вектора бит информационных. Это позволяет предполагать и существенно меньшую сложность кодирующей схемы по сравнению с основной и поэтому затраты на её защиту указанными средствами предполагаются оправданными. С другой стороны, ясно, что данный подход имеет смысл, когда сложность СВК, состоящей из схемы, вычисляющей контрольные биты и схемы декодирования и коррекции, менее, чем удвоенная сложность основной схемы при сравнении с TMR.

Определение кодового расстояния d произвольного кода – сложная задача. Поэтому при создании помехоустойчивых кодов на первый план выходит проблема построения кодов с заданным кодовым расстоянием. Она решается при использовании БЧХ-кодов [4-7]. На сегодняшний день уже построены БЧХ-коды с практически значимыми параметрами.

Избыточные коды

Рассмотрим кратко избыточные коды, применение которых принципиально возможно для решения наших задач [2-6].

Обнаружение ошибок возможно с применением *кода Бергера,* у которого проверочные символы представляют двоичную запись числа единиц (или нулей) в последовательности информационных символов. Коды Бергера обнаруживают все одиночные ошибки и некоторую часть многократных. *Остаточные* (k, b)-коды, имеющие k информационных и $b = 2^q - 1, q \geqslant 1$ контрольных разрядов, содержат двоичное представление остатка от деления десятичного эквивалента числа (задаётся в информационных разрядах) на b. Ясно, что при $q = 1$ имеем код с проверкой на чётность. Контроль по чётности достаточно эффективен для выявления одиночных и множественных ошибок в условиях, когда они являются независимыми.

Оба указанных выше кода – нелинейные. Большая часть теории блокового кодирования построена на *линейных кодах*, образующих векторное подпространство координатного пространства 2^n. В линейных кодах сумма по модулю 2 любых кодовых слов – также кодовое слово. Ли-

нейные коды позволяют реализовывать эффективные алгоритмы кодирования/декодирования и в двоичном случае их называют групповыми, так как они образуют группу относительно операции «сумма по модулю 2». Линейные (n, k)-коды могут быть заданы матрицами – *щей* $G_{n\times k}$ или *проверочной* $H_{m\times n}$. Для них выполняются ния $v = Gu$, $Hv = 0$ для любого кодового слова v, а невыполнение последнего равенства свидетельствует о наличии ошибки.

Код Рида-Маллера - линейный $\left(2^q, k, 2^{q-\delta}\right)$-код с параметрами $q \geqslant$ ми $q \geqslant 3$, $\delta < m$ - порядок кода, количество информационных дов $k = \sum_{i=0}^{\delta} C_q^i$. Имеется простой способ построения порождающей матрицы, при котором код Рида-Маллера является систематическим и циклическим. Важным свойством рассматриваемых кодов является простота их декодирования, при котором исключается этап определения места ошибок и имеется возможность использования мажоритарного принципа декодирования.

Обычно при использовании избыточного кодирования для сбоеустойчивых схем предлагают использовать циклические коды, являющиеся подклассом линейных кодов. Код называется *циклическим* или *сдвиговым* (CRC, Cyclic Redundancy Code, циклический избыточный код), если он инвариантен относительно циклических сдвигов. Это объясняется простотой реализации процессов кодирования и декодирования информации. Кодирование сообщения циклическими кодами может быть осуществлено его умножением на *производящий полином* $g(x)$, а декодирование производится с помощью вычисленных *синдромов* – остатков от деления полученного вектора на $g(x)$. Данные операции легко реализуются на регистрах сдвига с обратными связями.

Среди циклических кодов для решения рассматриваемых наиболее популярны БЧХ-коды. Для оценочных целей можно считать, что вероятность невыявления ошибки в случае использования БЧХ-кодов, если ошибка на самом деле имеет место, равна 2^{-r}, где $r = \deg g(x)$ – степень образующего полинома.

