

Учреждение образования
БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
ИНФОРМАТИКИ И РАДИОЭЛЕКТРОНИКИ

УДК 004.052.4

КУДЛАЦКАЯ
Марина Федоровна

**МНОГОПороГОВОЕ ДЕКОДИРОВАНИЕ БИНАРНЫХ
ИЗБИТОЧНЫХ КОДОВЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ
В СИСТЕМАХ ПЕРЕДАЧИ ИНФОРМАЦИИ**

АВТОРЕФЕРАТ

диссертации на соискание ученой степени
кандидата технических наук

по специальностям 05.13.19 – Методы и системы защиты информации,
информационная безопасность,
05.12.13 – Системы, сети и устройства телекоммуникаций

Минск 2016

Работа выполнена в учреждении образования «Белорусский государственный технологический университет».

Научный руководитель **Романенко Дмитрий Михайлович**, кандидат технических наук, доцент, заведующий кафедрой информатики и веб-дизайна учреждения образования «Белорусский государственный технологический университет»

Официальные оппоненты: **Борискевич Анатолий Антонович**, доктор технических наук, доцент, профессор кафедры сетей и устройств телекоммуникаций учреждения образования «Белорусский государственный университет информатики и радиоэлектроники»

Маликов Владимир Викторович, кандидат технических наук, доцент, начальник цикла технических и специальных дисциплин учреждения образования «Центр повышения квалификации руководящих работников и специалистов» Департамента охраны МВД Республики Беларусь

Оппонирующая организация **Белорусский национальный технический университет**

Защита состоится 29 декабря 2016 г. в 14.00 на заседании совета по защите диссертаций Д 02.15.06 при учреждении образования «Белорусский государственный университет информатики и радиоэлектроники» по адресу: 220013, г. Минск, ул. П. Бровки, 6, корп. 1, ауд. 232, тел. 293-89-89, e-mail: dissovet@bsuir.by.

С диссертацией можно ознакомиться в библиотеке учреждения образования «Белорусский государственный университет информатики и радиоэлектроники».

Автореферат разослан 11 ноября 2016 г.

Ученый секретарь совета по защите диссертаций, кандидат технических наук, доцент

Н.В. Насонова

КРАТКОЕ ВВЕДЕНИЕ

На сегодняшний день развитие информационных систем достигло значительных высот. Важными эксплуатационно-техническими характеристиками систем передачи информации являются высокая скорость и степень надежности передачи данных, что в свою очередь обеспечивает целостность и защиту передаваемой информации. Существует ряд аппаратных и программных методов, позволяющих повысить эти показатели. Одним из таких способов является использование помехоустойчивого кодирования данных с помощью избыточных кодов и соответствующих методов декодирования.

Современной теории кодирования известно несколько методов кодирования, способных работать вблизи пропускной способности канала, – турбокоды, LDPC-коды и другие, – а также методы их декодирования, позволяющие максимально реализовать корректирующие способности кодов. Среди этих методов можно выделить метод многопорогового декодирования (МПД), который позволяет декодировать очень длинные коды с линейной от длины кода сложностью исполнения. МПД обладает простотой и быстродействием обычного порогового декодера, что способствует его применению в высокоскоростных системах связи. Однако многопороговый декодер склонен к размножению ошибок (РО). Чтобы снизить степень РО, необходимо корректно подбирать параметры декодера (например, величины порогов на разных итерациях), а также тщательно подбирать коды, которые характеризуются малой степенью пересечения множеств ошибок, входящих в проверки относительно разных информационных символов. Архитектура итеративных кодов (ИК) легко поддается модификации, чтобы соответствовать этому требованию. При этом ИК обладают высокой корректирующей способностью, минимальной сложностью аппаратной и программной реализации и вместе с тем некоторыми недостатками: большой избыточностью, большой задержкой информации при декодировании и др. Предполагается, что итеративные коды и многопороговый декодер при совместном использовании нейтрализуют недостатки друг друга и приведут к решению главной проблемы – декодированию с эффективностью, близкой к оптимальной, но при максимально простой реализации.

Таким образом, совершенствование известных кодов, разработка новых, а также методов и алгоритмов их декодирования, обеспечивающих защиту информации в системах передачи двоичных данных, определили направление диссертационной работы.

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Связь работы с крупными научными программами, темами

Тема диссертационного исследования соответствует приоритетным направлениям научно-технической деятельности в Республике Беларусь на 2016–2020 гг. (Указ Президента Республики Беларусь от 22 апреля 2015 г. № 166 «О приоритетных направлениях научно-технической деятельности в Республике Беларусь на 2016–2020 годы»); выполнена в рамках ГПНИ «Информатика, космос и безопасность», подпрограмма «Информатика и космические исследования». Исследования проводились на кафедрах информационных систем и технологий и информатики и веб-дизайна учреждения образования «Белорусский государственный технологический университет» в рамках научно-исследовательских госбюджетных тем: ГБ 10-173 (№ ГР 20100307) «Разработка новых методов коррекции многократных группирующихся ошибок в каналах передачи информации, находящихся под воздействием электромагнитных помех и ионизирующих излучений», ГБ 14-024 (№ ГР 20141090) «Разработка и анализ методов адаптивного многопорогового декодирования низкоплотностных кодов для исправления многократных ошибок», ГБ 13-186 (№ ГР 20131234) «Разработка высокоскоростных адаптивных методов и аппаратно-программных средств декодирования избыточных кодов для исправления многократных модульных ошибок и стираний в каналах спутниковой передачи информации», ГБ 16-114 (№ ГР 20161346) «Разработка адаптивных помехоустойчивых кодеков на основе каскадных схем кодирования/декодирования для беспроводных систем передачи информации со стираниями, одиночными и модульными ошибками».

Цель и задачи исследования

Целью диссертационной работы является разработка и исследование методов преобразования информации на основе теории избыточного кодирования, предназначенных для обеспечения целостности информации за счет коррекции многократных ошибок в системах передачи данных путем многопорогового декодирования итеративных кодов.

Для достижения поставленной цели требуется решить следующие задачи:

- 1) проанализировать современное состояние проблемы использования методов кодирования/декодирования информации в системах передачи данных с целью повысить надежность и обеспечить целостность передаваемой информации;
- 2) разработать корректирующие коды для совместного применения с многопороговым декодером в системах передачи информации, которые обладают повышенными корректирующими способностями в отличие от известных кодов, обеспечивая повышенный контроль целостности и надежность передачи информации;

3) проанализировать эффективность исправления многократных независимых и группирующихся ошибок в кодовых последовательностях при многопороговом декодировании трехмерных линейных итеративных кодов;

4) разработать алгоритм исправления группирующихся ошибок высокой кратности в кодовых словах путем многопорогового декодирования трехмерных линейных итеративных кодов;

5) разработать модификацию многопорогового декодера, позволяющую сократить время декодирования;

6) разработать адаптивную систему кодирования/декодирования информации на основе многопорогового декодирования трехмерных линейных итеративных кодов с возможностью динамического изменения параметров кодов с целью повышения производительности системы передачи информации.

Научная новизна

Выполненные в работе исследования позволили получить следующие результаты:

– повышение надежности и целостности передаваемых данных путем исправления в кодовых словах двукратных, трехкратных и четырехкратных ошибок за счет увеличения числа линейно независимых проверок на четность (пять, семь и девять) в трехмерных линейных итеративных кодах, отличающихся от известных кодов данного класса большими минимальными кодовыми расстояниями (шесть, восемь и десять);

– сокращение времени многопорогового декодирования трехмерных линейных итеративных кодов в среднем на 50 % за счет динамического изменения порогового значения;

– повышение производительности помехоустойчивой системы передачи данных путем определения в режиме без отключения связи параметра качества канала связи BER на стадии декодирования с последующим изменением параметров (скорость, минимальное кодовое расстояние) используемого кода.

