

На правах рукописи

О В Е Ч К И Н Павел Владимирович

**РАЗРАБОТКА АЛГОРИТМОВ ПОВЫШЕНИЯ ЭФФЕКТИВНОСТИ  
НЕДВОИЧНЫХ МНОГОПороГОВЫХ ДЕКОДЕРОВ В СИСТЕМАХ  
ПЕРЕДАЧИ И ХРАНЕНИЯ БОЛЬШИХ ОБЪЕМОВ ИНФОРМАЦИИ**

Специальность 05.13.13 – «Телекоммуникационные системы  
и компьютерные сети»

**АВТОРЕФЕРАТ**

диссертации на соискание ученой степени  
кандидата технических наук

Рязань 2009

Работа выполнена в ГОУВПО «Рязанский государственный радиотехнический университет».

Научный руководитель: доктор технических наук, профессор  
**Золотарёв Валерий Владимирович**

Официальные оппоненты: доктор физико-математических наук  
**Назаров Лев Евгеньевич**

кандидат технических наук, доцент  
**Гаврилов Александр Николаевич**

Ведущая организация: **ФГУП «Научно-исследовательский институт радио»**

Защита диссертации состоится **«23» июня 2009 г. в 13 часов** на заседании диссертационного совета Д 212.211.02 в ГОУВПО «Рязанский государственный радиотехнический университет» по адресу: **390005, г. Рязань, ул. Гагарина, 59/1.**

С диссертацией можно ознакомиться в библиотеке ГОУВПО «Рязанский государственный радиотехнический университет».

Автореферат разослан **«21» мая 2009 г.**

Ученый секретарь  
диссертационного совета Д 212.211.02  
к.т.н., доцент

**И.А. Телков**

## ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

**Актуальность темы.** К современным системам передачи цифровых данных предъявляются очень жесткие требования по безошибочности передачи информации. Для обеспечения таких требований используют методы помехоустойчивого кодирования, применение которых позволяет улучшать многие важные характеристики систем передачи данных, например, экономить мощность передатчика, увеличивать дальность связи, уменьшать размеры антенн и др. Немаловажную роль помехоустойчивые коды играют и в системах хранения данных, в которых необходимо обеспечивать высокую надежность долговременного хранения информации на носителе. В связи с этим чрезвычайно актуальной является задача разработки эффективных методов коррекции ошибок, на решение которой направлены усилия многих специалистов во всем мире.

Огромный вклад в развитие теории кодирования внесли такие ученые, как К. Шеннон, В.А. Котельников, В.В. Зяблов, К.Ш. Зигангиров, В.В. Золотарёв, А. Витерби, Дж. Месси, Р. Галлагер, Д. Форни, Л.М. Финк, В.Л. Банкет, Дж. Возенкрафт, Е. Берлекэмп, Э.Л. Блох и др.

В настоящее время специалисты в области помехоустойчивого кодирования проявляют большой интерес к недвоичным кодам, работающим с цифровыми данными на уровне символов, например, с байтами информации. Недвоичные коды применяются в каналах с группирующимися ошибками, в качестве составляющих элементов различных каскадных кодов, для защиты от ошибок информации на различного рода носителях (CD, DVD, Blu-ray и др.).

Анализ недвоичных корректирующих кодов и алгоритмов их декодирования показал, что широкое применение в реальных системах передачи и хранения информации из недвоичных кодов нашли только коды Рида-Соломона. Однако декодеры коротких кодов Рида-Соломона, которые и применяются на практике, не могут обеспечить высокую эффективность декодирования, а для длинных кодов Рида-Соломона невозможно создать декодер из-за высокой сложности его реализации. Поэтому задача реализации простых и одновременно эффективных алгоритмов кодирования/декодирования для недвоичных кодов, гораздо более длинных, чем коды Рида-Соломона, остается чрезвычайно актуальной.

Среди других методов коррекции ошибок наиболее перспективным является метод недвоичного многопорогового декодирования, предложенный В.В. Золотарёвым. Отличительными особенностями данного метода являются линейная сложность реализации и высокая эффективность декодирования. Поэтому недвоичный многопороговый декодер ( $q$ МПД) может применяться в высокоскоростных системах передачи и хранения больших объемов информации.

Однако в соответствии с теорией кодирования характеристики недвоичного многопорогового декодера все еще достаточно удалены от границы Шеннона, определяющей потенциальные корректирующие возможности кода. Кроме того, на данный момент еще не исследованы возможности недвоичного многопорогового декодера в каналах с пакетирующимися ошибками, в каналах со стираниями и в каналах со стираниями и искажениями.

**Целью диссертационной работы** является разработка и исследование алгоритмов, применение которых позволит повысить эффективность работы недвоичного многопорогового декодера.

Для достижения поставленной цели необходимо решить следующие задачи:

- провести анализ наиболее известных и важных методов декодирования помехоустойчивых кодов, которые применяются в системах передачи и хранения информации, с целью выбора направлений дальнейшего исследования;

- разработать и исследовать алгоритмы построения наиболее эффективных недвоичных самоортогональных кодов (СОК) для  $q$ МПД, использование которых позволит повысить достоверность передачи и хранения информации;

- провести исследование работы недвоичных многопороговых декодеров в каналах с пакетирующимися ошибками, в каналах со стираниями и в каналах со стираниями и искажениями;

- разработать и исследовать каскадные схемы коррекции ошибок на основе  $q$ МПД, позволяющие уменьшить вероятность ошибки декодирования по сравнению с базовым некаскадным методом;

- разработать программные средства для исследования эффективности  $q$ МПД;

- разработать программные средства для защиты файлов от искажений.

**Научная новизна** диссертационной работы определяется тем, что в ней предложены и исследованы алгоритмы построения недвоичных самоортогональных кодов, существенно повышающие эффективность использования  $q$ МПД. Впервые проведено исследование работы  $q$ МПД в каналах Гилберта-Эллиота с пакетирующимися ошибками, в каналах со стираниями и в каналах со стираниями и искажениями, оптимизированы параметры  $q$ МПД для работы в таких условиях. Кроме того, были получены нижние оценки вероятности ошибки оптимального декодирования недвоичных самоортогональных кодов в каналах со стираниями и искажениями. Предложен новый алгоритм работы недвоичного порогового элемента, позволяющий существенно ускорить работу недвоичного многопорогового декодера. Доказана теорема о стремлении решения декодера каскадного кода, состоящего из недвоичного самоортогонального кода и кода контроля

по модулю  $q$ , к решению оптимального декодера. В работе впервые предложено каскадирование  $q$ МПД с кодеком модифицированных недвоичных кодов Хэмминга.

