На правах рукописи

Тахаан Осама

РАЗРАБОТКА КОРРЕКТИРУЮЩИХ КОДОВ ДЛЯ ИНФОРМАЦИОННОЙ ЗАЩИТЫ ТЕЛЕКОММУНИКАЦИЙ КОМПЬЮТЕРНЫХ СЕТЕЙ

Специальность: 05.12.13

‹‹Системы, сети и устройства телекоммуникаций››

АВТОРЕФЕРАТ

диссертации на соискание учёной степени

кандидата технических наук

Владимир 2012

Работа выполнена на кафедре радиотехники и радиосистем Владимирского государственного университета имени Александра Григорьевича и Николая Григорьевича Столетовых.

Научный руководитель: доктор технических наук, профессор
Галкин Александр Павлович

Официальные оппоненты: доктор технических наук, профессор
Монахов Михаил Юрьевич

кандидат технических наук
Вертилевский Никита Валерьевич

Ведущая организация: Владимирский филиал ОАО «Ростелеком»

Защита состоится « 22 » февраля 2012 г. в 14-00 часов на заседании диссертационного совета Д 212.025.04 при Владимирском государственном университете имени Александра Григорьевича и Николая Григорьевича Столетовых по адресу: 600000, г. Владимир, ул. Горького, д. 87.

Отзывы, заверенные печатью, просим направлять по адресу:
600000, г. Владимир, ул. Горького, д. 87, ВлГУ, ФРЭМТ.

С диссертацией можно ознакомиться в научной библиотеке Владимирского государственного университета имени Александра Григорьевича и Николая Григорьевича Столетовых.

Автореферат разослан « 20 » января 2012 г.

Ученый секретарь
диссертационного совета,
доктор технических наук, профессор Самойлов А.Г.

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Актуальность работы: Аналогично мировой экономике современная экономика Сирии опирается на новейшие информационные и телекоммуникационные технологии.

В настоящее время в стране широко используются компьютерные сети, которые привели к бурному распространению глобальных информационных сетей, открывающих принципиально новые возможности информационного обмена.

В то же время, в информационном пространстве Сирии потенциально существует угроза использования различных приемов создания мешающих воздействий, при этом преднамеренно или неумышленно создается опасность для жизни или здоровья людей или наступления других тяжких последствий, преследуются цели получения преимуществ при решении политических, экономических или социальных проблем.

Одним из перспективных направлений обеспечения работоспособности компьютерных сетей в экстремальных условиях, является разработка адаптивных отказоустойчивых систем, обеспечивающих автоматическое обнаружение, локализацию и исправление возникающих ошибок.

Вопросам использования корректирующих кодов для построения отказоустойчивых и информационно-защищенных вычислительных систем посвящены российские работы А.М. Гаврилова, Н.Д. Путинцева, Ю.Л. Сагаловича, Е.С. Согомоняна, Я.А. Хетагурова, Н.С. Щербакова, А.А. Павлова и других ученых.

Среди зарубежных работ в области использования корректирующих кодов для решения вопросов обеспечения надёжности и защиты от проникновений дискретных устройств большое значение имеют труды фон Неймана, Мура и Шеннона, Ф.Дж. Мак-Вильямс, Э. Берлекэмп, У. Питерсон.

Применение корректирующих кодов позволяет осуществлять процедуру поиска и коррекции ошибок, возникающих в процессе функционирования процессора телекоммуникационных сетей и повысить его эффективности. Поэтому обеспечение надежности и достоверности таких систем, как системы защиты, системы в контурах управления ответственными процессами или объектами, функционирующими в реальном масштабе времени и др. является одной из актуальных проблем.

Целью работы является разработка методического аппарата повышения отказоустойчивости функциональных узлов процессоров телекоммуникационных компьютерных сетей (КС) для обычных и экстремальных условий работы.

Объектом исследования работы являются функциональные узлы компьютеров банковских электронных сетей, систем управления движением транспортных средств, правительственных систем связи, элементов

технических систем безопасности Сирии.

Предметом исследования является теория и методики обеспечения отказоустойчивости функциональных устройств КС на основе корректирующих кодов.

Новизна научных исследований:

1. Предложен модифицированный итеративный линейный код повышенной обнаруживающей и корректирующей способности, адаптированный для защиты преобразователей информации КС.
2. Предложен методический аппарат функционально-кодовой защиты процессора при выполнении арифметических и логических операций.
3. Разработана методика построения структур защищенных вычислителей КС.

Методы исследования. При решении научной задачи использованы методы исследований, основанные на научных положениях: теории линейных корректирующих кодов, теории множеств, теории дискретных автоматов, теории надежности и элементов нечеткой логики, теории эксперимента.

Практическая значимость результатов работы состоит в следующем:

1. Ожидаемые научные результаты позволяют создать качественно новый уровень отказоустойчивости КС и обычных и в экстремальных условиях работы;
2. В зависимости от правила проведения дополнительных проверок, предлагаемые методики позволяют корректировать от 50% до 94% обнаруживаемых ошибок, обеспечить отказоустойчивость и достоверность функционирования компьютерных сетей в реальном масштабе времени, при допустимом снижении быстродействия исходного устройства.

