

На правах рукописи



Семин Дмитрий Сергеевич

**УНИВЕРСАЛЬНОЕ УСТРОЙСТВО
ПОМЕХОУСТОЙЧИВОГО КОДИРОВАНИЯ, АДАПТИВНОЕ К
ИЗМЕНЕНИЮ УСЛОВИЙ ФУНКЦИОНИРОВАНИЯ
РАДИОСИСТЕМЫ ПЕРЕДАЧИ ИНФОРМАЦИИ**

Специальность: 05.12.04

«Радиотехника, в том числе системы и устройства телевидения»

Автореферат

диссертации на соискание ученой степени
кандидата технических наук

Рязань 2013

Работа выполнена в ФГБОУ ВПО «Рязанский государственный радиотехнический университет» на кафедре радиоправления и связи

Научный руководитель: **Кириллов Сергей Николаевич**
доктор технических наук, профессор,
заведующий кафедрой радиоправления и связи
ФГБОУ ВПО «РГРТУ», г. Рязань

Официальные оппоненты: **Ручкин Владимир Николаевич**
доктор технических наук, профессор
кафедры информатики и вычислительной техники
ФГБОУ ВПО «РГУ им. С.А. Есенина», г. Рязань

Малинин Юрий Илларионович
кандидат технических наук, доцент
кафедры автоматизированных систем управления,
ФГБОУ ВПО «РГРТУ», г. Рязань

Ведущая организация: Рязанское региональное отделение Центрального
филиала ОАО «МегаФон», г. Рязань

Защита состоится «13» декабря 2013 г. В 11 часов на заседании диссертационного совета Д 212.211.04 в ФГБОУ ВПО «РГРТУ» по адресу: 390005, г. Рязань, ул. Гагарина, д. 59/1.

С диссертацией можно ознакомиться в библиотеке ФГБОУ ВПО «РГРТУ»

Автореферат разослан « 8 » ноября 2013 г.

Ученый секретарь
диссертационного совета
доктор технических наук



Г.В. Овечкин

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Актуальность темы. В настоящее время широкое распространение получили наземные и спутниковые радиосистемы передачи информации (РСПИ), обеспечивающие устойчивость к действию различных помех при помощи помехоустойчивых кодов (ПК). Во многом это связано с появлением быстродействующей элементной базы, позволившей существенно уменьшить размеры приемо-передающих модулей, а также повысить помехоустойчивость систем за счет усложнения процедур формирования и обработки сигналов.

Возможность повышения помехоустойчивости цифровых РСПИ за счет использования ПК доказана в работах отечественных ученых: В.Д. Гоппы, Э.Л. Блоха, В.В. Зяблова, А.Е. Крука, В.В. Золотарева, и зарубежных: К. Шеннона, Э. Хэмминга, И. Рида, Э. Соломона, Р.С. Боуза, Д.К. Рэй-Чоудхори, А. Хоквенгема, Р. Галагера, Р. Блейхута, Т. Касами и др.

В реальных условиях в радиоканалах могут действовать импульсные, узкополосные, структурные и другие типы помех. При этом характеристики радиоканала динамически изменяются с течением времени, что приводит к недостаточно эффективному использованию пропускной способности системы в случае, если параметры РСПИ выбираются однократно, без возможности их адаптации к условиям функционирования. Однако вопросы анализа устойчивости алгоритмов кодирования и декодирования при действии различного рода помех, а также защищенности от несанкционированного доступа в настоящее время недостаточно проработаны.

По этой причине при построении многофункциональных адаптивных РСПИ возникает проблема разработки универсальных модулей, позволяющих обеспечить быструю перестройку при изменении условий функционирования, в частности кодовой скорости, длины кодового слова и т.п. В связи с этим целесообразно построение универсальных кодирующего и декодирующего устройств, обеспечивающих формирование и обработку кодированных потоков как можно большего набора ПК.

Таким образом, актуальной является задача разработки процедуры проектирования универсальной системы помехозащищенного кодирования, позволяющей по заданным параметрам РСПИ выбирать ПК, наиболее подходящие к условиям функционирования. При этом необходимо учитывать такие факторы, как допустимые отношение сигнал-шум, вероятность ошибки на выходе РСПИ, доступные вычислительные ресурсы приемопередающих устройств, возможные типы помех, действующих в радиоканале и др.

Цель и задачи работы. Целью диссертационной работы является разработка универсального устройства помехоустойчивого кодирования, действующего при изменении условий функционирования РСПИ, по заданным показателям качества.