Однако при использовании избыточных кодов для построения сбоеустойчивых схем контролирующие биты вычисляются параллельно с информационными. В силу этого оценки сложности кодирования, рассматриваемые в литературе для кодирования передаваемых сообщений, не годятся для кодирования выходных векторов ИС и определяющей становится именно сложность декодирования полученного выходного вектора из информационных и проверочных бит. Поэтому представляется эффективным использование простых *кодов Хэмминга* или *Голея* (подкласс кодов БЧХ, способных исправлять одну или три ошибки соответственно). При этом возможно вычисление проверочных бит для последовательных или пересекающихся сегментов выходного вектора основной схемы, опреде-

ляемых решением соответствующей оптимизационной задачи, аналогично [8]. В случае кодов Хэмминга определение ошибочной позиции может стать тривиальной задачей.

Линейные блоковые *SEC-DED-коды* (*single-error-detection double-error-correction,* определения одной и исправления двукратной ошибок), к которым относится код Хэмминга, позволяют исправлять однократные и детектировать двукратные ошибки в кодовом слове. Для таких (n, k)-кодов $k = 2^m, n = n + m + 2, m$ – целое. Обычно рассматривают SEC-DED-коды для $m = 4, 5, 6$. В литературе известны также как SEC-DED-коды Дутта и Ричтера [10, 12].

Другим перспективным подходом представляется здесь использование *линейных коды низкой плотности* (*LDPC-коды,* низкоплотностные коды, Low Density Parity-check Codes) или *коды с малой плотностью проверок на чётность.* Предложенные Р. Галлагером ещё в 1963 году, они потом были почти что забыты. В 1990-х годах обнаружилась их связь со специальным классом графов – *экспандерами*, теория которых сейчас активно развивается. Данные коды описываются разреженными проверочными матрицами, что уменьшает количество символов, входящих в проверочные соотношения [13]. Существенной положительной стороной таких кодов является то, что не только кодирование, но и декодирование выполняется достаточно быстро: для них сложность декодирования линейно зависит от длины *n* кода (при этом неизвестны субквадратичные алгоритмы кодирования, что не является критичным для нашей задачи).

При построении помехозащищённых кодов, исправляющих ошибки, длина кода может составлять тысячи бит, размеры порождающих и проверочных матриц таковы, что их и хранение становится практически невозможным. Использование LDPC-кодов, имеющих относительно мало единиц в матрице H, позволяет в этом случае эффективнее организовать процесс её хранения или же напрямую реализовать процесс декодирования с помощью полупроводниковой схемы. Ясно, что в нашем случае интересны алгоритмы декодирования LDPC-кодов сравнительно небольшой длины (с точки зрения простоты их реализации).

LDPC-код длины n с k информационными разрядами, каждая из $r = n - k$ строк проверочной матрицы H которого содержит не лее j единиц, будем обозначать (n, j, k). Условия существования такого кода с $d \geqslant 3$ формулируются следующим образом:

1) каждый $n = r + k$ столбцов матрицы H содержит по крайней мере одну единицу;

2) значение k является минимальным для данных n и j.

При этом проверочная матрица любого (n, j, k)-LDPC кода имеет вид $H = (D_{r \times k}\ I_r)$, где I_r – единичная матрица порядка r, а количество единиц в матрице $D_{k,r}$ не превышает $r(j - 1)$.

Принято различать *регулярные* и *нерегулярные* LDPC-коды. У первых проверочная матрица содержит заданные количества единиц в каждом столбце и каждой строке, а у вторых указанные количества являются переменными.

Для построения проверочной матрицы LDPC-кода необходимо вычислить начальную проверочную матрицу с помощью псевдослучайного генератора или воспользоваться методами, основанными на теории полей Галуа. Соответствующие LDPC-коды называют *случайными* (*random-like*) и *структурированными* соответственно. При этом лучшие характеристики имеют случайные коды, а структурированные коды позволяют использовать методы оптимизации процедур хранения, кодирования и декодирования [15].

Изложенное выше указывает на перспективность применения LDPC-кодов небольшой длины для построения сбоеустойчивых комбинационных ИМС.