**Основные положения, выносимые на защиту:**

- алгоритм построения эффективных недвоичных самоортогональных кодов для  $q$ МПД;
- алгоритм работы недвоичного порогового элемента, позволяющий значительно ускорить работу  $q$ МПД;
- доказательство теоремы о стремлении решения декодера каскадного кода, состоящего из недвоичного СОК и кода контроля по модулю  $q$ , к решению оптимального декодера;
- каскадная схема кодирования, состоящая из недвоичного самоортогонального кода и модифицированного недвоичного кода Хэмминга.

**Практическая ценность работы.** Разработанный алгоритм построения недвоичных самоортогональных кодов для схем параллельного кодирования позволяет приблизить область эффективной работы  $q$ МПД к пропускной способности канала более чем на 13%. Предложенный алгоритм работы недвоичного порогового элемента позволяет повысить быстродействие недвоичного многопорогового декодера более чем в 2 раза. Разработанная каскадная схема на базе недвоичного самоортогонального кода и модифицированного недвоичного кода Хэмминга позволяет уменьшить частоту появления ошибок на выходе  $q$ МПД в области его эффективной работы более чем на 3 порядка. Программные средства на основе недвоичного многопорогового декодера для защиты файлов от искажений при длительном хранении информации позволяют ускорить процессы кодирования и восстановления информации в десятки раз по сравнению с известными программами-аналогами при сопоставимой эффективности восстановления данных.

**Внедрение результатов работы.** Результаты диссертационной работы были использованы: ООО «Объединенные радиоэлектронные технологии» при разработке аппаратуры передачи информации, предназначенной для работы в условиях городской застройки; Институтом космических исследований Российской академии наук при разработке исходных данных на наземный комплекс приема, обработки и распределения данных КНА «Фобос-Грунт»; разработанные программные средства моделирования недвоичного многопорогового алгоритма декодирования и его модификаций используются в учебном процессе Рязанского государственного радиотехнического университета, что подтверждается актами о внедрении.

**Достоверность** полученных в диссертационной работе результатов подтверждается:

- корректным использованием теории вероятностей и математической статистики;

– результатами компьютерных экспериментов, полученными при статистическом моделировании известных и новых алгоритмов кодирования и декодирования помехоустойчивых кодов, совпадающих с теоретическими оценками;

– внедрением результатов диссертации в ряде организаций, подтверждаемым соответствующими актами.

**Апробация работы.** Результаты работы докладывались на следующих конференциях и семинарах:

1. 11-я, 13-я, 14-я и 15-я международная научно-техническая конференция «Проблемы передачи и обработки информации в сетях и системах телекоммуникаций». – 2002 г., 2004 г., 2005 г., 2008 г., Рязань.

2. Всероссийская научно-техническая конференция «Новые информационные технологии в научных исследованиях и в образовании, НИТ». – 2003 г., 2005 г., 2006 г., Рязань.

3. Межвузовская научно-техническая конференция студентов, молодых ученых и специалистов «Новые информационные технологии в учебном процессе и производстве». – 2004 г., Рязань.

4. 52-я студенческая научно-техническая конференция «Математическое и программное обеспечение вычислительных систем». – 2005 г., Рязань.

5. Научно-практическая конференция «Научные исследования и их практическое применение. Современное состояние и пути развития», 2005 г., Одесса.

6. Всероссийский смотр-конкурс научно-технического творчества «Эврика-2005». – 2005 г., Новочеркасск.

7. 8-я, 9-я, 10-я, 11-я международная конференция и выставка «Цифровая обработка сигналов и ее применение». – 2006 г., 2007 г., 2008 г., 2009 г., Москва.

8. Межвузовская научно-методическая конференция «Методы организации учебного процесса в ВУЗе» – 2007 г., Рязань.

9. 5-я и 6-я конференция молодых ученых, посвященная Дню космонавтики «Фундаментальные и прикладные космические исследования». – 2008 г., 2009 г., Москва.

**Публикации.** По теме диссертации опубликовано 26 работ, из них 18 в соавторстве. В их числе 1 статья в журналах, рецензируемых ВАК, 4 статьи в межвузовских сборниках научных трудов, 20 тезисов докладов на международных и всероссийских конференциях. Разработан и зарегистрирован в Российском агентстве по патентам и товарным знакам 1 пакет программ.

**Структура и объем диссертации.** Диссертационная работа состоит из введения, четырех глав, заключения, библиографического списка и двух приложений. Содержит 131 страницу, 3 таблицы, 57 рисунков. Библиографический список состоит из 86 наименований.

## СОДЕРЖАНИЕ РАБОТЫ

**Во введении** обоснована актуальность темы диссертации, определены цель и задачи исследований, представлены основные положения диссертационной работы, выносимые на защиту.

**В первой главе** «Анализ современных методов помехоустойчивого кодирования. Выбор направлений исследования» изложены основные принципы помехоустойчивого кодирования, рассмотрены возможности наиболее распространенных на сегодняшний день алгоритмов декодирования недвоичных помехоустойчивых кодов, оценена сложность их реализации, описаны схемы коррекции ошибок, которые применяются в системах хранения информации.

В цифровых системах передачи и хранения информации обычно удобнее работать не с отдельными битами информации, а с целыми символами, например, одним или несколькими байтами. В этом случае для исправления ошибок целесообразно применять недвоичные коды. Дополнительным преимуществом таких кодов является то, что они эффективны для исправления пакетов ошибок, часто возникающих при передаче и хранении информации.

Наиболее широкое применение в реальных системах передачи и хранения информации из недвоичных кодов нашли коды Рида-Соломона (РС). Замечательным свойством данных кодов является то, что с их помощью всегда возможно исправление  $\lfloor t/2 \rfloor$  ошибок или  $t$  стираний ( $\lfloor x \rfloor$  – операция взятия целой части числа  $x$ ,  $t$  – число проверочных символов кода), т.е. коды РС позволяют добавлять минимальное число избыточных символов для исправления любой конфигурации ошибок заданного веса. Однако декодеры коротких кодов Рида-Соломона, которые и применяются на практике, не могут обеспечить высокую эффективность декодирования, а для длинных кодов РС невозможно создать декодер из-за высокой сложности его реализации. Отметим, что вычислительная сложность декодирования кодов Рида-Соломона достаточно велика и пропорциональна квадрату длины кода.