Достоверность полученных результатов подтверждается использованием математической модели, адекватно отображающей реальные процессы, протекающие в дискретных устройствах, обоснованием и доказательством впервые полученных научных результатов и выводов, применением широко известных частных научных результатов, результатами внедрения разработок, ясной физической интерпретацией полученных результатов и их непротиворечивостью с существующими методами коррекции ошибок отказоустойчивых вычислителей.

Результаты, выносимые на защиту:

1. Сформулированная концепция обеспечения отказоустойчивости вычислителей КС для экстремальных условий работы.

2. Разработанные правила построения модифицированного итеративного линейного кода повышенной обнаруживающей и корректирующей способности, отличающегося от известных методов организацией дополнительных проверок при формировании синдрома ошибки, позволяющих существенно повысить корректирующие способности итеративного кода. Предлагаемая методика применения модифицированных кодов, в отличие от существующих методов, позволяет:
   - осуществлять построение отказоустойчивых запоминающих устройств (ЗУ) при малом числе информационных разрядов;
   - корректировать трехкратные ошибки в полубайте информации при условии обнаружения ошибок;
   - исправлять ошибки различной конфигурации (имеет свойства нелинейного кода).
3. Выявленные свойства, и разработанные теоретические положения, позволяющие создать методический аппарат функционально-кодовой защиты процессора при выполнении арифметических и логических операций (впервые разработана процедура адаптации линейных кодов для защиты преобразователей информации).
4. Разработанная функциональная модель, отказоустойчивого процессора, реализующего предлагаемый методический аппарат.
5. Полученное выражение для оценки аппаратурных затрат, вводимых для обеспечения отказоустойчивости при использовании предлагаемой методики кодирования информации.

Реализация и внедрение. Основные теоретические и практические результаты получены автором при выполнении диссертационной работы были внедрены на предприятиях ООО ‹‹Электроприбор››г. Москва; и НПО ‹‹РИК››(Ремонт Инженерных Конструкции) г. Владимир.

Апробация работы. Основные положения диссертационной работы докладывались и обсуждались на 4-х международных конференциях: 8-й Международной НТК «Перспективные технологии в средствах передачи информации», Владимир, РФ, 2009г.; Международной НК «Экономическая проблемы ресурсного обеспечения инновационного развития региона» Владимир, РФ, 2009г.; Международной НПК «Факторы развития региональных рынков» Владимир, РФ, 20011г.; 9-й Международной НТК «Перспективные технологии в средствах передачи информации», Владимир, РФ, 2011г.

Публикации. Результаты работы отражены в 11-ти научных трудах, в том числе в 3-х статьях Всероссийского издания из перечня ВАК; В 2-х отчетах о НИР (Г/Б №118, ВлГУ).

Структура и объем работы. Диссертация состоит из введения, трех глав, заключения, списка литературы и приложений. Общий объем работы составляет 169 страниц, в том числе 144 страниц основного текста, 10 страниц списка литературы и 15 страниц приложений, 30 рисунков, 10 таблиц.

СОДЕРЖАНИЕ РАБОТЫ

Во введении проводится обоснование актуальности диссертационной работы, научной значимости поставленной научной задачи, исследование состояния вопроса и постановка цели научных исследований, применительно, в частности, к Сирии.

В первой главе проводится анализ методик построения отказоустойчивых автоматизированных систем контроля, выбрана модель исследований, введены основные понятия, приняты ограничения и допущения, выявление существующих противоречий.

Обоснована целесообразность и выявлены особенности использования корректирующих кодов для обеспечения отказоустойчивости систем памяти КС. Определен класс корректирующих линейных кодов, требующих минимальных аппаратурных затрат на кодирование и декодирование информации.

Определена проблема использования корректирующих кодов для обеспечения отказоустойчивости преобразователей информации вычислителей КС.

Вторая глава посвящена разработке модифицированного итеративного кода повышенной обнаруживающей и корректирующей способности.

В результате проведенных исследований в работе были предложены шесть подходов построения модифицированных итеративных кодов.

Предлагаемые методы кодирования включают следующие основные положения: информация представляется в две строки, в каждой строке проводится проверка на четность, организуются диагональные проверки с участием, либо без участия контрольных разрядов.

Алгоритм кодирования информации первым подходом включает следующие положения:

1) информационные разряды делятся на две равных части и представляются в две строки

2) для каждой строки информационной матрицы организуется проверка на четность, т.е. информационная матрица представляется в виде:

$$\begin{matrix} y_1 & y_2 \ldots\ldots\ldots\ldots\ldots\ldots y_{k/2} & r_{\times 1} \\ y_{(k/2)+1} & y_{(k/2)+2} \ldots\ldots\ldots\ldots\ldots\ldots y_k & r_{\times 2} \end{matrix} \qquad (1)$$

3) для полученной информационной матрицы организуются правые и левые диагональные проверки. Число диагональных проверок (число контрольных разрядов диагональных проверок) определяется по формуле:

$$R_{\ddot{A}} = k + 4 \qquad (2)$$

4) кодовый набор передается в виде:

$$Y = y_1 y_2 \ldots . y_k \, r_1 r_2 \ldots \ldots . r_{k+4} \qquad (3)$$

5) результат сложения значений сигналов переданных и сформированных контрольных разрядов даст синдром ошибки:

$$E = e_1 e_2 e_3 \ldots \ldots \ldots . e_{k+4} \qquad (4)$$

6) при формировании синдрома ошибки относительно полученных и сформированных значений контрольных разрядов организуются дополнительные диагональные проверки, число которых определяется выражением:

$$R_V = 2(k + 5) \qquad (5)$$

7) в результате имеем множество ошибок заданной кратности (в данном случае от одиночной до кратности k-1, определяемое выражением: $N = \sum_{i=1}^{k-1} C_n^i$), характеризующихся определенными значением синдрома ошибки и дополнительной проверки.