Положения диссертации, выносимые на защиту

1. Трехмерные линейные итеративные коды с числом линейно независимых проверок на четность пять, семь и девять, отличающиеся от известных кодов данного класса как большими минимальными кодовыми расстояниями (шесть, восемь и десять), так и избыточностью, что позволяет повысить надежность передачи и обеспечить целостность информации за счет исправления в кодовых словах двукратных, трехкратных и четырехкратных ошибок соответственно.

2. Метод защиты информации от ошибок на основе динамического многопорогового декодирования трехмерных линейных итеративных кодов, отличающийся от известного метода многопорогового декодирования возможностью сокращения числа итераций декодирования и, соответственно, сокращением време-

ни обнаружения и исправления ошибок в кодовых последовательностях (в среднем на 50 %) за счет динамического изменения порогового значения.

3. Метод защиты информации от многократных группирующихся ошибок, отличающийся использованием специализированных трехмерных итеративных кодов и модифицированного метода многопорогового декодирования с минимальными пороговыми значениями, что позволяет повысить кратность исправляемых пакетных ошибок до $k/4+1$ при $R = 0.39$, $k/8+1$ при $R = 0.47$ и $k/16+1$ при $R = 0.5$ и обеспечить целостность передаваемой информации.

4. Адаптивная система кодирования/декодирования информации на основе многопорогового декодирования трехмерных линейных итеративных кодов, отличающаяся от известных возможностью определения в режиме без отключения связи параметра качества канала связи BER (bit error rate – параметр ошибки по битам) на стадии декодирования с последующим изменением параметров (скорость, минимальное кодовое расстояние) используемого кода.

Личный вклад соискателя ученой степени

Все результаты, приведенные в диссертации, получены либо соискателем лично, либо при его непосредственном участии. В соавторстве разработаны «Адаптивное устройство кодирования/декодирования на основе итеративных кодов и многопорогового декодирования» (патент на полезную модель № u 2014479 от 01.06.15) и «Запоминающее устройство» (патент на изобретение № а 2011272 от 26.02.13). Определение целей и задач исследований, интерпретация и обобщение полученных результатов проводились совместно с научным руководителем канд. техн. наук, доц. Д. М. Романенко. В публикациях с соавторами вклад соискателя определяется рамками излагаемых в диссертации результатов.

Апробация диссертации и информация об использовании ее результатов

Основные положения и результаты диссертационной работы были представлены на следующих конференциях: VIII International Conference “News electrical and electronic technologies and their industrial implementation” (Zakopane, Poland, 2013); Международный форум «XLIII Неделя науки СПбПУ» (Санкт-Петербург, УО СПбПУ, 2014); XV и XVI Республиканская научная конференция студентов и аспирантов «Новые математические методы и компьютерные технологии в проектировании, производстве и научных исследованиях» (Гомель, ГГУ им. Ф. Скорины, 2012, 2013); Международная научная конференция «Информационные технологии и системы» (Минск, УО БГУИР, 2014) и др.

На основе предложенных в работе решений:

1) запатентовано изобретение «Запоминающее устройство», которое обладает повышенной надежностью и может быть использовано при производстве сверхбольших интегральных схем запоминающих устройств высокой информационной емкости, а также в системах кодирования двоичной информации;

2) разработана и зарегистрирована компьютерная программа, представляющая собой программную модель адаптивной системы кодирования/декодирования данных на основе многопорогового декодирования трехмерных итеративных кодов;

3) запатентована полезная модель «Адаптивное устройство кодирования/декодирования на основе итеративных кодов и многопорогового декодирования», которая обладает возможностью выбора кода в зависимости от качества канала и может быть использована в системах связи для повышения скорости и надежности передачи.

Результаты диссертационной работы внедрены и используются в учебном процессе УО «Белорусский государственный технологический университет», при разработке коммутатора Ethernet П-215 шифр «Вектор» на ОАО «АГАТ-СИСТЕМ – управляющей компании холдинга «Системы связи и управления».

Опубликование результатов диссертации

По результатам выполненных исследований опубликовано 18 печатных работ, в том числе 8 статей (7 из них в научных изданиях, рекомендуемых ВАК РФ, в том числе 2 – в зарубежных изданиях на английском языке), 6 тезисов докладов и материалов конференций, 2 авторских свидетельства о регистрации компьютерных программ, 1 патент на изобретение, 1 патент на полезную модель. Без соавторов опубликовано 6 работ.

Структура и объем диссертации

Работа состоит из перечня условных обозначений, введения, общей характеристики работы, четырех глав, заключения, библиографического списка и 6 приложений. Общий объем диссертационной работы составляет 140 страниц, из них 93 страницы основного текста, 38 иллюстраций на 19 страницах, 29 таблиц на 11 страницах, библиография из 83 наименований и 6 приложений на 25 страницах.

ОСНОВНАЯ ЧАСТЬ

Во **введении** определена область исследования диссертационной работы, обоснована актуальность темы диссертации, показана необходимость разработки и исследования алгоритмов и методов кодирования/декодирования с минимальной сложностью программной и аппаратной реализации и высокой эффективностью исправления многократных ошибок, возникающих в информации передаваемой по каналу связи.

В **общей характеристике** работы сформированы цели и задачи работы, связь работы с крупными научными программами и темами, охарактеризована

научная значимость полученных результатов, изложены основные положения диссертации, выносимые на защиту, объяснен личный вклад автора и апробация результатов диссертации.

В **первой главе** диссертации рассматривается помехоустойчивое кодирование как метод защиты информации от угроз непреднамеренного воздействия в системах передачи информации. Защита информации от непреднамеренного воздействия подразумевает предотвращение воздействия на нее ошибок пользователя, сбоя технического и программного обеспечения информационных систем, а также природных явлений и другой деятельности, приводящей к изменению информации, в том числе к искажению, уничтожению, копированию.

В компьютерных системах информационная безопасность достигается обеспечением конфиденциальности, достоверности и целостности обрабатываемых данных. При этом под целостностью информации понимается свойство информации сохранять свою структуру и содержание в процессе хранения и передачи. Целостность информации может быть нарушена как преднамеренно злоумышленником, так и в результате непреднамеренного воздействия на компьютерную систему. Особенно высока подобная угроза для систем передачи, так как передаваемые данные подвержены помехам, возникающим в результате воздействия окружающей среды на канал связи. Обеспечение целостности передаваемых данных является одной из сложных задач защиты информации, которая может решаться путем совместного применения как криптографических методов, так и методов помехоустойчивого кодирования.

За счет добавления избыточности помехоустойчивые коды позволяют обнаружить ошибки в передаваемой информации, обеспечивая тем самым контроль целостности, и исправить ошибки, возникающие при передаче данных, что приводит к восстановлению целостности передаваемой информации, что является основной задачей помехоустойчивого кодирования. Таким образом, помехоустойчивое кодирование является одним из методов защиты информации в контексте исправления ошибок в системах передачи данных, повышая надежность передачи информации.

Подробнее рассматриваются линейные блочные коды. Уделено внимание пакетным ошибкам, возникающим в кодовых последовательностях, передаваемых по каналу связи. Особое внимание в первой главе уделено параметрам качества канала связи: приводятся основные (наиболее часто используемые) параметры качества современных систем передачи данных, режимы и способы их измерения.

Анализ литературы показывает, что перспективным направлением повышения надежности систем передачи информации и обеспечения целостности передаваемой информации является применение методов кодирования/декодирования данных, позволяющих исправлять многократные ошибки с меньшими временными затратами. Основными требованиями к методам декодирования информации являются простота аппаратно-программной реализации и высокая скорость вы-

полнения вычислений. Как было отмечено, этим требованиям соответствует метод многопорогового декодирования (МПД).

Анализ существующих избыточных кодов, их свойств, методов кодирования и декодирования данных, а также технических параметров и надежностных характеристик современных систем передачи информации показал, что существует необходимость разработки новых избыточных кодов с высокими корректирующими способностями, которые совместно с быстродействующими алгоритмами декодирования кодовых последовательностей позволят достичь высокой эффективности исправления многократных независимых и пакетных ошибок в кодовых словах.