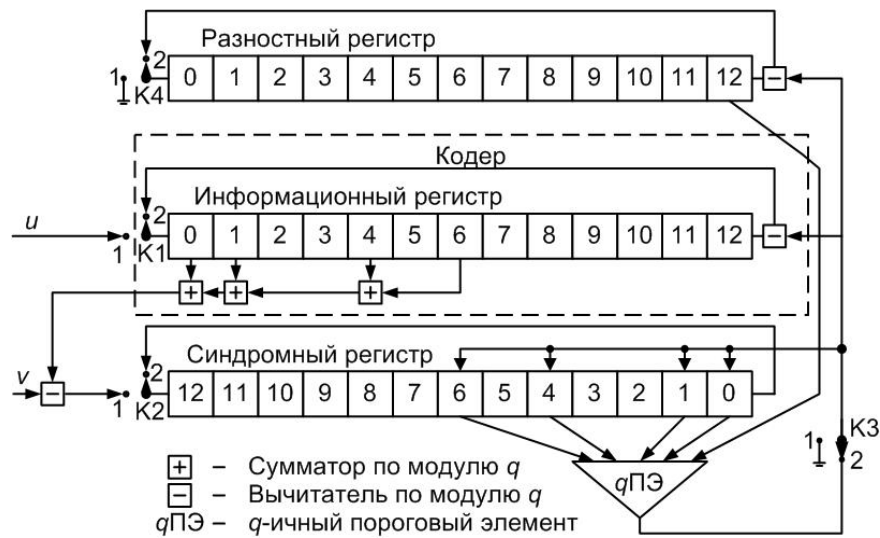
Сравнительно недавно появились недвоичные низкоплотностные коды и недвоичные турбо коды. Данные коды, безусловно, обладают высокой эффективностью, но из-за высокой сложности реализации в настоящее время на практике не применяются. Отметим, что вычислительная сложность декодирования большинства недвоичных кодов зависит от размера  $q$  алфавита используемых символов. Поэтому в реальных системах передачи и хранения информации встречаются только коды, работающие с символами размером не более одного байта ( $q \leq 256$ ).

Наиболее перспективным методом коррекции ошибок является метод недвоичного многопорогового декодирования. Ценность  $q$ МПД за-

ключается в том, что он обладает свойством стремления к решению оптимального декодера при сохранении линейной от длины кода сложности реализации. Также для  $q$ МПД не существует ограничений на размер символа, и он одинаково быстро может производить действия как над однобайтовыми символами, так и над символами, состоящими из нескольких байт. Однако в соответствии с теорией кодирования характеристики  $q$ МПД достаточно удалены от границы Шеннона, определяющей потенциальные корректирующие возможности кода. Дополнительному улучшению характеристик этого простого и эффективного метода и посвящена представленная работа.

**Во второй главе** «Исследование недвоичного многопорогового декодера» рассмотрен недвоичный многопороговый алгоритм декодирования, описаны модификации  $q$ МПД для его использования в каналах со стираниями и в каналах со стираниями и искажениями, получены экспериментальные характеристики  $q$ МПД в каналах Гилберта-Эллиота с пакутирующимися ошибками, в каналах со стираниями и в каналах со стираниями и искажениями.

Недвоичный многопороговый декодер ( $q$ МПД) является простейшим декодером мажоритарного типа.  $q$ МПД используется для декодирования недвоичных самоортогональных кодов (СОК). Пример схемы  $q$ МПД блочного недвоичного СОК, заданного образующим полиномом  $g(x) = 1 + x + x^4 + x^6$ , представлен на рисунке 1.



**Рисунок 1** – Пример схемы  $q$ МПД блочного недвоичного СОК

Процедура декодирования  $q$ МПД заключается в том, что для очередного контролируемого недвоичным пороговым элементом ( $q$ ПЭ) информационного символа кода  $u_j$  происходит подсчет количества и определение значений двух относящихся к нему наиболее часто встречающихся проверок кода, например,  $b_1$  и  $b_2$ , причем  $b_1$  встречается  $m_1$  раз,  $b_2$  –  $m_2$  раз ( $m_1 \geq m_2$ ), а остальные значения проверок для декодируемого символа  $u_j$  встречаются не более  $m_2$  раз. Если разница  $m_1 - m_2$  будет больше значения порога  $T$ , то на



выходе  $q$ ПЭ будет значение  $b_1$ , которое вычитается из соответствующих элементов синдромного регистра, из текущего элемента информационного регистра и заносится в связанный с информационным элемент разностного регистра. Если окажется, что два наиболее часто встречающихся значения проверок таковы, что  $m_1=m_2$ , то выход  $q$ ПЭ устанавливается равным нулю, т. е. символ  $u_j$  не изменяется, и делается попытка декодирования любого другого информационного символа кода.

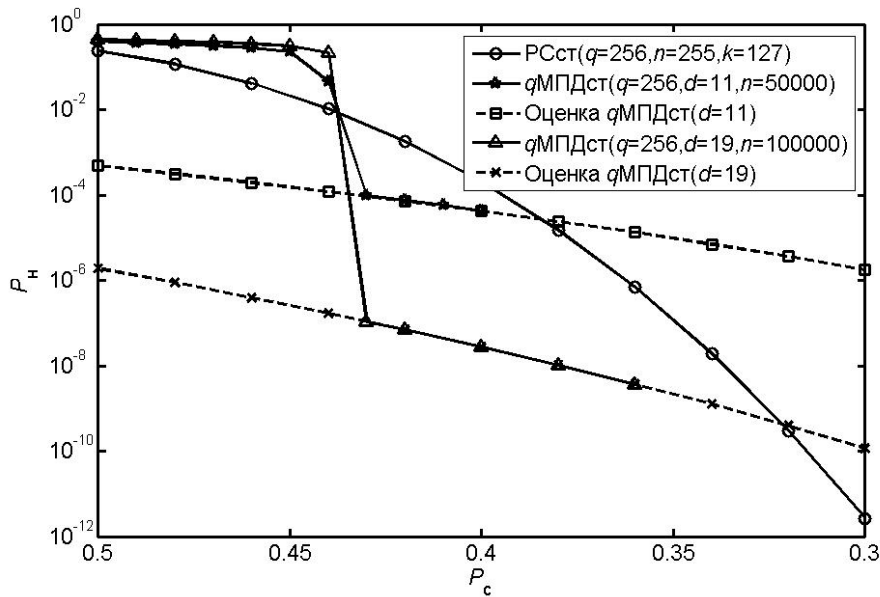
До настоящего времени были известны характеристики  $q$ МПД только для  $q$ -ичных симметричных каналов ( $q$ СК), где ошибки появлялись независимо друг от друга с равной вероятностью. Однако часто в реальных системах передачи и хранения информации возникают пакеты ошибок, которые обычно существенно ухудшают эффективность классических методов коррекции ошибок. Для описания таких каналов подходит модель канала Гилберта-Эллиота. Поэтому в диссертационной работе были проведены исследования эффективности  $q$ МПД в этих более сложных условиях. Результаты такого исследования показали, что  $q$ МПД для кода с кодовой скоростью  $R=1/2$ , минимальным кодовым расстоянием  $d=17$ , длиной  $n=32000$  однобайтовых символов (размер алфавита  $q=256$ ) эффективно исправляет около 25% ошибок в данном канале, а декодер кодов Рида-Соломона длиной 255 однобайтовых символов – только 1% ошибок.