8) множество N разбивается на четыре подмножества $N = n_1 + n_2 + n_3 + n_4$,

где n_1 - синдромы, имеющие совпадения по дополнительным проверкам (некорректируемые ошибки, признак отказа устройства);

n_2-подмножество групп (каждая группа включает 2^k-одинаковых значений синдромов) при наличии ошибок только в информационных разрядах;

n_3-подмножество групп (каждая группа включает 2^k-одинаковых значений синдромов) при наличии ошибок только в контрольных разрядах;

n_4-подмножество групп (каждая группа включает 2^k-одинаковых значений синдромов) при наличии ошибок одновременно в информационных и контрольных разрядах.

Заметим, что для ошибок, не превышающих кратность k-1 нет

ошибочных кодовых наборов, трансформируемых в разрешенные (исправные) кодовые наборы.

Второй подход кодирования полностью включает правила кодирования информации, используемые в первом подходе кодирования, но при этом наряду с контрольными разрядами, сформированными относительно диагональных проверок, передаются контрольные разряды, сформированные относительно проверок на четность столбцов информационной матрицы.

Третий подход основан на следующих правилах кодирования:

1) из прямых инверсных значений информационных разрядов формируется информационная матрица:

$$y_1 \quad y_2 \ldots\ldots\ldots\ldots\ldots y_k$$
$$\overline{y}_1 \quad \overline{y}_2 \ldots\ldots\ldots\ldots\ldots \overline{y}_k$$

2) для полученной информационной матрицы организуются правые и левые диагональные проверки. Число диагональных проверок (число контрольных разрядов) определяется по формуле:

$$R_Д = 2(k+1)$$

3) кодовый набор передается в виде:

$$Y = y_1 y_2 \ldots . y_k \, r_1 r_2 \ldots\ldots\ldots r_{2(k+1)}$$

Процедура получения множеств синдромов ошибок для рассматриваемого кода включает положения, рассмотренные при построении первого и второго методов кодирования.

Четвертая методика кодирования включает следующие положения:

1) из прямых инверсных значений информационных разрядов и полученного значения разряда четности формируется двухстрочная информационная матрица, для каждой строки которой организуется проверка на четность:

$$y_1 y_2 \ldots\ldots\ldots\ldots\ldots y_k r_{ЧЕТ}$$

$$\overline{y}_1 \quad \overline{y}_2 \ldots\ldots\ldots\ldots\ldots \overline{y}_k \overline{r}_{ЧЕТ}$$

2) для полученной информационной матрицы организуются правые и левые диагональные проверки. Число диагональных проверок определяет число контрольных разрядов (контрольные разряды, соответствующие проверкам на четность не передаются). В этом случае число контрольных разрядов определяется по формуле:

$$R_Д = 2(k+2) \quad .$$

3) кодовый набор передается в виде:

$$Y = y_1 y_2 \ldots . y_k \, r_1 r_2 \ldots\ldots\ldots r_{2(k+2)} \; .$$

Пятый и шестой подходы кодирования включают положения, аналогичные третьему подходу кодирования, но при этом в пятом подходе дополнительно к контрольным разрядам, сформированным относительно диагональных проверок, передается контрольный разряд четности полученный относительно информационных разрядов, а в шестом - дополнительно передаются разряды четности, сформированные относительно прямого и инверсного кодовых наборов.

В таблице 1 представлены результаты исследования корректирующих и обнаруживающих способностей предлагаемых методик кодирования информации (число информационных разрядов – 4, кратность ошибок изменяется от 0 до 3-х).

Таблица 1 - Обобщенная характеристика предлагаемых подходов

Контролируемый параметр	**№ варианта**					
	1	**2**	**3**	**4**	**5**	**6**
Количество информационных разрядов	4	4	4	4	4	4
Количество контрольных разрядов	8	10	10	12	13	14
Количество разрядов доп. проверки	18	20	22	26	28	30
% коррекции ошибок	**46**	**75**	**72**	**88**	**90**	**94**
Общее количество ошибок	4784	7520	7520	11152	13344	15808
Количество некорректируемых кодов	16	16	16	16	16	16
Количество совпадающих кодов доп. пр.	2544	1824	2096	1272	1280	960
Количество не совпадающих кодов доп. пр.	2224	5680	5408	9864	12048	14832
Ошибки только в информационных разрядах	224	224	224	224	224	0
Ошибки только в контрольных разрядах	592	2064	2016	4416	5680	7312
Ошибки и в информационных и в контрольных разрядах	1408	3392	3168	5224	6144	7520

Анализ табл. 1 показывает, что из предлагаемых шести подходов кодирования 4-х информационных разрядов, наибольшей обнаруживающей и корректирующей способностью обладает шестой подход (94 % от общего количества возможных ошибок), а наименьшее количество передаваемых контрольных разрядов (8 разрядов) может быть получено при использовании первого подхода.