Распространённым графическим способом является представление кода в виде двудольного графа, в котором k строк проверочной цы k соответствуют нижним вершинам графа, а n столбцов – верхним, при этом верхняя и нижняя вершины графа соединены ребром, если на пересечении соответствующих строки и столбца стоит единица. Такое представление LDPC-кодов задаёт экспандерный граф.

Экспандерами (расширяющими графами) называют сильно связанные разреженные графы, обладающими многим особыми свойствами [16]. Почти все однородные разреженные графы являются экспандерами; однако очень непросто построить такой граф явно. Эти графы оказались эффективным инструментом во многих приложениях, в том числе в теории кодирования. Построение экспандеров оказалось связано с глубокими вопросами алгебры и комбинаторики.

Заключение

Можно сказать, что избыточными кодами, наиболее перспективными в применении для синтеза помехозащищённых комбинационных схем являются SEC-DED-коды – код Хэмминга, код Голея, коды Рида-Маллера и LDPC-коды, при условии небольшого числа ожидаемых ошибок и длины кодов до нескольких десятков. При ожидаемом числе ошибок более 3 наиболее эффективны, по-видимому, соответствующие БЧХ-коды.

В дальнейшем планируется проведение проверки полученных в данной статье выводов, а также исследование числа маскированных, обнаруженных и пропущенных ошибок, полученных при внедрении ошибки в защищённые SEC-DED-кодами схемы набора ISCAS’85.

Литература

1. Huang H.-M., Wen H.-P. W. Fast-yet-accurate statistical soft-error-rate analysis considering full-spectrum charge collection / IEEE Design & Test, March/April 2013, pp. 77-86.
2. Согомонян Е. С., Слабаков Е. В. Самопроверяемые устройства и отказоустойчивые системы. М.: Радио и связь. 1989. - 208 с.
3. Хетагуров Я. А., Руднев Ю. П. Повышение надёжности цифровых устройств методами избыточного кодирования. М.: Энергия, 1974. С. 270.
4. Блейхут Р. Теория и практика кодов, контролирующих ошибки // М.: Книга по требованию, 2013. – 566 с.
5. Кодирование информации (двоичные коды). Справочник // Под ред. проф. Н. Т. Березнюка. - Харьков: Вища школа. - 1978.
6. Дадаев Ю. Г. Теория арифметических кодов. - М.: Радио и связь. – 1981.
7. Poolakkaparambil M., Mathew J. BCH code based multiple bit error correction in finite field multiplier circuits // ISQED, 2011, pp. 1-6.
8. Soobeeh, M. Yiorgos. Fault tolerant design of combinational and sequential logic based on a party check code // Proceedings of 18th IEEE international Symposium on Design and Fault Tolerance VLSI Systems (DFT'03).
9. Электронный ресурс [http://icdm.ippm.ru/w/Схемы ISCAS85].
10. Richter M. and all. New linear SEC-DED codes with reduced triple bit error miscreation probability // 14th Int. On-Line Testing Symposium. 2008. P 37-40.
11. Holland J.H. Adaptation in natural and artificial systems. University of Michigan Press, Ann Arbor. 1975.
12. Reviriego P., Martínez J., Maestro J. A. A method to design SEC-DED-DAEC codes with optimized decoding // IEEE Transactions on Device and Materials Reliability 14(3): 884-889.
13. Gallager R. G. Low density parity check codes. - Cambridge: M.I.T. Press, 1963.
14. Суханова Н. В. Методы обеспечения отказоустойчивости аппаратных средств вычислительных систем на основе искусственных нейронных сетей / Автореферат дисс. на соискание уч. степени д. тех. наук, Москва 2016 г.
15. Иванов Ф. И., Зяблов В. В., Потапов В. Г. Коды с малой плотностью проверок на чётность, основанные на полях Галуа // Информационные процессы, Том 12, № 1, 2012, стр. 68–83.
16. Hoory S., Linial N., Wigderson A. Expander graphs and their applications / Bulletin of the AMS, vol. 43, Number 4, Oct. 2006, pp.439-561.