Типичными представителями каналов с пакетирующимися ошибками являются системы хранения данных. Например, для защиты информации, находящейся на DVD дисках, используются коды произведения Рида-Соломона с  $R=7/8$  и общей длиной  $n \approx 38000$ . Во второй главе диссертации были подобраны недвоичные СОК с аналогичными параметрами, обладающие существенно лучшими корректирующими способностями.

Часто в системах передачи и хранения данных для дополнительного повышения эффективности декодирования ненадежные символы отмечаются как стертые. В дальнейшем восстановить стертые символы оказывается значительно проще, чем исправлять ошибки.

Работа  $q$ МПД в таком канале отличается от работы в  $q$ -ичном симметричном канале тем, что при вычислении символов синдрома стертые информационные и проверочные символы на значение проверок не влияют, но при этом для каждой проверки запоминается число участвующих в его формировании стираний. Затем в процессе декодирования стертого информационного символа среди относящихся к нему проверок ищется проверка, содержащая только одно стирание. Очевидно, что это стирание вызвано декодируемым информационным символом, который по значению данной проверки может быть легко восстановлен.

На рисунке 2 представлены зависимости вероятности невозможности восстановления символа на выходе декодера от вероятности стирания в канале. Здесь показаны характеристики декодера кодов РС и  $q$ МПД для кодов с  $R=1/2$ . Из рисунка видно, что эффективность  $q$ МПД при существенно



**Рисунок 2 – Характеристики  $q$ МПД и декодера кодов РС в каналах со стираниями**

меньшей сложности реализации превосходит эффективность практически реализуемого декодера кодов РС длиной 255 однобайтовых символов.

Также в диссертационной работе были проведены исследования возможности использования  $q$ МПД в каналах со стираниями и искажениями, в которых, в отличие от каналов со стираниями, возможно появление ошибочных символов. Канал со стираниями и искажениями характеризуется тем, что символы по нему передаются правильно с вероятностью  $1-P_c-P_0$ , «стираются» с вероятностью  $P_c$  и искажаются с вероятностью  $P_0$ .

При работе в таком канале  $q$ МПД на каждой итерации декодирования должен уметь исправлять как стирания, так и ошибки. Процедура исправления ошибок в этом случае полностью аналогична исправлению ошибок для  $q$ СК, а при декодировании стираний решение о значении восстанавливаемого символа по одной проверке вынести уже нельзя, поскольку проверка может быть ошибочной из-за возможных искажений в канале. Поэтому при декодировании стертого символа сначала среди проверок относительно данного символа ищутся все проверки, содержащие только по одному стиранию. Затем по каждой из них определяется значение стертого символа, после чего принимается окончательное решение о значении декодируемого символа по большинству голосов.

Также во второй главе оценена нижняя граница вероятности ошибки декодирования для рассматриваемого  $q$ МПД в таком канале. Для этого были выписаны наиболее частые события, которые всегда приводят к ошибкам оптимального декодера не двоичных СОК, и определены вероятности появления этих событий:

1. Все проверочные символы и информационный символ стерты:

$$P_1 = P_c^d .$$

2. Информационный символ стерт, один проверочный символ принят правильно, один проверочный символ ошибочен, остальные проверочные символы стерты:

$$P_2 = P_0 \cdot (1 - P_c - P_0) \cdot P_c^{d-2} \cdot (d-1) \cdot (d-2).$$

3. Информационный символ ошибочен, один проверочный символ принят правильно, остальные проверочные символы стерты:

$$P_3 = P_0 \cdot (1 - P_c - P_0) \cdot P_c^{d-2} \cdot (d-1)$$

4. Информационный символ стерт, один проверочный символ ошибочен, остальные проверочные символы стерты:

$$P_4 = P_0 \cdot P_c^{d-1} \cdot (d-1).$$

5. Информационный символ стерт, два проверочных символа ошибочны, один проверочный символ принят правильно, остальные проверочные символы стерты:

$$P_5 = P_0^2 \cdot (1 - P_c - P_0) \cdot P_c^{d-3} \cdot \frac{(d-1) \cdot (d-2) \cdot (d-3)}{2}.$$

Нижняя оценка вероятности символьной ошибки оптимального декодирования определяется суммой найденных выше вероятностей:

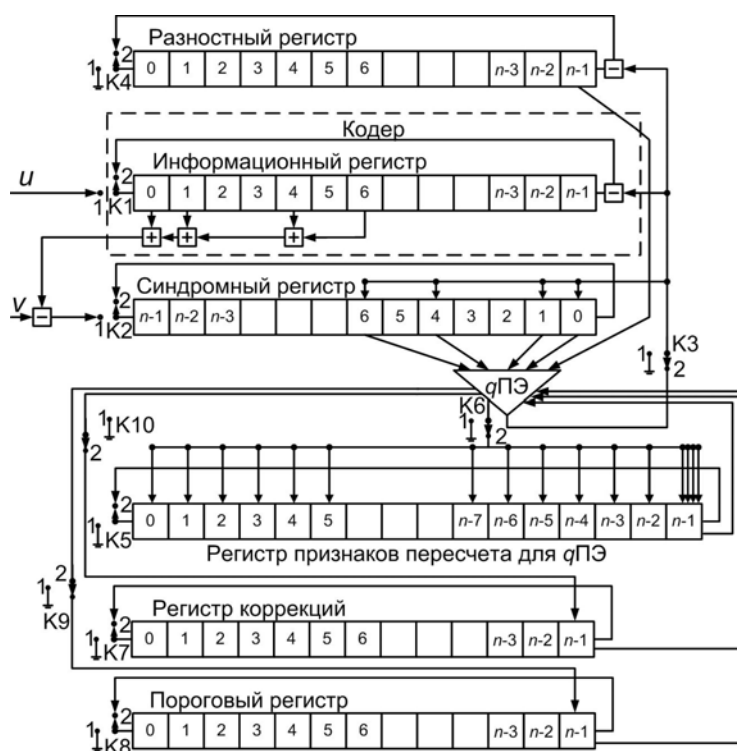
$$P_s = \sum_{i=1}^5 P_i.$$

Данная оценка оказывается достаточно точной для предварительного оценивания характеристик  $q$ МПД, способного исправлять ошибки и восстанавливать стирания.