Аппаратурные затраты, вводимые для обеспечения отказоустойчивости, выразим через простейшие (двухвходовые) логические элементы. В этом случае сложность одного элемента неравнозначности равна четырем простейшим логическим элементам.

Число диагональных проверок (число контрольных разрядов диагональных проверок) формируется относительно информационных разрядов, дополненных контрольным разрядом на четность определяется по формуле:

$$R_Д = k + 4 \qquad (6)$$

Общие аппаратурные затраты для вычисления значений контрольных разрядов четности информационных разрядов, реализованные на сумматорах по mod 2 составят: $C_{ЧЕТ} = k - 2$.

Аппаратурные затраты кодирующего устройства для вычисления диагональных проверок, относительно информационных разрядов, дополненных контрольным разрядом на четность и выраженные через сумматоры по mod 2 равны:

$$C_{\mathrm{mod}\,2} = k. \tag{7}$$

Тогда аппаратурные затраты кодирующего устройства составят

$C_{КУ\,\mathrm{mod}\,2}\,2k-2$ сумматоров по mod 2. (8)

Аппаратурные затраты кодирующего устройства выраженные через простейшие логические элементы равны:

$$C_{КУ_ь} = 8(k-1). \tag{9}$$

Кроме этого, в состав устройства входит схема вычисления синдрома ошибки (схема поразрядного сравнения), аппаратурные затраты которой оценивается выражением:

$$C_{СИН} = 4R_{Д} = 4(k+4), \tag{10}$$

Аппаратурные затраты регистра памяти, при условии что для записи одного разряда потребуется отдельный триггер, выполненный на четырех двухвходовых логических элементах и два элемента И (соответственно для записи и считывания информации) составят:

$$C_{Рег} = 6R_{Д}M = 6*(k+4)*M, \tag{11}$$

где M - число слов памяти.

Число логических элементов И, разрешающих поступление значений сигналов информационных разрядов на входы кодирующего устройства при записи и считывании информации составит:

$$C_{И1} = 2k. \tag{12}$$

Аппаратурные затраты элемента ИЛИ, обеспечивающего поступление сигналов на вход кодирующего устройства при записи или при считывании информации составят:

$$C_{ИЛИ1} = k. \tag{13}$$

Число логических элементов И, разрешающих поступление значений сигналов контрольных разрядов при вычислении синдрома ошибок составят:

$$C_{ИСИНДР} = k + 4. \tag{14}$$

Аппаратурные затраты дешифратора, определим учитывая что множество ошибок заданной кратности (в данном случае от одиночной до кратности k-1) определяется выражением $N = \sum_{i=1}^{k-1} C_n^i$ и при этом данное множество разбивается на четыре подмножества $N = n_1 + n_2 + n_3 + n_4$,

где n_1 - ошибки, синдромы которых имеют одинаковые дополнительные проверки (некорректируемые ошибки, признак отказа устройства);

n_2 - подмножество ошибок только в информационных разрядах (каждая группа включает 2^k - одинаковых значений синдромов);

n_3 - подмножество ошибок только в контрольных разрядах (каждая группа включает 2^k - одинаковых значений синдромов);

$n4$ - подмножество ошибок одновременно в информационных и контрольных разрядах.

Каждое n_i - подмножество ошибок включает l_j - групп, а каждая группа включает 2^k - одинаковых значений синдромов.

В этом случае группа:

l_1 - число групп синдромов для ошибок только в информационных разрядах;

l_2 - число групп синдромов для ошибок только в контрольных разрядах;

l_3 - число групп синдромов для ошибок, возникающих одновременно в информационных и контрольных разрядах.

Тогда аппаратурные затраты дешифратора составят: $C_{ДЕШ} = 16(l_1 + l_2 + l_3)$ r-разрядных элементов И, или для двухвходовых элементов:

$$C_{ДЕШ} = 16(l_1 + l_2 + l_3)(R_Д - 1) = 16(l_1 + l_2 + l_3)(k + 3). \quad (15)$$

Выходы дешифратора соответствующие синдромам, входящих в n_3, объединим с помощью элемента ИЛИ на n_2 - входов, тогда аппаратурные затраты данного элемента, выраженные через двухвходовые логические элементы, составят:

$$C_{ИЛИ2} = (l_2 - 1). \quad (16)$$

Подмножество групп l_2+l_3 объединим с помощью (l_2+l_3)/2- входовых элементов ИЛИ, для подачи управляющих сигналов, корректирующих соответствующий информационный разряд.

В этом случае аппаратурные затраты данной группы элементов ИЛИ составят:

$$C_{ИЛИ3} = k[(l_1 + l_3)/2 - 1]. \quad (17)$$

Аппаратурные затраты, обеспечивающие формирование сигнала «Отказ», для группы синдромов, принадлежащих подмножеству n_1, включают: r-входовый элемент ИЛИ, (k+1)-входовый элемент ИЛИ, элемент НЕ и двухвходовый элемент И.