Поставленная цель работы включает решение следующих задач:

- анализа ПК, применяемых в современных РСПИ;
- разработки универсального устройства кодирования, позволяющего формировать известные и неизвестные ПК при изменении условий функционирования РСПИ;

- разработки универсального алгоритма помехозащищенного кодирования, обеспечивающего устойчивость к действию помех и защиту передаваемой информации в РСПИ;

- анализа алгоритмов декодирования в интересах использования универсального декодера при изменении условий функционирования РСПИ;

- построения математической модели РСПИ, позволяющей производить исследования ПК при действии различных мешающих факторов;

- исследования устойчивости алгоритмов кодирования и декодирования ПК к действию помех различного типа;

- обоснования исходных данных и показателей качества, необходимых для разработки процедуры проектирования системы ПК;

- обоснования процедуры проектирования системы помехоустойчивого кодирования по заданным показателям качества при изменении условий функционирования РСПИ.

Методология и методы исследования. В диссертационной работе были использованы методы имитационного моделирования, математической статистики, методы линейного и динамического программирования, методы статистической радиотехники.

Научная новизна. В результате выполнения диссертационной работы были получены следующие новые научные результаты:

1 Обоснована структурная схема универсального устройства помехозащищенного кодирования, позволяющего формировать широкий класс циклических (коды БЧХ, РС, квадратично-вычетные, Голея, циклические LDPC, и др.), сверточных кодов, а также составных ПК, обеспечивающего защиту передаваемой информации со степенью стойкости более 10^9 ключей.

2 Разработан алгоритм адаптации системы помехоустойчивого кодирования к уровню помех в радиоканале передачи информации при заданной задержке передаваемых данных, обеспечивающий снижение вероятности ошибки в 2...16 раз.

3 Представлена модификация алгоритма списочного декодирования на базе синдромов, позволяющая сократить объем необходимой памяти от 1,3 до 3 и более раз, а также реализовать в параллельной форме до 99 % операций декодирования в интересах увеличения скорости вычислений.

4 Обоснована процедура проектирования системы помехоустойчивого кодирования, осуществляющая выбор кода по заданным показателям качества РСПИ при изменении условий функционирования и позволяющая увеличить пропускную способность радиоканала до 1,6 раза.

Теоретическая и практическая значимость полученных результатов заключается в использовании разработанных универсального помехозащищенного кодирующего устройства, а также процедуры проектирования системы помехоустойчивого кодирования в различных радиотехнических системах передачи информации.

Результаты, полученные в диссертационной работе, внедрены в ОАО «Российские космические системы».

Основные положения, выносимые на защиту

1 Универсальное устройство помехозащищенного кодирования, позволя-

ющее формировать широкий класс линейных кодов, обеспечивающее заданную степень устойчивости к действию различных помех и защищенность передаваемой информации на уровне не менее 10^9 ключей.

2 Алгоритм адаптации системы помехоустойчивого кодирования к уровню помех в канале передачи информации при заданной задержке передаваемых данных, обеспечивающий снижение вероятности ошибки в 2...16 раз.

3 Процедура проектирования устройства помехоустойчивого кодирования, позволяющая по заданным показателям качества осуществлять выбор помехоустойчивого кода и алгоритма декодирования при изменении условий функционирования радиосистемы передачи информации, обеспечивающая увеличение пропускной способности не менее чем в 1,6 раза.

Степень достоверности и апробация результатов. Достоверность результатов и выводов, полученных при выполнении исследований, проверена путем сопоставления с известными результатами, полученными в теории помехоустойчивого кодирования.

Результаты диссертационной работы были представлены на всероссийских научно-технических конференциях (ВНТК) и международных научно-технических конференциях (МНТК): МНТК и выставка «Цифровая обработка сигналов и ее применение» (г. Москва 2009, 2010, 2011, 2012); МНТК с элементами научной школы молодежи «Биотехнические, медицинские и экологические системы и комплексы» (г. Рязань 2009, 2011); МНТК «Перспективные технологии в средствах передачи информации» (г. Рязань 2009, 2010, 2011, 2012); ВНТК «Информационные и телекоммуникационные технологии. Подготовка специалистов для инфокоммуникационной среды»; ВНТК «Новые информационные технологии в научных исследованиях и в образовании. Всероссийская научно-техническая конференция студентов, молодых ученых и специалистов» (Рязань 2010); ВНТК «Проблемы передачи и обработки информации в сетях и системах телекоммуникаций» (г. Владимир 2011, 2013); ВНТК «Актуальные проблемы ракетно-космического приборостроения и информационных технологий» (г. Москва 2010, 2011, 2012).

Структура и объем работы. Диссертационная работа состоит из введения, трех глав, заключения, списка литературы, включающего 102 наименования, содержит 197 стр., в том числе 131 стр. основного текста, 15 таблиц и 94 рисунка.

Публикации. По теме диссертации опубликовано 28 работ. Из них 4 статьи опубликовано в изданиях, рекомендуемых ВАК РФ, 2 статьи в межвузовских сборниках и 22 работы в материалах международных и всероссийских конференций.