Во **второй главе** описываются новые разработанные структуры и свойства трехмерного линейного итеративного кода (ТЛИК), отличающиеся от известного итеративного кода увеличенным числом проверок на четность: ТЛИК5 (5 проверок), ТЛИК7 (7 проверок), ТЛИК9 (9 проверок). Коды обладают большим минимальным кодовым расстоянием $d = 6$, $d = 8$ и $d = 10$ соответственно, а значит, высокой корректирующей способностью. Коды позволяют корректировать многократные независимые ошибки, например, ТЛИК9 гарантированно одновременно исправляет четырехкратные ошибки и обнаруживает пятикратные, обеспечивая тем самым повышенный контроль целостности передаваемой информации. В таблице 1 представлены максимальные возможности кодов.

Таблица 1. – Максимальное число обнаруживаемых и исправляемых ошибок

Максимальное число ошибок	Количество линейно независимых проверок p			
	3	5	7	9
Исправляемые ошибки	1	2	3	4
Обнаруживаемые ошибки	3	5	7	9

Поскольку рассматриваемые итеративные коды характеризуются минимальной сложностью кодирования и декодирования, позволяют исправлять ошибки высокой кратности, а значит, соответствуют требованиям, предъявляемым к средствам исправления ошибок в системах передачи информации, предлагается использовать их совместно с МПД и рассмотреть их основные характеристики и корректирующие способности. Так как описываемые коды аналогичны по своей структуре, рассмотрим их свойства на примере ТЛИК с пятью проверками.

ТЛИК5 включает следующие проверки: проверки по горизонтали (h), проверки по вертикали (v), первые диагональные проверки между плоскостями со смещением по горизонтали ($dzh1$), первые диагональные проверки между плоскостями со смещением по вертикали ($dzv1$) и z -проверки. Все контрольные суммы в плоскостях исключаются, так как для метода МПД проверочные отношения должны быть линейно независимыми. В общем случае линейный трехмерный итеративный код можно определить как блочный (k_1, k_2, k_3) -код, формирующий кодовые последовательности длиной k информационных и r проверочных разря-

дов. Длина информационного слова k , а также величина избыточности r и длина кодовой последовательности n будут определяться следующими соотношениями:

$$r = \begin{cases} a \cdot k_m^2, & \text{при } k_1 = k_2 = k_3 \\ 2 \cdot k_1 \cdot k_3 + 2 \cdot k_2 \cdot k_3 + k_1 \cdot k_2, & \text{при } k_3 \leq k_2 \\ k_1 \cdot k_3 + k_2 \cdot k_3 + 3 \cdot k_1 \cdot k_2, & \text{при } k_3 > k_2 \end{cases}$$

$$n = k + r = k_m^3 + 5 \cdot k_m^2, \quad k = k_1 \cdot k_2 \cdot k_3,$$

где k_1 – количество горизонтальных проверок в плоскости;

k_2 – количество вертикальных проверок в плоскости;

k_3 – количество плоскостей трехмерного итеративного кода (в случае кубической конструкции кода – $k_1 = k_2 = k_3 = k_m$).

Скорость кода R и относительная избыточность $r_{\text{отн}}$ для кубической структуры кода равны

$$R = \frac{k}{n} = \frac{k_m^3}{k_m^3 + 5 \cdot k_m^2}, \quad r_{\text{отн}} = \frac{r}{n} = \frac{5 \cdot k_m^2}{k_m^3 + 5 \cdot k_m^2}.$$

Минимальное кодовое расстояние кода ТЛИК5 равно шести ($d = 6$). Следовательно, код позволяет корректировать все двукратные ошибки и обнаруживать трехкратные. Предлагаемые коды обладают высокой степенью избыточности, которая, как показывает график на рисунке 1, возрастает с числом проверок на четность и уменьшается с ростом длины информационной последовательности.

Доказано, что увеличение числа проверок не влияет на время кодирования информационной последовательности, поскольку операции вычисления проверочных символов, представляющие суммирование по модулю два соответствующих информационных битов, можно осуществлять параллельно, при этом количество операций с увеличением числа проверок не возрастает в случае кубической структуры кода или возрастает незначительно в ином случае. Таким образом, увеличение количества проверочных символов не влияет на время кодирования данных, а лишь повышает корректирующие способности ТЛИК.

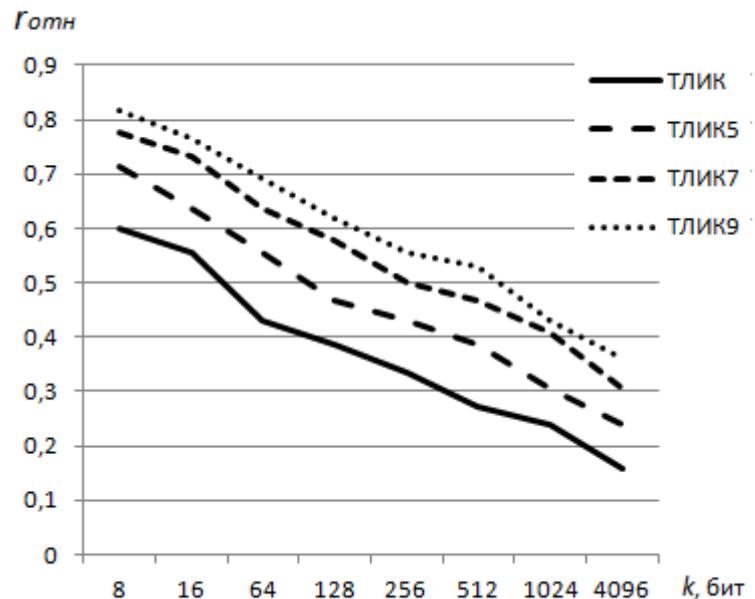


Рисунок 1. – Сравнительная характеристика ТЛИК

Значения основных параметров рассматриваемых трехмерных итеративных кодов представлены в таблице 2. Это длина кодовой последовательности n , скорость кода R и относительная избыточность $r_{\text{отн}}$. Стоит отметить, что коды с кубической конструкцией (т. е. $k_1 = k_2 = k_3$) характеризуются более высокой скоростью кодирования, чем коды с другими значениями параметров k_1, k_2, k_3 .

Таблица 2. – Свойства кодов ТЛИК

Код, $k (k_1, k_2, k_3)$	Количество проверок на четность p								
	5			7			9		
	n	R	$r_{\text{отн}}$	n	R	$r_{\text{отн}}$	n	R	$r_{\text{отн}}$
8 (2, 2, 2)	28	0.29	0.71	36	0.22	0.78	44	0.18	0.82
16 (2, 2, 4)	44	0.36	0.64	60	0.27	0.73	68	0.24	0.77
64 (4, 4, 4)	144	0.44	0.56	176	0.36	0.64	208	0.31	0.69
128 (4, 4, 8)	240	0.53	0.47	304	0.42	0.58	336	0.38	0.62
256 (8, 8, 4)	448	0.57	0.43	512	0.50	0.50	576	0.44	0.56
512 (8, 8, 8)	832	0.62	0.39	960	0.53	0.47	1088	0.47	0.53
1024 (8, 8, 16)	1472	0.70	0.30	1728	0.59	0.41	1792	0.57	0.43
4096 (16, 16, 16)	5376	0.76	0.24	5888	0.70	0.30	6400	0.64	0.36

Предлагаемые коды с повышенным числом проверок на четность обладают высокой скоростью кодирования, которая уменьшается с ростом числа линейно независимых проверок на четность и стремится к единице с ростом числа информационных символов (рисунок 2).