При реализации на двухвходовых элементах данные аппаратурные затраты составят:

$$C_{ОТКАЗ} = k + 3 + k + 2 = 2k + 5. \quad (18)$$

Аппаратурные затраты элемента И, разрешающего прохождение управляющих сигналов на корректор составят:

$$C_{И2} = k. \quad (19)$$

Аппаратурные затраты корректора составят: $C_{КОР} = 4л$.

Таким образом, для реализации предлагаемого метода коррекции аппаратурные затраты составят:

$$C_{ОБЩ} = C_{ЧЕТ} + C_{КУ} + C_{СИН} + C_{РЕГ} + C_{И_1} + C_{ИЛИ_1} + C_{ИСИНДР} +$$
$$+ C_{ДЕШ} + C_{ИЛИ2} + C_{ИЛИ3} + C_{ОТКАЗ} + C_{И2} + C_{КОР}$$

или

$$C_{ОБЩ} = 6 * M * (k + 4) + k * [(l_1 + l_3)/2 - 1] + 16 * (k + 3) * (l_1 + l_2 + l_3) + l_2 + 24k + 14 \quad (20)$$

Аппаратурные затраты декодирующего устройства включают затраты на реализацию схемы синдрома ошибок, дешифратора, (k+1) - логических элементов ИЛИ, объединяющих группы выходов дешифратора, логических элементов для формирования сигнала отказ, корректора и логических элементов И, разрешающих прохождение управляющих сигналов на корректор:

$$C_{ДЕК} = C_{СИН} + C_{ДЕШ} + C_{ИЛИ2} + C_{ИЛИ3} + C_{ОТК} + C_{И2},$$

или

$$C_{ДЕК} = 16(l_1 + l_2 + l_3)(k + 3) + k[(l_1 + l_3)/2 - 1] + 7k + 8 + l_2. \quad (21)$$

Сравнительная оценка достоверности функционирования аппаратуры, изложена для случая использования четырех разрядных информационных слов. Однако при увеличении разрядности информационных слов картина может измениться (рис.2).

В случае использования восьми разрядной аппаратуры существует два подхода к выбору лучшего метода:

1) Применение одного из предлагаемых методов для целого восьми разрядного слова;

2) Применение одного из предлагаемых методов для каждой половины восьмиразрядного слова (два по четыре).

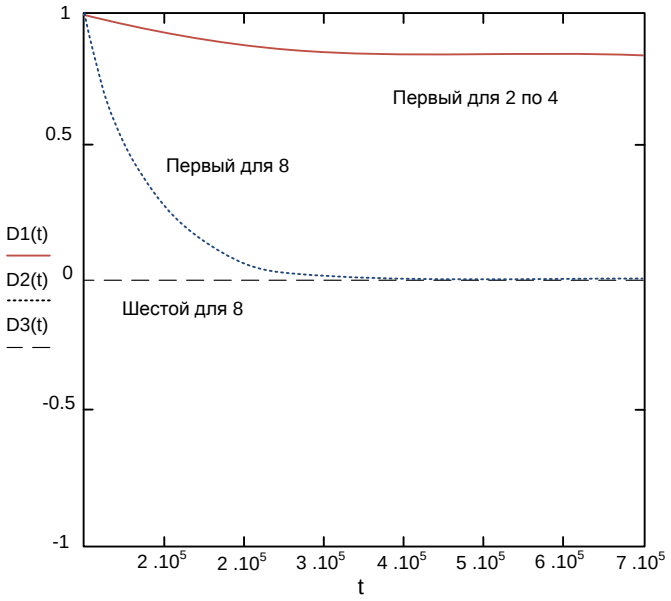

Рис. 2. Сравнительная оценка достоверности функционирования предлагаемых методик кодирования для восьми разрядного слова

Проведенный выше анализ показывает, что лучшую достоверность функционирования дает первый из предлагаемых методов. Поэтому он и был выбран для сравнения с существующими (применяемыми на практике) в настоящее время методами (рис. 3).

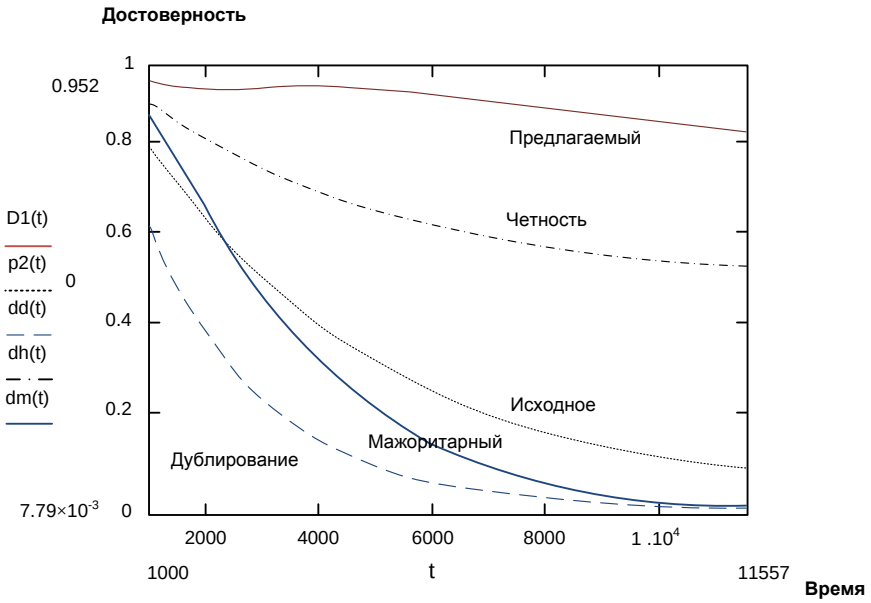

Рис. 3. Сравнительная оценка достоверности функционирования предлагаемой методики резервирования с существующими методами