СОДЕРЖАНИЕ РАБОТЫ

Во введении обоснована актуальность работы, определены цель и решаемые задачи. Представлены методика и методология проведенных исследований, основные положения, выносимые на защиту, степень достоверности и апробация результатов, а также структура и объем работы.

В первой главе проведен анализ алгоритмов ПК, применяемых в современных системах РСПИ, а также технологии Soft Definition Radio (SDR), позво-

ляющей программно изменять систему кодирования. Показано, что в большинстве современных наземных стандартов применяются как блочные коды (БК), так и сверточные коды (СК) различных типов и параметров. При этом использование того или иного ПК обусловлено множеством различных факторов: исправляющей способностью кода, наличием эффективного, реализуемого на практике алгоритма декодирования, доступными в приемно-передающих устройствах вычислительными и энергетическими ресурсами, допустимой задержкой информационного потока, необходимой для кодирования и декодирования и др.

Помехоустойчивые коды, получившие наиболее широкое распространение в РСПИ, можно разделить на пять основных групп: БК, которые включают в себя класс циклических кодов (РС, БЧХ, и др.) и нециклических (в частности коды с малым числом проверок на четность, в англоязычной литературе Low Density Parity Check – LDPC), СК, составные коды (последовательно декодируемые коды и турбо-коды), сигнально-кодовые конструкции или решетчатое кодирование (Trellis coded modulation – TCM). При этом основной тенденцией развития структуры радиопередающих систем является переход к турбо-кодам и сигнально-кодовым конструкциям.

На основе проведенного анализа структур различных ПК обосновано универсальное кодирующее устройство (рисунок 1), позволяющее формировать блочные, сверточные и составные ПК, а также обеспечивающее перемежение и защиту информационного потока путем изменения своих коэффициентов.

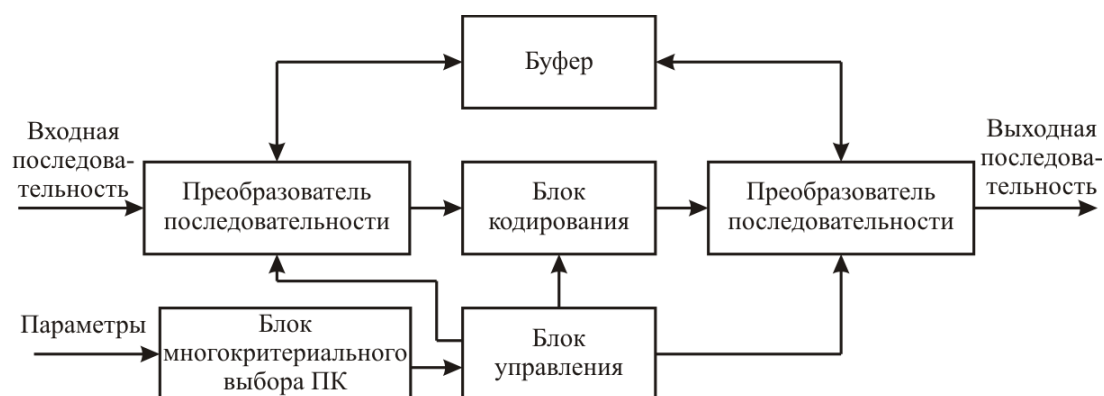


Рисунок 1

На рисунке 1 входной преобразователь последовательности осуществляет подготовку входной последовательности к кодированию (разбиение на кадры), выходной – преобразует поток данных, полученный на выходе блока кодирования. Блок кодирования путем изменения своих коэффициентов выполняет процедуру вычисления проверочных символов. Буфер необходим для работы преобразователя последовательности, а также для повторного кодирования данных при формировании составных кодов. Общая настройка и управление схемой осуществляются при помощи блока управления. В случае использования универсального кодера, в составе адаптивной РСПИ также необходим блок многокритериального выбора ПК, осуществляющий вычисление типа и параметров кода в соответствии с заданными показателями качества.

Увеличение защищенности информационного потока может производиться одновременно с процедурой помехоустойчивого кодирования в блоке кодирования. Прямое и обратное преобразования алгоритма защиты информации $\bar{v} = F_{cr}(\bar{u})$ и $\bar{u} = F_{cr}^{-1}(\bar{v})$ могут быть записаны аналогично разностным уравнениям цифрового фильтра, заданного в поле Галуа, в следующем виде:

$$\bar{w} = F_{cr}(\bar{y}) \Leftrightarrow \begin{cases} w'_i = a_0(y_i) + \sum_{j=1}^p a_j(w'_{i-j}), \\ v_i = b_0(v'_i) + \sum_{j=1}^p b_j(v'_{i-j}), \end{cases} \quad (1)$$

$$\bar{y} = F_{cr}^{-1}(\bar{w}) \Leftrightarrow \begin{cases} w_i = a_0^{-1}(w'_i) - \sum_{j=1}^p a_j(w'_{i-j}), \\ w'_i = b_0^{-1}(y_i) - \sum_{j=1}^p b_j(y'_{i-j}), \end{cases} \quad (2)$$