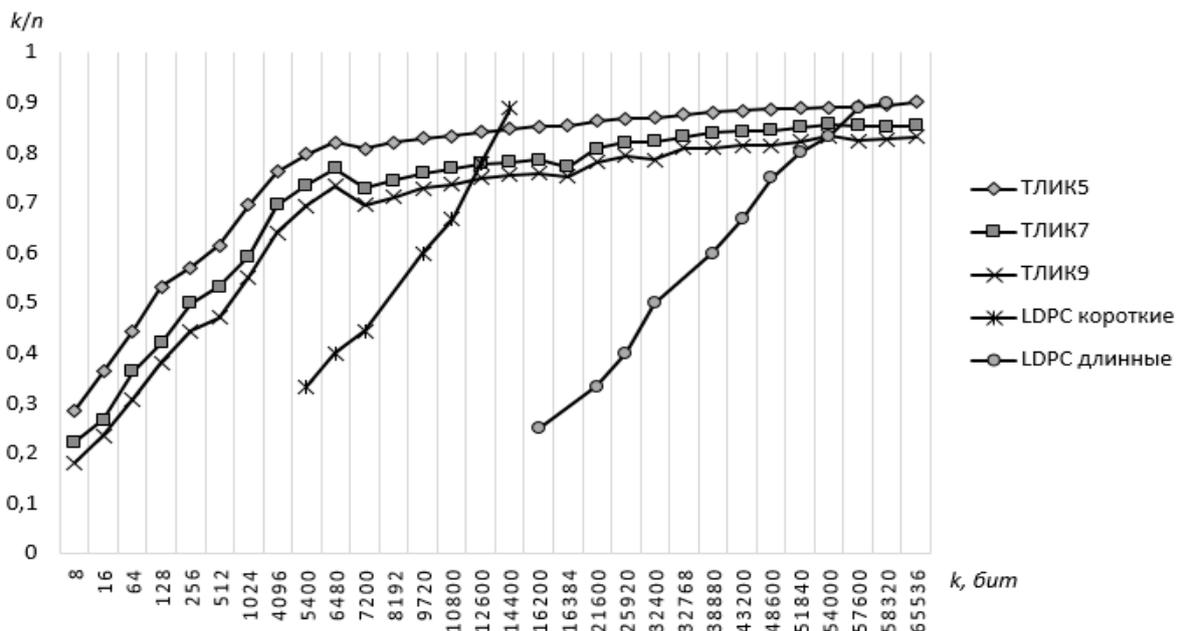


Рисунок 2. – Скорость кодов

Проверочные матрицы описываемых кодов содержат малое число единиц. Так матрицы H ТЛИ-кодов, конструкции которых близки к кубической, содержат

от $0.02n$ до $0.0009n$ единиц в строке, при $256 \leq n \leq 65536$. Кроме того, при некоторых значениях k (рисунок 2) предлагаемые коды не уступают по скорости низкоплотным кодам (рассматриваемые LDPC-коды нерегулярные, проверочные матрицы построены согласно алгоритму случайных перестановок).

Как известно, одной из важнейших задач построения помехоустойчивых кодов с заданными характеристиками является установление соотношения между его способностью обнаруживать и исправлять ошибки и избыточностью. Существуют граничные оценки, связывающие минимальное кодовое расстояние d , длину кода n , длину информационного слова k и кратность корректируемых ошибок t . Результаты расчета граничных условий приведены на рисунках 3 и 4 (кривая 1 – граница Хэмминга, 2 – граница Варшавова–Гилберта, 3 – граничные соотношения для данного кода).

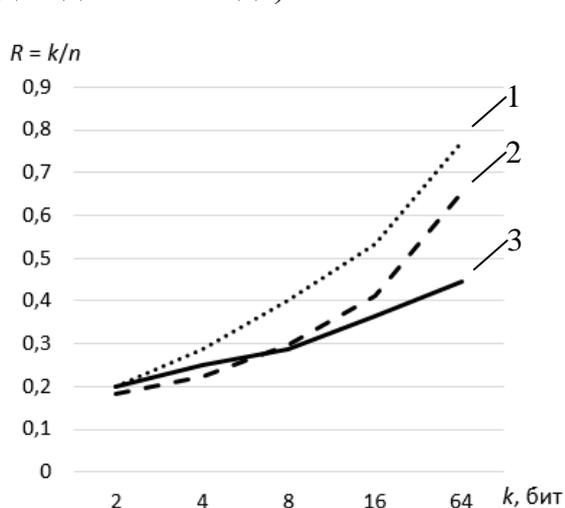


Рисунок 3. – Граничные соотношения для кода ТЛИК7

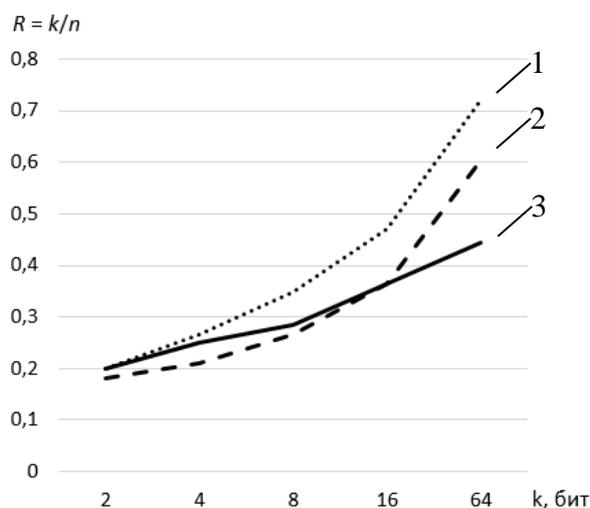


Рисунок 4. – Граничные соотношения для кода ТЛИК9

Граничные соотношения изучались с параметрами $d = 8$ и $t = 3$ – ТЛИК7 (рисунок 3), $d = 10$ и $t = 4$ – ТЛИК9 (рисунок 4) для трехмерного линейного кода с кубической конструкцией. Как видно из графиков, ТЛИК7 при значениях k от 2 до 8 бит, является совершенным (кривая граничных соотношений данного кода расположена между границами Хэмминга и Варшавова–Гилберта), код ТЛИК9 является совершенным при значениях k от 2 до 16 бит. При остальных значениях k с точки зрения избыточности трехмерный итеративный код совершенным не является. Надо отметить, что высокая избыточность свойственна всем итеративным кодам, в том числе и трехмерным.

В третьей главе проведен анализ эффективности исправления многократных группирующихся и независимых ошибок методом многопорогового декодирования кодов ТЛИК5, ТЛИК7, ТЛИК9. Анализ позволил сделать следующие выводы:

1. С увеличением длины информационной последовательности и с ростом скорости трехмерного линейного итеративного кода наблюдается рост доли исправленных многократных ошибок в кодовых словах. Так, например, для кода

ТЛИК5 при $k = 512$ бит данный параметр для трехкратных ошибок достигает величины 99,99 %, а для четырехкратных – 99,82 % (рисунок 5).

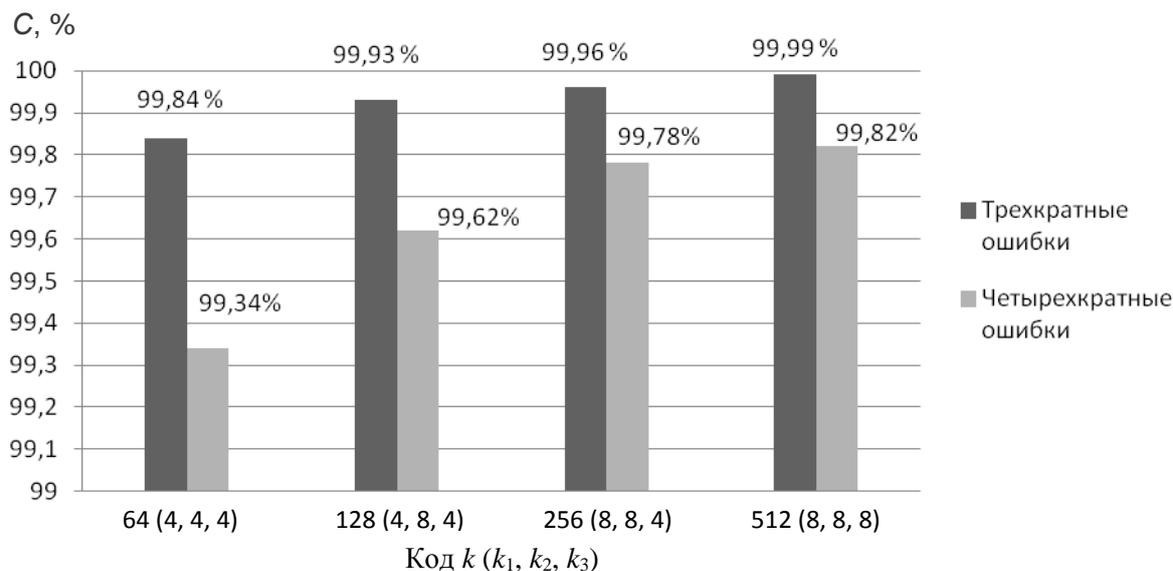


Рисунок 5. – Эффективность исправления многократных ошибок в кодовых последовательностях с различным числом информационных символов k