Результаты исследования возможности использования  $q$ МПД в каналах со стираниями и искажениями показали, что характеристики  $q$ МПД в области его эффективной работы сопоставимы с характеристиками декодера кодов Рида-Соломона. Подчеркнем, что при этом  $q$ МПД оказывается более чем в 30 раз проще для практической реализации.

**В третьей главе** «Алгоритмы улучшения характеристик  $q$ МПД» приводятся алгоритмы, применение которых позволяет ускорить работу и повысить эффективность декодирования  $q$ МПД; разработаны каскадные схемы коррекции ошибок на базе  $q$ МПД, позволяющие улучшить характеристики  $q$ МПД в области его эффективной работы.

Несмотря на то, что скорость работы  $q$ МПД во много раз превосходит скорость работы других недвоичных декодеров, существует возможность дополнительного ускорения работы  $q$ МПД. Среди элементов  $q$ МПД наибольшую сложность имеет недвоичный пороговый элемент ( $q$ ПЭ). В результате проведенного анализа был предложен новый алгоритм работы  $q$ ПЭ, позволяющий существенно ускорить  $q$ МПД. Схема  $q$ МПД, использующего модифицированный  $q$ ПЭ, представлена на рисунке 3. Отметим, что в эту схему вводится дополнительный регистр, элементы которого показывают, нужно ли заново обрабатывать информацию, поступающую на



**Рисунок 3 – Модифицированный  $q$ МПД не двоичного СОК**

пороговый элемент с синдромного и разностного регистров. При этом, так как на различных итерациях может измениться значение порога  $qПЭ$ , необходимо запоминать значение разности  $m_1 - m_2$  и значение  $b_1$  наиболее популярной проверки, которое используется при срабатывании  $qПЭ$ .

Процедура декодирования принятого сообщения модифицированным  $q$ МПД состоит в следующем:

1. Произвольно выбирается декодируемый информационный символ  $u_j$  принятого сообщения.

2. Если элемент регистра признаков пересчета, соответствующий информационному символу  $u_j$ , равен 1, то подсчитывается число двух наиболее часто встречающихся проверок. Значения этих двух проверок равны  $b_1$  и  $b_2$ , а их количество равно  $m_1$  и  $m_2$  соответственно, причем  $m_1 \geq m_2$ . Если элемент регистра признаков пересчета равен 0, то значение разности  $m_1 - m_2$  устанавливается равным значению текущего элемента порогового регистра, а значение  $b_1$  – значению текущего элемента регистра коррекций.

3. Если  $m_1 - m_2 \leq T$ , то устанавливается в 0 значение элемента регистра признаков пересчета, соответствующего информационному символу  $u_j$ , в текущий элемент порогового регистра заносится разность  $m_1 - m_2$ , в текущий элемент регистра коррекций – значение  $b_1$ . Если  $m_1 - m_2 > T$ , то из  $u_j$ ,  $d_j$  и всех проверок относительно  $u_j$  вычитается оценка ошибки, равная  $b_1$ . Также устанавливаются в 1 все элементы регистра признаков, соответствующие информационным символам которых участвовали в формировании измененных символов синдромного регистра.

4. Осуществляется переход к новому  $u_m$ ,  $m \neq j$  и далее переход к п. 2.

Для большего выигрыша по объему операций данную модификацию  $q$ МПД в некоторых случаях следует применять после нескольких обычных итераций декодирования. Использование предложенного алгоритма позволяет в 2-3 раза ускорить работу  $q$ МПД, при этом эффективность декодирования по сравнению с обычным  $q$ МПД остается без изменений.

Для того чтобы  $q$ МПД показывал высокую эффективность, необходимо уделить большое внимание выбору используемых кодов. Как известно, лучшими недвоичными СОК являются коды с параллельным кодированием с несколькими информационными и проверочными ветвями. При этом чрезвычайно трудоемкой задачей является определение количества символов информационной ветви, участвующих в формировании символов каждой проверочной ветви. Для решения этой задачи был предложен алгоритм, позволяющий строить наиболее эффективные самоортогональные коды для схем параллельного кодирования. На рисунке 4 представлена схема данного алгоритма.

Здесь  $poly[][][]$  – полином, определяющий недвоичный СОК;  $poly[i][j][0]$  – определяет количество символов  $i$ -й информационной ветви, участвующих в формировании символов  $j$ -й проверочной ветви;  $min[i][j]$  – минимальное количество символов  $i$ -й информационной ветви, участвующих в формировании символов  $j$ -й проверочной ветви;  $max[i][j]$  – макси-