На основе приведенных алгоритмов кодирования и декодирования информации разработана программная модель защиты ПЗУ от ошибок.

Алгоритм программной модели представлен на рис.4.Вариант №1.

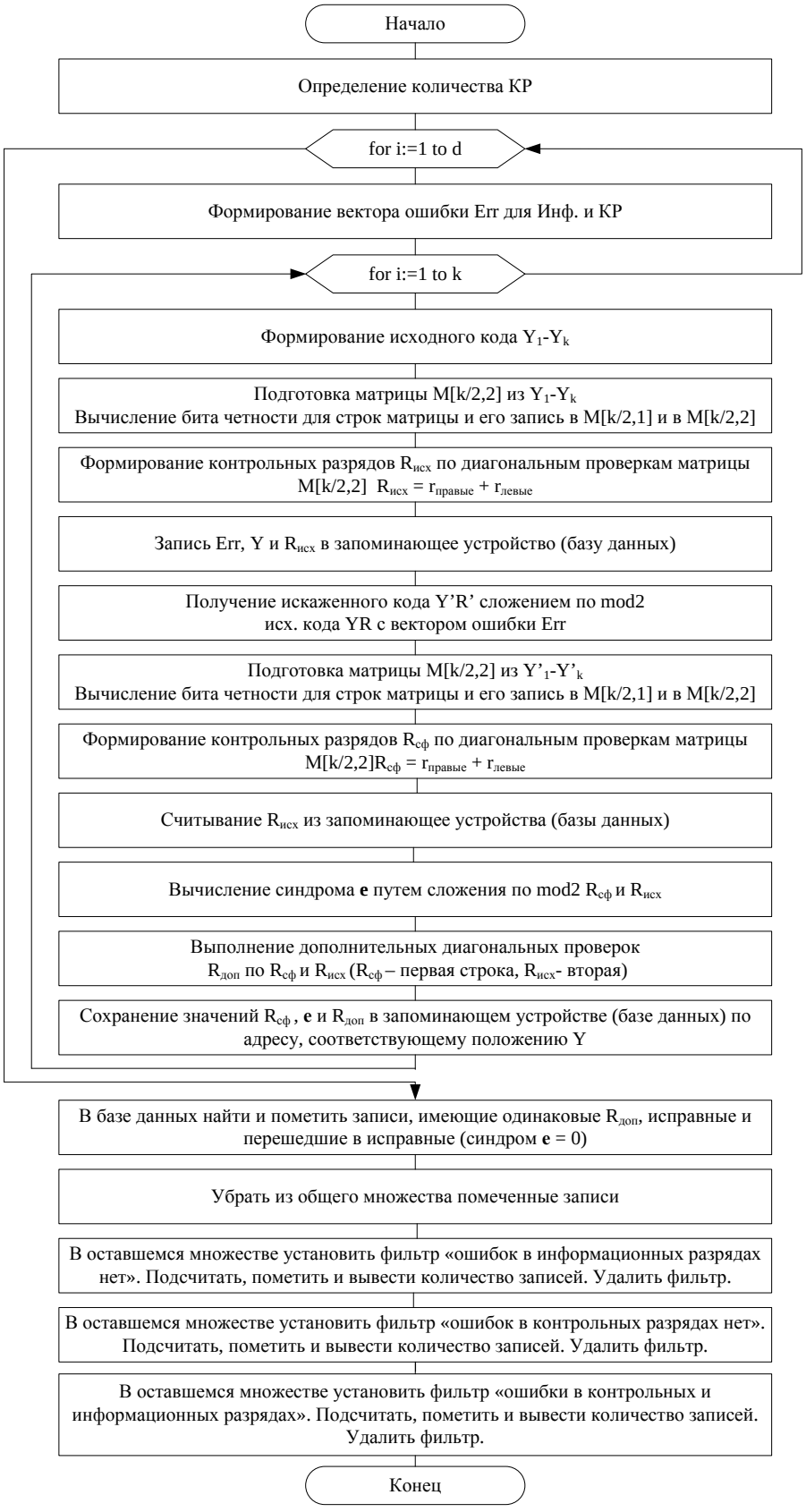

Рис. 4. Алгоритм функционирования программной модели предлагаемого метода кодирования

Существенным отличием построения предлагаемых модифицированных итеративных кодов от известных является организация дополнительных диагональных проверок при вычислении синдрома ошибки, относительно двух строчной матрицы построенной на основе переданных значений контрольных разрядов и значений контрольных разрядов, сформулированных на основе значений полученных информационных разрядов, что позволило в два раза повысить корректирующие возможности итеративного кода.