2. Наибольшей доли исправленных многократных независимых ошибок методом многопорогового декодирования кодов ТЛИК можно достичь при использовании кодов с наименьшим количеством плоскостей при условии, что преобладают проверки на четность между плоскостями (рисунок 6).

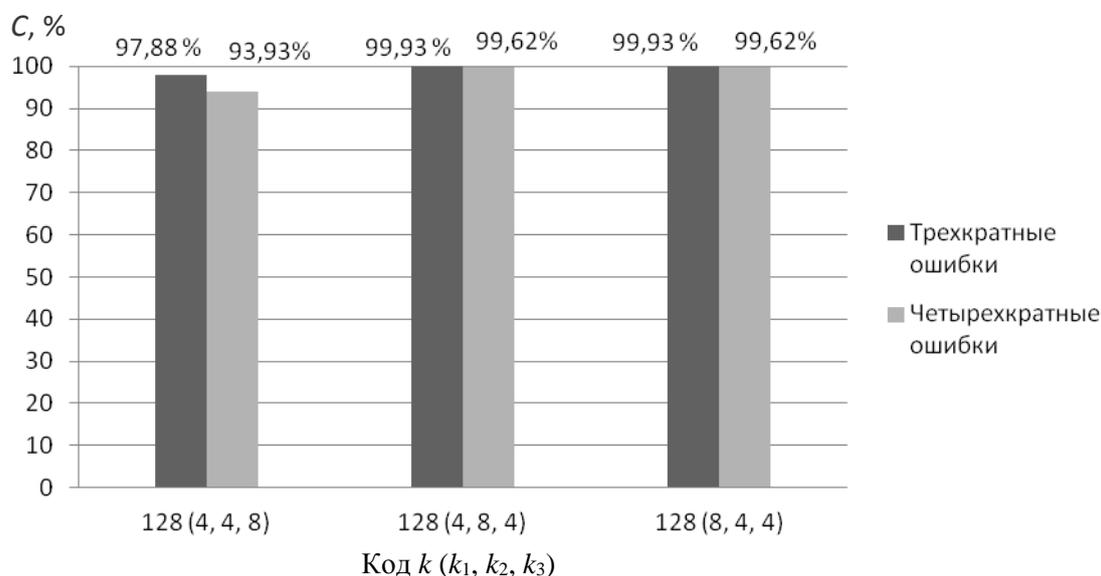


Рисунок 6. – Эффективность исправления многократных ошибок при использовании трехмерных кодов с разным числом плоскостей k_3

Доля исправленных многократных ошибок C (%) определяется отношением

$$C = \frac{C_{\text{и}}}{C_{\text{о}k+r}^m} \cdot 100,$$

где C_n – число исправленных ошибок кратностью m ;

C_{ok+r}^m – общее число сгенерированных ошибок в кодовом слове, которое рассчитывается как число сочетаний из $k+r$ по m .

3. Доля исправленных группирующихся ошибок трехмерными линейными итеративными кодами зависит от числа вертикальных проверок в плоскости, при этом наблюдается следующая зависимость: чем больше вертикальных проверок, тем больше кратность пакетов, которые гарантированно будут исправлены. Кроме того, результаты исследований показали, что многопороговый декодер гарантированно исправляет все пакеты, кратность которых не превышает количество столбцов в плоскости трехмерного итеративного кода (таблица 3).

Таблица 3. – Результаты исправления группирующихся ошибок

Код $k (k_1, k_2, k_3)$	Кратность группирующихся ошибок m , бит											
	3	4	5	6	7	8	9	10	11	12	13	14
	Доля исправленных группирующихся ошибок C , %											
64 (4, 4, 4)	100	100	100	67.6	78.9	78.1	56.6	62.2	55.2	63.9	61.3	55.7
128 (4, 4, 8)	100	100	47.4	47.2	47.0	46.7	46.5	46.3	46.0	56.3	46.0	45.8
128 (4, 8, 4)	100	100	100	100	100	100	75.8	63.5	63.8	75.5	51.6	58.4
128 (8, 4, 4)	100	100	100	62.9	75.6	75.1	50.8	60.3	50.4	68.1	66.3	50.2
256 (8, 8, 4)	100	100	100	100	100	100	71.8	57.6	57.7	71.6	43.5	51.0
512 (8, 8, 8)	100	100	100	100	100	100	100	46.4	84.7	53.9	69.5	61.5

Учитывая установленную зависимость, предлагается модифицировать коды ТЛИК путем увеличения числа вертикальных проверок в плоскости. Примером такого кода является разработанный для моделирования код ТЛИК4-16, структура которого включает 16 столбцов в плоскости, при этом код включает четыре линейно независимые проверки: горизонтальные (h), вертикальные (v), диагональные проверки между плоскостями со смещением по вертикали ($dzv1$), z -проверки. Проверочные символы рассчитываются в соответствии с соотношениями:

$$\begin{aligned}
 R_1 &= X_1 \oplus X_2 \oplus X_3 \oplus X_4 \oplus X_5 \oplus X_6 \oplus X_7 \oplus X_8 \oplus \\
 &\quad \oplus X_9 \oplus X_{10} \oplus X_{11} \oplus X_{12} \oplus X_{13} \oplus X_{14} \oplus X_{15} \oplus X_{16}, \\
 R_2 &= X_{17} \oplus X_{18} \oplus X_{19} \oplus X_{20} \oplus X_{21} \oplus X_{22} \oplus X_{23} \oplus X_{24} \oplus \\
 &\quad \oplus X_{25} \oplus X_{26} \oplus X_{27} \oplus X_{28} \oplus X_{29} \oplus X_{30} \oplus X_{31} \oplus X_{32}, \dots \\
 R_5 &= X_1 \oplus X_{17}, \quad R_6 = X_2 \oplus X_{18}, \quad \dots \\
 R_{37} &= X_1 \oplus X_{49}, \quad R_{38} = X_{17} \oplus X_{33}, \quad \dots \\
 R_{69} &= X_1 \oplus X_{33}, \quad \dots \quad R_{100} = X_{32} \oplus X_{64}.
 \end{aligned}$$

Как известно, эффективность исправления ошибок зависит не только от используемого кода, но и от декодера. Путем экспериментального подбора парамет-

ров модифицирован многопороговый декодер с целью повышения доли исправленных пакетных ошибок. Для кода ТЛИК4-16 модификация многопорогового декодера подразумевает декодирование кодовой последовательности в две итерации с минимальными пороговыми значениями на каждой итерации (таблица 4).

Анализ результатов моделирования, проведенного с помощью разработанного программного средства MPD v.1.0, показал, что наиболее эффективного исправления группирующихся ошибок можно достичь совместным использованием специализированного ТЛИК и модифицированного МПД, который помимо эффективности декодирования кодовых последовательностей превосходит обычные трехмерные итеративные коды и МПД еще и скоростью декодирования за счет сокращения числа итераций.