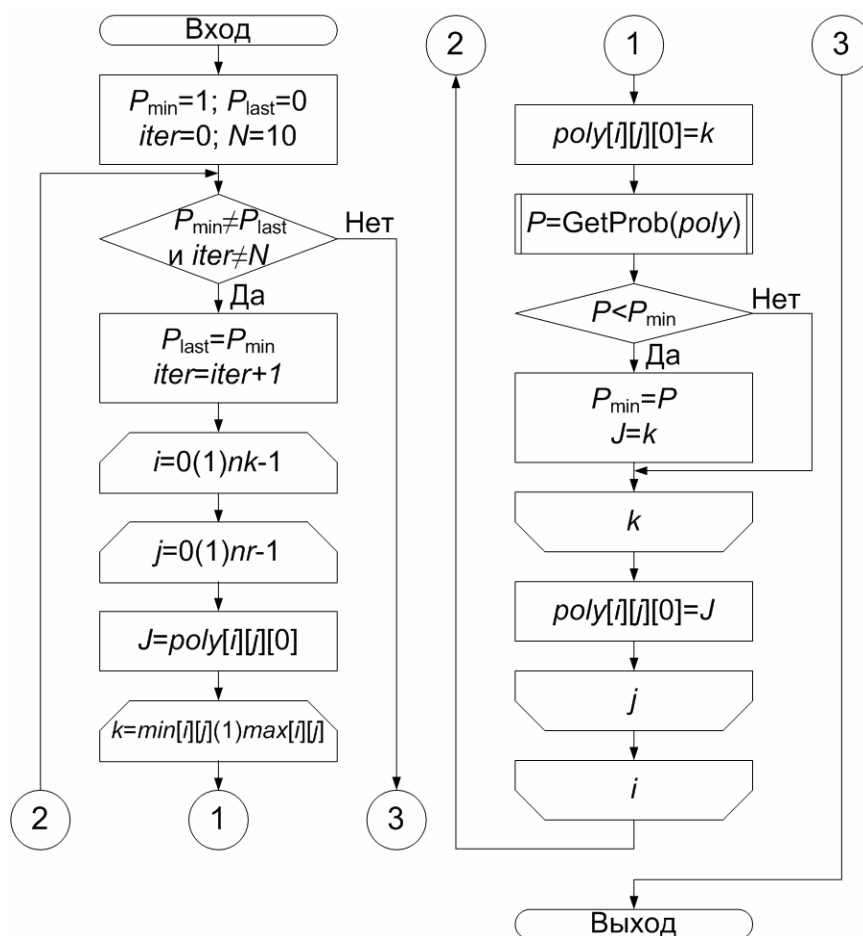
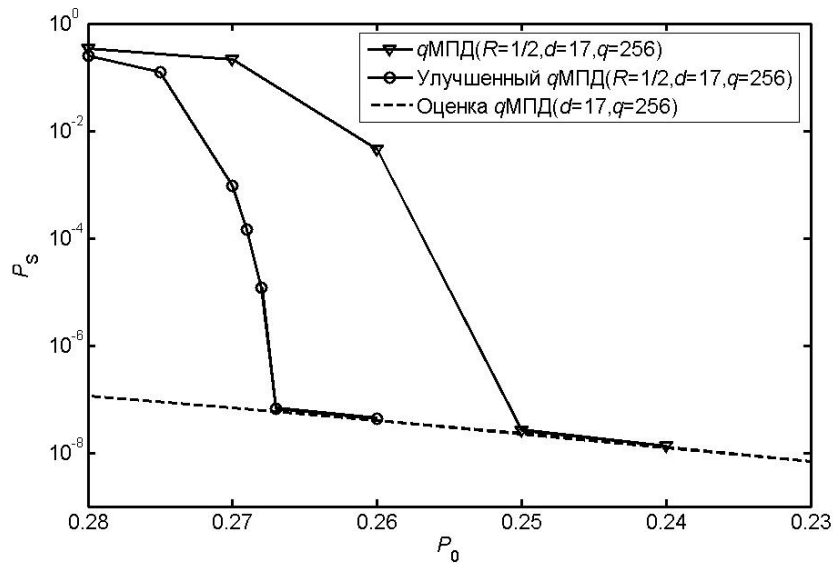


Рисунок 4 – Алгоритм построения недвоичных СОК

мальное количество символов  $i$ -й информационной ветви, участвующих в формировании символов  $j$ -й проверочной ветви;  $\text{GetProb}(poly)$  – функция для определения вероятности ошибки на выходе  $q$ МПД для недвоичного СОК, заданного полиномом  $poly$ .

Результаты моделирования недвоичных параллельных СОК в  $q$ СК показаны на рисунке 5. Из рисунка видно, что область эффективной работы параллельного недвоичного СОК с  $R=1/2$ , полученного с помощью применения данного алгоритма, оказывается на 13% ближе к пропускной способности канала по сравнению с лучшими из известных недвоичных СОК. Область эффективной работы параллельного кода с  $R=7/8$  оказывается на 20% ближе к пропускной способности канала.



**Рисунок 5 – Результаты моделирования параллельных СОК в  $q$ СК**

Из теории кодирования известно, что использование каскадных схем коррекции ошибок позволяет повысить эффективность применения кодирования по сравнению с базовыми некаскадными методами. В третьей главе диссертации рассмотрены вопросы применения  $q$ МПД в составе каскадных схем кодирования. Рассмотрена известная каскадная схема, состоящая из недвоичного самоортогонального кода и кода контроля по модулю  $q$ . Для данной каскадной схемы сформулирована и доказана следующая теорема.

**Теорема. Основная теорема декодирования каскадного кода, состоящего из недвоичного самоортогонального кода и кода контроля по модулю  $q$ .** При каждом изменении декодируемых символов декодером каскадного кода происходит переход к более правдоподобному решению для всего каскадного кода по сравнению с предыдущими состояниями декодера.

Предложена новая каскадная схема кодирования, состоящая из недвоичного СОК и модифицированного недвоичного кода Хэмминга. Обычные недвоичные коды Хэмминга используют вычисления в полях

Галуа, что является сложным для реализации при большом размере символа. Поэтому на базе обычных кодов Хэмминга были построены модифицированные двоичные коды Хэмминга, которые используют только операции сложения и вычитания целых чисел по модулю  $q$ . Декодер таких кодов всегда исправляет одну ошибку и в большинстве случаев две ошибки в блоке. Доля блоков с двумя ошибками, исправляемых декодером модифицированных двоичных кодов Хэмминга, равна  $1 - \frac{3^{m+1} - 3 \cdot 2^m + 1}{4^m}$ ,

где  $m$  – количество проверочных символов в кодовом слове. Например, для  $m=8$  исправляется порядка 71% блоков с двумя ошибками.

Доля блоков с двумя ошибками, исправляемых декодером модифицированных двоичных расширенных кодов Хэмминга, равна  $(q-2)/q$ . Например, для  $q=256$  исправляется 99.2% блоков с двумя ошибками, а при  $q=65536$  исправляется 99.997% блоков с двумя ошибками.

Получена нижняя оценка вероятности ошибки на выходе каскадной схемы, состоящей из  $q$ МПД и декодера модифицированного двоичного кода Хэмминга:

$$P_{err} = (1 - P_s)^{N_h - 2} \cdot P_s^2 (N_h - 1) \cdot \frac{3^{m+1} - 3 \cdot 2^m + 1}{4^m} + \frac{(1 - P_s)^{N_h - 3} P_s^3 (N_h - 1)(N_h - 2)}{2},$$

где  $P_s$  – оценка вероятности ошибки на выходе  $q$ МПД,  $N_h = 2^m - 1$  – длина блока двоичного кода Хэмминга

Получена нижняя оценка вероятности ошибки на выходе каскадной схемы, состоящей из  $q$ МПД и декодера модифицированного двоичного расширенного кода Хэмминга:

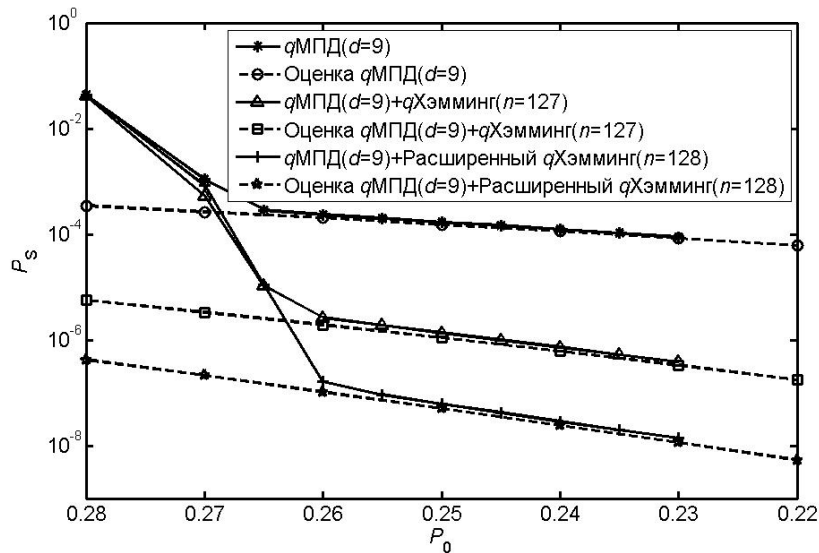
$$P_{errExt} = \frac{2 \cdot (1 - P_s)^{N_{ext} - 2} \cdot P_s^2 (N_{ext} - 1)}{q} + \frac{(1 - P_s)^{N_{ext} - 3} \cdot P_s^3 (N_{ext} - 1)(N_{ext} - 2)}{2},$$

где  $N_{ext} = 2^m$  – длина блока двоичного расширенного кода Хэмминга.

На рисунке 6 представлены характеристики каскадных схем кодирования, состоящих из двоичного СОК и двоичных кодов Хэмминга.

Из рисунка видно, что применение совместно с  $q$ МПД в области его эффективной работы декодеров модифицированных двоичных кодов Хэмминга позволяет снизить вероятность ошибки на выходе каскадной схемы на три и более порядков.

**В четвертой главе** «Программные средства моделирования двоичных многопороговых декодеров и каналов связи. Программные средства для защиты файлов от искажений» рассматриваются вопросы построения программного обеспечения, необходимого для исследования эффективности  $q$ МПД. Разработано программное средство MTDProtect для обеспечения дополнительной защиты от искажений информации, находящейся на оптических и магнитных носителях. Программа позволяет для отдельного



**Рисунок 6 – Характеристики каскадных схем кодирования**

файла или набора файлов создавать с помощью кодера недвоичного самоортогонального кода дополнительный проверочный файл, используя который можно восстановить исходную информацию даже в случае ее сильного повреждения. Показано, что использование  $q$ МПД для защиты файлов позволяет повысить скорость кодирования/восстановления информации в десятки раз по сравнению с известными программами-аналогами.

**В заключении** сформулированы основные результаты работы:

1. Проведено исследование существующих алгоритмов кодирования/декодирования, которые могут быть использованы в системах передачи и хранения информации для защиты данных от ошибок. Показано, что одними из наилучших с точки зрения отношения эффективности и сложности практической реализации являются недвоичные многопороговые декодеры недвоичных самоортогональных кодов. Выбраны направления исследований.

2. Рассмотрены вопросы использования  $q$ МПД в каналах Гилберта-Эллиота с пакетирующимися ошибками, в каналах со стираниями и в каналах со стираниями и искажениями. Показано, что в данных каналах  $q$ МПД является существенно более эффективным, чем декодер кодов Рида-Соломона, который до сих пор применяется практически во всех системах хранения информации. Кроме того, были получены нижние оценки вероятности ошибки оптимального декодирования недвоичных самоортогональных кодов в каналах со стираниями и искажениями.

3. Предложен алгоритм построения наиболее эффективных недвоичных самоортогональных кодов для схем параллельного кодирования. Применение таких кодов позволило приблизить области эффективной работы  $q$ МПД для кодов с  $R=1/2$  на 13% и для малоизбыточных кодов с  $R=7/8$  на 20% к границе Шеннона, определяющей потенциальные корректирующие возможности кодов.



4. Предложен новый алгоритм работы недвоичного порогового элемента  $q$ МПД, применение которого позволило повысить быстродействие  $q$ МПД более чем в 2 раза.

5. Доказана теорема о стремлении решения декодера каскадного кода, состоящего из недвоичного СОК и кода контроля по модулю  $q$ , к решению оптимального декодера.

6. Впервые была рассмотрена и исследована каскадная схема кодирования, состоящая из недвоичного СОК и модифицированных недвоичных кодов Хэмминга. Получены аналитические оценки эффективности данной каскадной схемы. Показано, что использование предложенной каскадной схемы позволяет уменьшить вероятность ошибки декодирования в области эффективной работы  $q$ МПД на три и более порядков.

7. Предложена методика применения  $q$ МПД для защиты файлов от искажений при длительном хранении. На базе данной методики было разработано программное средство MTDProtect, быстродействие которого в десятки раз превышает быстродействие программ-аналогов при сопоставимой эффективности восстановления данных.

8. Разработаны программные средства для исследования эффективности  $q$ МПД.

**В приложении** приводятся копии свидетельств об официальной регистрации разработанных программных средств и копии актов о внедрении результатов диссертации.

## **ПУБЛИКАЦИИ ПО ОСНОВНЫМ РЕЗУЛЬТАТАМ ДИССЕРТАЦИИ**

1. Золотарёв В.В., Овечкин Г.В., Овечкин П.В. Сравнение алгоритмов декодирования помехоустойчивых кодов для цифровых систем связи // Материалы 11-й Межд. науч.-техн. конф. «Проблемы передачи и обработки информации в сетях и системах телекоммуникаций». Рязань: РГРТА, 2002, С. 91–93.

2. Овечкин Г.В., Овечкин П.В. Эффективность применения многопорогового декодера в каскадных схемах // Материалы 8-й Всероссийской науч.-техн. конф. «Новые информационные технологии в научных исследованиях и в образовании». Рязань: РГРТА, 2003, С. 131–132.

3. Овечкин Г.В., Овечкин П.В. Эффективность каскадной схемы кодирования на базе многопорогового декодера и кодов Хэмминга // Межвуз. сб. науч. тр. «Математическое и программное обеспечение вычислительных систем». Рязань: РГРТА, 2004, С. 79–82.

4. Золотарёв В.В., Епишина Т.А., Овечкин Г.В., Овечкин П.В. Программные средства моделирования цифрового спутникового канала связи // Материалы межвуз. науч.-техн. конф. студентов, молодых ученых и специалистов «Новые информационные технологии в учебном процессе и производстве». Рязань: РИМГОУ, 2004, С. 77–79.

5. Денисова М.А., Овечкин Г.В., Овечкин П.В. Применение многопорогового декодера в системах передачи данных с многопозиционными системами модуляции // Материалы 13-й Межд. науч.-техн. конф. «Проблемы передачи и обработки информации в сетях и системах телекоммуникаций». Рязань: РГРТА, 2004, С. 58–59.