Проведены исследования по расчету аппаратурных затрат на реализацию кодирующего и декодирующего устройства при использовании предлагаемых подходов, обоснована кратность исправляемой ошибки.

Установлено, что наименьшие аппаратурные затраты соответствуют модифицированному итеративному коду, исправляющему трехкратные ошибки в полубайте информации при этом, наибольшей обнаруживающей и корректирующей способностью обладает шестой подход (корректирует 94 % от общего количества возможных ошибок) однако, наименьшее количество контрольных разрядов, наименьшие аппаратурные затраты соответствуют модифицированному итеративному коду при использовании первого подхода кодирования, который был принят для обеспечения отказоустойчивости устройств хранения и передачи информации.

Защищать информационную систему имеет смысл только комплексно.

Предлагаемые методики модифицированных итеративных кодов позволяют:

1. корректировать ошибки трехкратные ошибки в полубайте информации (в настоящее время неизвестны эффективные методы построения линейных кодов исправляющих больше двух - кратной ошибки), при условии обнаружения ошибок в остальных разрядах кодового набора, за исключением ошибок трансформируемых в разрешенные кодовые наборы (новое свойство линейного кода - коррекция ошибок заданной кратности при условии обнаружения максимального количества некорректируемых ошибок), при этом обеспечивается возможность:

2. исправлять ошибки различной конфигурации (имеет свойства нелинейного кода);

3. осуществлять коррекцию модульных ошибок при малом числе информационных разрядов, т.е. исключить основной недостаток кода Рида-Соломона (при исправлении ошибки в восьми разрядном модуле информации код Рида-Соломона требует 2040 информационных разрядов - поэтому исключается возможность его использования для обеспечения отказоустойчивости мало разрядных специализированных вычислителей КС);

4. иметь минимальные временные затраты на декодирование (в отличие от кодов Рида-Соломона реализующих процедуру циклического декодирования);

5. исключить влияние неисправного резервного оборудования на работу устройств КС при наличии ошибок в контрольных разрядах и отсутствии ошибок;

6. сигнализировать о неисправности устройства памяти при возникновении некорректируемой ошибки.

Третья глава посвящена разработке функционально-кодовой защиты процессора при выполнении арифметических и логических операций (адаптации предлагаемого модифицированного кода для защиты данных операций).

Для формирования “правильных” значений контрольных разрядов возникает необходимость определения правил формирования поправки к значению контрольных разрядов, полученных в результате выполнения арифметической операции S_{k+}.

Правило формирования поправки, при выполнении операции сложения основано построения матрицы поправок, учитывающих перенос единицы в старший разряд, при наличии единиц в одноименных разрядах.

Выявлены свойства корректирующих кодов, позволяющие сформулировать правила формирования контрольных разрядов для логических операций.

Предложена методика обеспечения отказоустойчивости сумматора на основе корректирующих линейных кодов.

Разработаны подходы к обнаружению и коррекции ошибок арифметических операций функционального ядра КС.

Разработаны функциональные схемы отказоустойчивого процессора повышенной достоверности функционирования с использованием ПЛИС, которые были внедрены и показали хорошие результаты.

Выбран комплекс защиты информации для информационно-телекоммуникационных сетей (ИТС), с учетом исследованных и предложенных методик кодирования.

Обобщенный алгоритм поиска оптимального состава средств защиты (СЗ), противодействующего атаке злоумышленника при реализации его конкретной цели в ИТС приведен на рис.5.