Таблица 4. – Эффективность исправления группирующихся ошибок

Код	Кратность исправляемой группирующейся ошибки m , бит															
	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
	Доля исправленных пакетных ошибок C , %															
ТЛИК5	100	67.63	78.99	78.1	56.62	62.22	55.22	63.91	61.36	55.73	54.62	53.49	53.13	52.76	52.36	52
ТЛИК4-16	100	100	100	100	100	100	100	100	100	100	100	100	100	81.63	95.89	79.31

В данной главе приводится модифицированный метод МПД, позволяющий пропускать итерации декодирования, если это не влияет на результате исправления ошибки, и сокращать тем самым время декодирования кодовых последовательностей. Суть метода заключается в том, что на некоторых итерациях многопорогового декодирования ни один бит не будет определен как ошибочный, а значит, не будет инвертирован, что в свою очередь никак не повлияет на результат декодирования. В таком случае эти итерации декодирования можно пропустить. Результаты моделирования модифицированного метода многопорогового декодирования ТЛИК показали, что никакой зависимости между количеством пропущенных итераций, длиной информационной последовательности и структурой кода не наблюдается, но при этом видна зависимость от числа проверок на четность и кратности исправляемых ошибок (таблица 5).

Таблица 5. – Среднее количество пропущенных итераций (%)

Кратность независимых ошибок m , бит	Число линейно независимых проверок p		
	5	7	9
1	52	66	74
2	41	58	68
3	32	51	63
4	24	44	56

Из таблицы 5 видно, что с ростом числа проверок возрастает среднее количество итераций, на которых ошибки не будут исправлены. Так в случае исправления однократной ошибки при использовании матрицы с пятью проверками было в среднем пропущено 52 % итераций, при семи проверках – в среднем 66 %, а при девяти – в среднем 74 % итераций.

Также можно отметить, что с ростом кратности независимых ошибок среднее количество пропущенных итераций будет уменьшаться, например, при использовании проверочной матрицы с пятью проверками для исправления однократных ошибок число итераций сокращается в среднем на 52 %, при исправлении двукратных – в среднем на 41 %, при трехкратных – в среднем на 32 %, и при четырехкратных – на 24 %.

Таким образом, модификация метода многопорогового декодирования трехмерного линейного итеративного кода позволяет сократить число итераций декодирования в среднем на 50 %, сократив тем самым время декодирования.

Проведенный в данной главе анализ показал, что предлагаемые алгоритмы и методы кодирования и декодирования повышают эффективность обнаружения и исправления ошибок в передаваемых битовых последовательностях, повышая тем самым контроль целостности информации и надежность передачи данных.

В четвертой главе описана разработанная адаптивная система кодирования/декодирования данных на основе многопорогового декодирования трехмерных итеративных кодов. Система позволяет динамически изменять параметры ТЛИК кодов с целью повышения надежности или скорости кода, адаптируясь к качеству канала связи. Блоки кодирования и декодирования информации адаптивной системы включают запоминающее устройство, в котором хранятся 14 проверочных матриц кодов ТЛИК, представленных в таблице 6.

Система включает блок определения кратности исправляемых ошибок, что позволяет определить число ошибочных бит и рассчитать коэффициент ошибок по битам BER в режиме без отключения связи. По рассчитанному коэффициенту можно определить категорию качества канала. Качество канала предлагается условно разделить на пять категорий (таблица 7).

Если качество канала соответствует категориям С и ниже, нужно повысить корректирующие способности кода, выбрав код с более высоким числом проверок четности.

Определение кратности исправляемой

Таблица 6. – Параметры трехмерных итеративных кодов

Скорость кода R	Количество линейно независимых проверок p		
	5	7	9
	Длина информационной последовательности k , бит		
4/13			64
4/11		64	
8/21			128
8/19		128	
16/37			256
4/9	64	128	256
16/35		256	
1/2	128	256	
8/15	128		
4/7	256		
16/27	256		

Таблица 7. – Категории качества канала

Категория	Значение BER
A (высокое)	$BER \leq 10^{-6}$
B (хорошее)	$10^{-6} < BER \leq 10^{-5}$
C (среднее)	$10^{-5} < BER \leq 10^{-4}$
D (низкое)	$10^{-4} < BER \leq 10^{-3}$
E (деградация)	$BER < 10^{-3}$

ошибки, расчет параметра BER, определение качества канала и выбор соответствующего кода осуществляет блок анализа. На сторону передатчика передается адрес нового выбранного кода и весь процесс осуществляется заново. Если качество канала соответствует категории

A (высокое) или B (хорошее), то при следующей передаче выбирается код с более высокой скоростью, так как высокое качество канала не повлияет на целостность передаваемой информации, значит, нет необходимости использовать код с повышенной корректирующей способностью.

Разработанное программное средство ASDecoder v.1.0 позволило получить результаты моделирования адаптивного устройства, которые показали, что динамическое изменение параметров кода приводит к повышению производительности предложенного метода кодирования/декодирования данных по сравнению с кодированием/декодированием без изменения параметров. Кроме того, в случае повышения качества канала динамически устанавливается более быстрый код, что увеличит скорость передачи информации.

ЗАКЛЮЧЕНИЕ

Основные научные результаты диссертации

1. Разработаны конструкции и исследованы свойства трехмерных линейных итеративных кодов с числом линейно-независимых проверок на четность 5, 7 и 9, отличающихся от известных кодов данного класса большими минимальными кодовыми расстояниями ($d = 6$, $d = 8$ и $d = 10$ соответственно, для известного трехмерного линейного итеративного кода $d = 4$), что позволяет корректировать не только одиночные ошибки, но и ошибки, кратность которых достигает 4, а также повысить контроль целостности передаваемой информации [1, 3].

2. Установлено, что наибольшей эффективности исправления многократных ошибок многопороговым декодированием трехмерных итеративных кодов можно достичь при использовании кодов с наименьшим числом плоскостей k_3 при условии, что преобладают проверки между плоскостями: при длине информационной последовательности $k = 512$ бит эффективность исправления трехкратных ошибок для кодов с $k_3 = 4$ достигает 99.62 %, с $k_3 = 8$ – 93.93 %, четырехкратных ошибок для кодов с $k_3 = 4$ – 99.93 %, с $k_3 = 8$ – 97.88 %. Показано, что с увеличением длины информационной последовательности k и с ростом скорости кода R наблюдается рост доли исправленных многократных ошибок: при $R = 0.62$, $k = 512$ бит данный параметр для трехкратных ошибок достигает 99.99 %, а для четырехкратных – 99.82 %.

Чем больше вертикальных проверок в плоскости трехмерного итеративного кода, тем больше кратность группирующихся ошибок, которые гарантированно будут исправлены. На основании этого предложен метод исправления группирующихся ошибок путем модифицированного многопорогового декодирования трехмерного итеративного кода с максимальным числом вертикальных проверок в плоскости, который гарантированно исправляет группирующиеся ошибки кратностью до $k/4+1$ при $R = 0.39$, $k/8+1$ при $R = 0.47$ и $k/16+1$ при $R = 0.5$, при декодировании с минимальными пороговыми значениями на всех итерациях декодирования [3, 8].

3. Разработан метод динамического многопорогового декодирования с новым алгоритмом выбора пороговых значений, который позволяет сократить число итераций декодирования трехмерных итеративных кодов по сравнению со стандартным методом многопорогового декодирования, сократив тем самым время декодирования. Например, при $k = 512$ бит, $R = 0.62$ в процессе исправления однократных ошибок можно сократить число итераций (время декодирования) в среднем на 46 %, при $R = 0.47$ – на 71 %, в процессе исправления четырехкратных ошибок при $R = 0.62$ – на 25 %, при $R = 0.47$ – на 54 % [2, 13].

4. Разработана адаптивная система кодирования/декодирования с контролем целостности на основе трехмерных итеративных кодов и метода многопорогового декодирования, обладающая возможностью определять количество ошибочных бит и рассчитывать коэффициент ошибок по битам BER в режиме без отключения связи для определения качества канала. В зависимости от качества канала система позволяет динамически изменять параметры кода с целью повысить надежность передачи данных при ухудшении качества канала или увеличить скорость передачи информации, если качество канала улучшилось [4, 5, 6, 7, 11, 15, 16].