6. Овечкин П.В., Цыплаков Д.А. Разработка методов декодирования помехоустойчивых кодов на базе многопороговых декодеров // Материалы всероссийского смотра-конкурса научно-технического творчества студентов высших учебных заведений «Эврика-2005». Новочеркасск, 2005, Часть 1., С. 140–144.

7. Овечкин Г.В., Овечкин П.В. Построение самоортогональных кодов устойчивых к эффекту размножения ошибок // Мат. 14-й Межд. науч.-техн. конф. «Проблемы передачи и обработки информации в сетях и системах телекоммуникаций». Рязань: РГРТА, 2005, С. 70–71.

8. Золотарёв В.В., Овечкин Г.В., Овечкин П.В. Многопороговые декодеры: новые достижения // Мат. 14-й Межд. науч.-техн. конф. «Проблемы передачи и обработки информации в сетях и системах телекоммуникаций». Рязань: РГРТА, 2005, С. 57–58.

9. Гринченко Н.Н., Овечкин Г.В., Овечкин П.В. Развитие многопороговых алгоритмов декодирования помехоустойчивых кодов // Мат. науч.-практ. конф. «Научные исследования и их практическое применение. Современное состояние и пути развития». Одесса: Черноморье, 2005, Том 7, С. 13–14.

10. Овечкин П.В. Каскадное кодирование на базе многопороговых декодеров // Материалы 52-й студенческой науч.-техн. конф. «Математическое и программное обеспечение вычислительных систем». Рязань: РГРТА, 2005, С. 30.

11. Золотарёв В.В., Овечкин Г.В., Овечкин П.В. Современные методы помехоустойчивого кодирования для высокоскоростных спутниковых систем связи // Материалы 10 Всероссийской науч.-техн. конф. «Новые информационные технологии в научных исследованиях и в образовании НИТ-2005». Рязань: РГРТА, 2005, С. 2–3.

12. Гринченко Н.Н., Овечкин П.В. Свидетельство РОСПАТЕНТ №2006614261 о регистрации программы для ЭВМ «Имитационная модель многопорогового декодера помехоустойчивых кодов» (MultiDec) от 17.12.06.

13. Гринченко Н.Н., Золотарёв В.В., Овечкин Г.В., Овечкин П.В. Применение многопорогового декодера в каналах со стираниями // Труды НТОРЭС им. А.С.Попова, 2006, С. 338–340.

14. Гринченко Н.Н., Овечкин Г.В., Овечкин П.В. Вопросы применения многопороговых декодеров в каналах связи со стираниями // Межвуз. сб. науч. тр. «Математическое и программное обеспечение вычислительных систем». Рязань: РГРТА, 2006, С. 47–50.

15. Овечкин П.В. Эффективность использования многопорогового декодера в каналах связи со стираниями // мат. Всероссийской научно-технической конференции НИТ-2006. Рязань: 2006, С. 74–76.
16. Гринченко Н.Н., Овечкин Г.В., Овечкин П.В. Разработка каскадных схем кодирования на основе многопороговых декодеров // 8-я межд. конф. и выст. «Цифровая обработка сигналов и ее применение». М.: 2006, Том 1, С. 60–63.
17. Гринченко Н.Н., Золотарёв В.В., Овечкин Г.В., Овечкин П.В. Многопороговое декодирование в каналах с многопозиционной модуляцией // Вестник РГРТУ, Вып. 19, 2006, С. 179–182.
18. Овечкин П.В. Использование программных средств имитации цифрового спутникового канала в учебном процессе // Материалы XII межвузовской научно-методической конференции «Методы организации учебного процесса в ВУЗе». Рязань: РГРТУ, 2007, С. 73–74.
19. Золотарёв В.В., Овечкин Г.В., Овечкин П.В. Эффективность многопороговых декодеров при использовании многопозиционных ФМ и КАМ // 9-я межд. конф. и выст. «Цифровая обработка сигналов и ее применение». М.: 2007, Том 1, С. 5.
20. Овечкин П.В. Помехоустойчивое кодирование в широкоэмитальном видео // Межвуз. сб. науч. тр. «Математическое и программное обеспечение информационных систем». Рязань: РГРТУ, 2007, С. 68–71.
21. Овечкин П.В. Использование недвоичных многопороговых декодеров в магнитных и оптических запоминающих устройствах // 10-я Межд. конф. «Цифровая обработка сигналов и ее применение, DSPA-08». М.: 2008.
22. Овечкин П.В. Каскадные схемы на основе недвоичного многопорогового декодера // Мат. 15-й Межд. науч.-техн. конф. «Проблемы передачи и обработки информации в сетях и системах телекоммуникаций». Рязань: РГРТУ, 2008, С. 34–35.
23. Овечкин Г.В., Овечкин П.В. Использование многопороговых декодеров в системах дистанционного зондирования Земли // V Конференция молодых ученых, посвященная Дню космонавтики «Фундаментальные и прикладные космические исследования». М.: ИКИ РАН, 2008, С. 33.
24. Овечкин П.В. Применение недвоичного многопорогового декодера для защиты файлов от искажений // 11-я Межд. конф. «Цифровая обработка сигналов и ее применение, DSPA-09». М.: 2009, С. 200–202.
25. Овечкин Г.В., Овечкин П.В. Оптимизация структуры недвоичных самоортогональных кодов для схем параллельного кодирования // Труды НИИР, №2, 2009.
26. Овечкин П.В. Использование многопороговых декодеров в системах хранения больших объемов данных // VI Конференция молодых ученых, посвященная Дню космонавтики «Фундаментальные и прикладные космические исследования». М.: ИКИ РАН, 2009, С. 33–34.

Овечкин Павел Владимирович

**РАЗРАБОТКА АЛГОРИТМОВ ПОВЫШЕНИЯ ЭФФЕКТИВНОСТИ  
НЕДВОИЧНЫХ МНОГОПороГОВЫХ ДЕКОДЕРОВ В СИСТЕМАХ  
ПЕРЕДАЧИ И ХРАНЕНИЯ БОЛЬШИХ ОБЪЕМОВ ИНФОРМАЦИИ**

**А в т о р е ф е р а т**

диссертации на соискание ученой степени  
кандидата технических наук

Подписано в печать 19.05.2009 г. Формат бумаги 60×84 1/16.

Бумага офсетная. Печать ризографическая.

Усл. печ. л. 0,93. Уч.-изд. л. 1,0. Тираж 100 экз.

Отпечатано в ЗАО «Колорит»,  
г. Рязань, Первомайский проспект, д. 37/1.