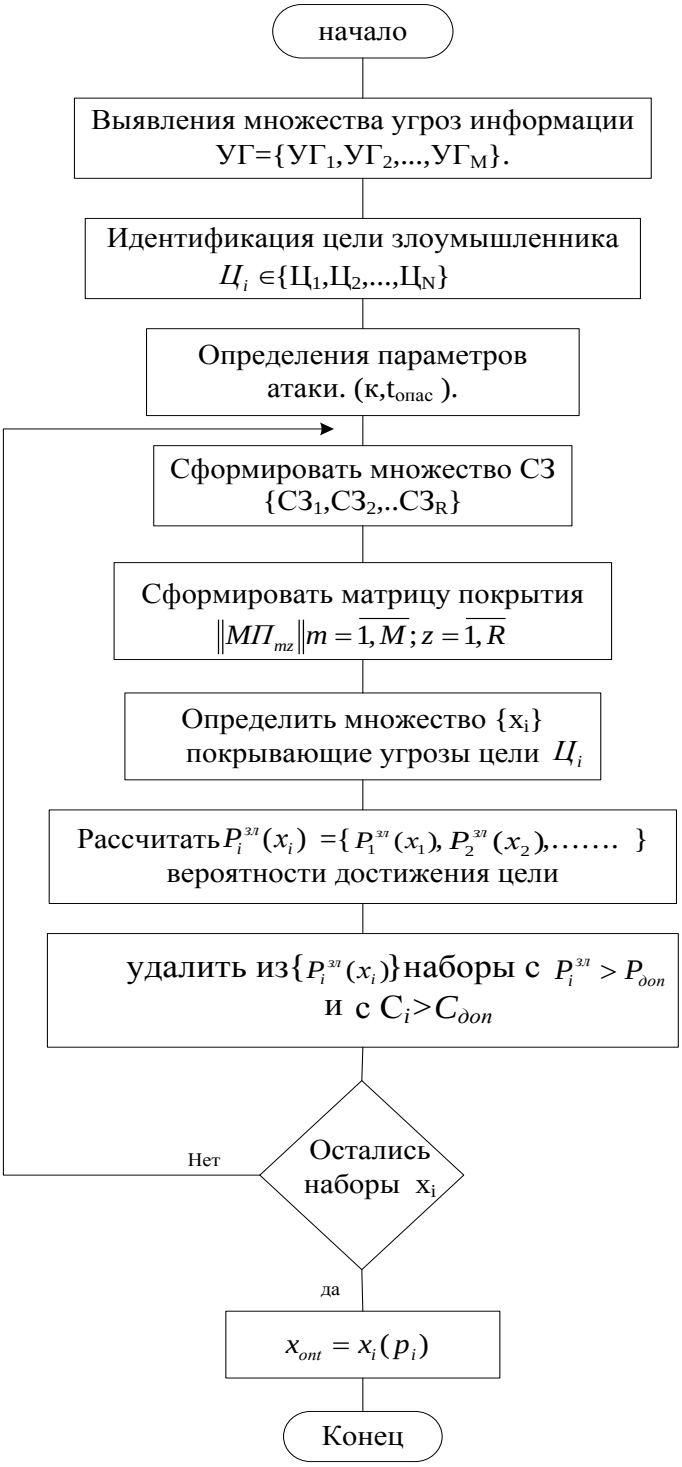

Рис. 5. Схема алгоритма определения состава комплекса средств защиты информации в ИТС

В приложениях разработано функционально–кодовая защита на основе итеративных кодов**;** программная модель функционально-кодовой защиты ПЗУ функционального ядра КСОН, а также акты внедрения.

В заключении подведены итоги работы. Перечислены результаты и выводы.

СПИСОК ПУБЛИКАЦИЙ ПО ТЕМЕ ДИССЕРТАЦИИ

- в изданиях по перечню ВАК:

1. Тахаан Осама. Информационная защита корпоративной сети системой обнаружением атак с нечеткой логикой/Галкин А.П.// Известия института инженерной физики. № 4. 2009.С.3-6.

2. Тахаан Осама. Угрозы информационной безопасности и защита от них для телекоммуникационных сетей радиосистем / Галкин А.П.// Проектирование и технология электронных средств. № 2. 2010. С. 28-30.

3. Тахаан Осама. Выбор комплекса защиты информации для корпоративных информационно-телекоммуникационных сетей/Галкин А.П.// Известия института инженерной физики. № 2. 2010.С. 2-6.

- в других изданиях:

4. Тахаан Осама. Обнаружения атак и нарушений в корпоративной сети / А.П. Галкин, Аль-Муриш Мохаммед // Перспективные технологии в средствах передачи информации. Материалы 8-й Международной НТК. Владимир, 2009. С.184-188.

5. Тахаан Осама. Поэлементная или комплексная информационная защита/ Дерябин А.В., Дерябин В.М.// Перспективные технологии в средствах передачи информации. Материалы 8-й Международной НТК. Владимир, 2009. С.189-192.

6. Тахаан Осама. Финансовая и информационная безопасность и риски при проектировании / А.П. Галкин, Аль-Муриш Мохаммед, Е.Г.Суслова// Экономические проблемы ресурсного обеспечения инновационного развития региона. Материалы международной НК. Владимир,2009. С.112-118.

7. Тахаан Осама. Кризис, безработица и информационная безопасность предприятия / А.П. Галкин, Аркадьева М.С., Суслова Е.Г. // Экономические проблемы ресурсного обеспечения инновационного развития региона. Материалы международной НК. Владимир,2009. С.119-122.

8. Тахаан Осама. Улучшение экономических характеристик при повышении отказоустойчивости транспортного уровня вычислительных сетей/ А.П. Галкин, Кирсенко И.Н., Ахмед Бадван //Факторы развития региональных рынков. Материалы межд.НПК. Владимир, 2011. С.23-26.

9. Тахаан Осама. Защита от угроз информационной безопасности в телекоммуникационных сетях / Галкин А.П., Ахмед Бадван // Перспективные технологии в средствах передачи информации. Материалы 9-й Международной НТК. Владимир, 2011. С.42-45.

10. Тахаан Осама. Повышение отказоустойчивости транспортного уровня вычислительных сетей путём реорганизации сквозной «точка-точка» множественной адресации / Галкин А.П. // Перспективные технологии в средствах передачи информации. Материалы 9-й Международной НТК. Владимир, 2011. С.123-125.

11. Тахаан Осама. Повышение эффективности сложных РЭС. (Г/Б НИР) № 118 / Каф. РТиРС // ВлГУ, 2009-2010 гг.

Подписано в печать 11.01.12.
Формат 60×84/16. Усл. печ. л. 1,16. Тираж 100.
Заказ
Издательство
Владимирского государственного университета
имени Александра Григорьевича и Николая Григорьевича Столетовых
600000, Владимир, ул. Горького, 87.