Рекомендации по практическому использованию результатов

1. Разработанные конструкции трехмерных линейных итеративных кодов с повышенным числом линейно независимых проверок на четность использовались при разработке изобретения «Запоминающее устройство» с целью повышения надежности и обеспечения целостности информации [9].

2. Разработано программное средство, представляющее имитационную модель адаптивной системы кодирования/декодирования с контролем целостности на основе трехмерных итеративных кодов и метода динамического многопорогового декодирования и позволяющее моделировать процесс кодирования, декодирования, генерацию ошибок в кодовой последовательности, реальный канал передачи данных [7, 12].

Результаты диссертационной работы внедрены и используются в учебном процессе учреждения образования «Белорусский государственный технологический университет», при разработке коммутатора Ethernet шифр «Вектор» П-215 на ОАО «АГАТ-СИСТЕМ – управляющей компании холдинга «Системы связи и управления».

СПИСОК ПУБЛИКАЦИЙ СОИСКАТЕЛЯ УЧЕНОЙ СТЕПЕНИ

Статьи в рецензируемых научных журналах

1. Романенко, Д.М. Многопороговое мажоритарное декодирование низкоплотных кодов / Д.М. Романенко, Д.В. Шиман, М.Ф. Виткова // Труды БГТУ. Сер. VI. Физ.-мат. науки и информ. – Минск. – Вып. XIX. – 2011. – С. 128–132.

2. Виткова, М.Ф. Адаптивное многопороговое декодирование многомерных итеративных кодов / М.В. Виткова, Д.М. Романенко // Труды БГТУ. Сер. VI. Физ.-мат. науки и информ. – Минск. – Вып. XX. – 2012. – С. 134–138.

3. Multithreshold majority decoding of LDPC-codes / P. Urbanovich, D. Romanenko, D. Shiman, M. Vitkova // Informatyka Automatyka Pomiaru. – Poland, Lublinie. – R. 84, № 4a/2012. – 2012. – P. 22–24.

4. Виткова, М.Ф. Особенности определения параметров качества канала связи при многопороговом декодировании итеративных кодов / М.Ф. Виткова, Д.М. Романенко // Труды БГТУ. Сер. VI. Физ.-мат. науки и информ. – Минск. – Вып. XXI. – 2013. – С. 111–114.

5. Urbanovich, P.P. The algorithm for determining the errors multiplicity by multi-threshold decoding of iterative codes / P.P. Urbanovich, M.F. Vitkova, D.M. Romanenko // Electrical Review. – Poland, Lublinie. – 2013. – P. 235–238.

6. Виткова, М.Ф. Адаптивная система кодирования/декодирования на основе многомерных итеративных кодов и многопороговых декодеров / М.Ф. Виткова, Д.М. Романенко // Труды БГТУ. Сер. VI. Физ.-мат. науки и информ. – Минск. – Вып. XXII. – 2014. – С. 116–120.

7. Кудлацкая, М.Ф. Программная имитационная модель адаптивного многопорогового декодирования линейных блочных кодов / М.Ф. Кудлацкая // Труды БГТУ. Сер. VI. Физ.-мат. науки и информ. – Минск. – Вып. XXIII. – 2015. – С. 208–212.

Статьи в других научных изданиях

8. Виткова, М.Ф. Программное средство для изучения свойств многопороговых декодеров в системах передачи информации / М.Ф. Виткова, Д.М. Романенко // Научные стремления: сб. науч. ст. НАН Беларуси. – Минск, 2012. – № 1. – С. 121–124.

Патенты и авторские свидетельства

9. Запоминающее устройство: пат. на изобретение Респ. Беларусь, МПК: G 11С 11/00, Н 03М 13/09 / П.П. Урбанович, Д.М. Романенко, Н.В. Пацей, Д.В. Шиман, М.Ф. Виткова, Ю.О. Булова; заявитель Бел. гос. технолог. ун-т. – № а 2011272; заявл. 30.09.11; опубл. 26.02.13 // Офиц. бюл. / Нац. центр интелект. собств. – 2013.

10. Компьютерная программа MPD v.1.0: а. с. 510 Респ. Беларусь / Д.М. Романенко, М.Ф. Виткова; заявитель Бел. гос. технолог. ун-т. – № С20130033; заявл. 04.04.2013; опубл. 23.05.2013.

11. Адаптивное устройство кодирования/декодирования данных на основе итеративных кодов и многопорогового декодирования: пат. на полезную модель Респ. Беларусь, МПК: Н 03М 13/43, Н 04L 1/00 / М.Ф. Кудлацкая, Д.М. Романенко; заявитель Бел. гос. технолог. ун-т. – № и 2014479; заявл. 30.12.2014; опубл. 01.06.15 // Офиц. бюл. / Нац. центр интелект. собств. – 2015.

12. Компьютерная программа ASDecoder v.1.0: а. с. 801 Респ. Беларусь / Д.М. Романенко, М.Ф. Кудлацкая; заявитель Бел. гос. технолог. ун-т. – № С20150046; заявл. 04.06.2015; опубл. 11.09.2015.

Статьи в сборниках материалов научных конференций

13. Виткова, М.Ф. Оптимизация процесса многопорогового декодирования многомерных линейных итеративных кодов / М.Ф. Виткова // Новые математические методы и компьютерные технологии в проектировании, производстве и научных исследованиях: материалы XV Респ. науч. конф. студентов и аспирантов: в 2 ч., Гомель, 26–28 марта 2012 г. / ГГУ им. Ф. Скорины – Гомель, 2012. – Ч. 2. – С. 50–51.

14. Виткова, М.Ф. Особенности определения кратности ошибки в процессе многопорогового декодирования избыточных кодовых последовательностей / М.Ф. Виткова // Новые математические методы и компьютерные технологии в проектировании, производстве и научных исследованиях: материалы XVI Респ. науч. конф. студентов и аспирантов: в 2 ч., Гомель, 23–25 апреля 2013 г. / ГГУ им. Ф. Скорины. – Гомель, 2013. – Ч. 2. – С. 55–56.

15. Urbanovich, P.P. The algorithm for determining the multiplicity of errors by multithreshold decoding of iterative codes / P.P. Urbanovich, M.F. Vitkova, D.M. Romanenko // News electrical and electronic technologies and their industrial implementation: proc. VIII International Conference, Zakopane, Poland, June 18–21, 2013 / Poland, 2013. – P. 148.

16. Кудлацкая, М.Ф. Идентификация многократных ошибок в процессе многопорогового декодирования трехмерных итеративных кодов / М.Ф. Кудлацкая // Информационные технологии и системы: материалы международной науч. конф., Минск, октябрь 2014 г. / БГУИР. – Минск, 2014. – С. 270–271.

Тезисы докладов на научных конференциях

17. Виткова, М.Ф. Особенности адаптивной системы кодирования/декодирования на основе многомерных итеративных кодов и многопороговых декодеров / М.Ф. Виткова, Д.М. Романенко // Издательское дело и полиграфия: тез. 78-й науч.-техн. конф. профессорско-преподавательского состава, научных

сотрудников и аспирантов, Минск, 4 февраля 2014 г. / БГТУ; отв. за издание И.М. Жарский. – Минск, 2014. – С. 36.

18. Кудлацкая, М.Ф. Программная реализация имитационной модели адаптивного многопорогового декодирования / М.Ф. Кудлацкая // Информационные технологии: тез. 79-й науч.-техн. конф. профессорско-преподавательского состава, научных сотрудников и аспирантов, Минск, 4 февраля 2015 г. / БГТУ; отв. за издание И. М. Жарский. – Минск, 2015. – С. 21.

РЭЗІЮМЭ

Кудлацкая Марына Фёдараўна

ШМАТПАРОГАВАЕ ДЭКАДЗІРАВАННЕ БІНАРНЫХ ЗАЛІШНІХ КОДАВЫХ ПАСЛЯДОЎНАСЦЯЎ У СІСТЭМАХ ПЕРАДАЧЫ ІНФАРМАЦЫІ

Ключавыя словы: памехаўстойлівае кадзіраванне, ітэратыўны код, шматпарогавае дэкадзіраванне, надзейнасць перадачы, цэласнасць інфармацыі, памылка, сістэма перадачы.

Мэта працы: распрацоўка і даследаванне метадаў пераўтварэння інфармацыі на аснове тэорыі залішняга кадзіравання для забеспячэння цэласнасці інфармацыі за кошт карэкцыі шматразовых памылак у сістэмах перадачы даных шляхам шматпарогавага дэкадзіравання ітэратыўных кодаў.

Метады даследавання. Даследаванні праводзіліся на аснове метадаў і палажэнняў тэорыі перашкодаўстойлівага кадзіравання даных, метадаў эксперыментальнага мадэліравання.

Атрыманыя вынікі і іх навізна. У працы абгрунтавана, што найболей простым у рэалізацыі, хуткадзейным і надзейным спосабам забяспечыць цэласнасць перадаваемай інфармацыі з'яўляецца ўжыванне метаду шматпарогавага дэкадзіравання трохмерных ітэратыўных кодаў у сістэмах перадачы інфармацыі. Распрацаваны канструкцыі і даследаваны ўласцівасці трохмерных ітэратыўных кодаў, якія адрозніваюцца ад вядомых ітэратыўных кодаў павялічанай мінімальнай кодавай адлегласцю, за кошт павелічэння колькасці праверак на цотнасць, што дазваляе павялічыць надзейнасць перадачы даных. Распрацаваныя трохмерныя ітэратыўныя коды разам са шматпарогавым дэкодэрам эфектыўна выпраўляюць шматразовыя незалежныя і згрупаваныя памылкі. Прапанавана мадыфікацыя шматпарогавага дэкодэра, якая дазваляе скараціць час дэкадзіравання, за кошт скарачэння ліку ітэратыўных дэкадзіравання. Распрацавана адаптыўная сістэма кадзіравання/дэкадзіравання даных на аснове прапанаваных трохмерных ітэратыўных кодаў і метаду шматпарогавага дэкадзіравання з магчымасцю дынамічнай змены параметраў выкарыстаных кодаў і вызначэння параметра BER якасці канала сувязі ў рэжыме без адключэння сувязі.

Рэкамендацыі па выкарыстанні. Вынікі дысертацыі ўкаранёны і выкарыстоўваюцца ў навучальным працэсе БДТУ, пры распрацоўцы камутатара Ethernet П-215 шыфр «Вектар» на ААТ «АГАТ-СІСТЭМ кіруючай кампаніі холдынгу «Сістэмы сувязі і кіравання».

Галіна выкарыстання: інфармацыйная бяспека.

РЕЗЮМЕ

Кудлацкая Марина Федоровна

МНОГОПороГОВОЕ ДЕКОДИРОВАНИЕ БИНАРНЫХ ИЗБЫТОЧНЫХ КОДОВЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ В СИСТЕМАХ ПЕРЕДАЧИ ИНФОРМАЦИИ

Ключевые слова: помехоустойчивое кодирование, итеративный код, многопороговое декодирование, надежность передачи, целостность информации, ошибка, система передачи.

Цель работы: разработка и исследование методов преобразования информации на основе теории избыточного кодирования, предназначенных для обеспечения целостности информации за счет коррекции многократных ошибок в системах передачи данных путем многопорогового декодирования итеративных кодов.

Методы исследования. Исследования проводились на основе методов и положений теории помехоустойчивого кодирования данных, методов экспериментального моделирования.

Полученные результаты и их новизна. В работе обосновано, что наиболее простым в реализации, быстросдействующим и надежным способом обеспечить целостность передаваемой информации является применение метода многопорогового декодирования трехмерных итеративных кодов в системах передачи информации. Разработаны конструкции и исследованы свойства трехмерных итеративных кодов, отличающихся от известных итеративных кодов увеличенным минимальным кодовым расстоянием за счет увеличения числа проверок на четность, что позволяет повысить надежность передачи данных. Разработанные трехмерные итеративные коды совместно с многопороговым декодером эффективно исправляют многократные независимые и группирующиеся ошибки. Предложена модификация многопорогового декодера, позволяющая сократить время исправления ошибок за счет сокращения числа итераций декодирования. Разработана адаптивная система кодирования/декодирования данных на основе предлагаемых трехмерных итеративных кодов и метода многопорогового декодирования с возможностью динамического изменения параметров используемых кодов и определения параметра качества канала связи BER в режиме без отключения связи.

Рекомендации по использованию. Результаты диссертационной работы внедрены и используются в учебном процессе БГТУ, при разработке коммутатора Ethernet П-215 шифр «Вектор» на ОАО «АГАТ-СИСТЕМ - управляющей компании холдинга «Системы связи и управления».

Область применения: информационная безопасность.

SUMMARY

Kudlatskaya Marina Fedorovna

MULTITHRESHOLD DECODING OF BINARY REDUNDANT CODE SEQUENCES IN COMMUNICATION SYSTEMS

Keywords: noiseproof coding, iterative code, multithreshold decoding, transmission reliability, information integrity, error, communication system.

Objective: development and research of methods for the transformation of information based on redundant coding theory, designed to ensure data integrity by correcting multiple errors in data transmission systems by multithreshold decoding of iterative codes.

Methods. Researches were conducted on the basis of methods and provisions of the noiseproof coding theory of data, methods of experimental modeling.

Obtained results and their novelty. It is proved in work that the most simple to implement, fast and reliable way to ensure the integrity of the transmitted information is to use the method multithreshold decoding three-dimensional iterative codes in data transmission systems. Constructions are developed and the properties of three-dimensional iterative codes different from known iterative codes by the increased minimum code distance, at the expense of increase in number of checks at parity that allows to increase reliability of data transmission are investigated. The developed three-dimensional iterative codes, together with multithreshold decoder effectively corrects multiple independent and packet errors. The modification of multithreshold decoder that reduces the decoding time, by reducing the number of decoding iterations is proposed. The adaptive system of data coding/decoding based on proposed three-dimensional iterative codes and multithreshold decoding method that allow to dynamically change the parameters of used codes and determining the quality parameter BER of a communication channel at the mode without turning off the connection is developed.

Recommendations for application. Results of dissertation work are introduced and are used in educational process of BSTU, in development the Ethernet P-215 switchboard the code "Vector" on OJSC "AGAT-SYSTEM" – Management Company of "Communication and Control Systems" Holding.

Scope: information protection.

Научное издание

Кудлацкая Марина Федоровна

**МНОГОПороГОВОЕ ДЕКОДИРОВАНИЕ БИНАРНЫХ ИЗБЫТОЧНЫХ
КОДОВЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ В СИСТЕМАХ ПЕРЕДАЧИ
ИНФОРМАЦИИ**

АВТОРЕФЕРАТ

диссертации на соискание ученой степени
кандидата технических наук

по специальностям 05.13.19 – Методы и системы защиты информации,
информационная безопасность, 05.12.13 – Системы, сети и устройства
телекоммуникаций

Подписано в печать . Формат 60×84 1/16. Бумага офсетная. Гарнитура «Таймс».
Отпечатано на ризографе. Усл. печ. л. . Уч.-изд. л. . Тираж 60 экз. Заказ .

Издатель и полиграфическое исполнение: учреждение образования
«Белорусский государственный университет информатики и радиоэлектроники».
Свидетельство о государственной регистрации издателя, изготовителя,
распространителя печатных изданий №1/238 от 24.03.2014,
№2/113 от 07.04.2014, №3/615 от 07.04.2014.
ЛП №02330/264 от 14.04.2014.
220013, Минск, П. Бровки, 6