где $\bar{y} = (y_0, y_1, \dots, y_n)$, $\bar{w}' = (w'_0, w'_1, \dots, w'_n)$, $\bar{w} = (w_0, w_1, \dots, w_n)$ – соответственно входной, промежуточный и выходной векторы длиной n , $a_j(x), b_j(x)$, $j = \overline{0, p}$ – арифметические функции кодирующего устройства (для линейных фильтров имеют вид $a_j(x) = A_j x$; $b_j(x) = B_j x$, где A_j, B_j – заданные коэффициенты). $a_0^{-1}(x), b_0^{-1}(x)$ – функции, обратные к $a_0(x), b_0(x)$, то есть $a_0^{-1}(a_0(x)) = x$. Все арифметические операции и числа задаются в соответствии с полем Галуа в котором определен ПК. Помехозащищенное кодирование выполняется с использованием функции (1) в два этапа. На первом этапе значения коэффициентов $\{A_j, B_j\}$ изменяются по закону псевдослучайной последовательности, формируемой на базе заданного ключа, обеспечивая защиту потока данных. На втором этапе коэффициенты $\{A_j, B_j\}$ устанавливаются в соответствии с выбранным ПК, обеспечивая внесение избыточности. Декодирование также производится в два этапа: на первом – исправляются ошибки, произошедшие в канале, на втором – выполняется восстановление исходной информации с использованием функции (2).

Проведенное имитационное моделирование предложенного алгоритма помехозащищенного кодирования для модели канала с аддитивным белым гауссовским шумом (АБГШ) показало, что применение алгоритма защиты передаваемой информации при повышении скрытности до 10^{38} ключей приводит к снижению помехоустойчивости системы ПК не более чем на 0,7 дБ при вероятности необнаруживаемой ошибки менее 10^{-5} . В качестве примера в таблице 1 представлены зависимости величины энергетических потерь Δq для некоторых ПК, использованных при моделировании. Результаты имитационного моделирования показали, что величина энергетического проигрыша для блочных кодов напрямую зависит от длины информационной части ПК, а, следовательно, увеличивается с увеличением длины кодового слова при одной и той же кодовой скорости. Для сверточных и составных кодов, используемых при модели-

Таблица 1

№	Название ПК и параметры	Δq , дБ
1	БЧХ(63, 30)	0,28
2	БЧХ(127, 64)	0,32
3	БЧХ(255, 131)	0,33
4	РС(63, 33)	0,31
5	РС(127, 65)	0,3
6	РС(255, 129)	0,4
7	Сверточный код ДКО 7 скорость 1/2	0,7
8	Сверточный код ДКО 7 скорость 2/3	0,7
9	Составной РС(127,111) + сверточный ДКО 7 ско- рость 3/4	0,4
10	Составной РС(127,111) + сверточный длина кодово- го ограничения 7 кодовая скорость 2/3	0,4
11	Составной РС(127,111) + сверточный длина кодово- го ограничения 7 кодовая скорость 11/19	0,4

мерно 30% ширины спектра основного лепестка полезного радиосигнала при различных смещениях относительно центральной частоты, структурной помехи в виде ФМн-2 сигнала с параметрами, близкими к полезному радиосигналу, импульсной помехи, со средней длительностью импульса, равной десяти символам модулированного сигнала, а также аддитивного белого гауссовского шума (АБГШ).

Имитационное моделирование производилось для БЧХ, РС, сверточных и составных – РС+сверточных кодов. В качестве критерия, отображающего устойчивость ПК к действию помех, была использована величина $P_{ош} / P_{ошк}$ (отношение вероятности необнаруживаемой ошибки после декодирования $P_{ош}$ к вероятности ошибки в радиоканале передачи данных $P_{ошк}$), характеризующая исправляющую способность кода для заданного распределения ошибок. Уменьшение значения отношения $P_{ош} / P_{ошк}$ при фиксированной вероятности ошибки в канале $P_{ошк}$ характеризует исправляющую способность ПК. В качестве примера на рисунке 2 показаны зависимости $P_{ош} / P_{ошк}$ от $P_{ошк}$ для кода БЧХ(127,64) при воздействии импульсной, структурной и узкополосной помех, а также АБГШ. Показано, что исправляющая способность анализируемых кодов существенно зависит от распределения ошибок в канале передачи данных, возникающих при действии различных типов помех. При этом наиболее силь-

ровании, величина энергетического проигрыша не зависит от кодовой скорости.

Показано также, что предложенное универсальное помехозащищенное кодирующее устройство помимо известных ПК позволяет формировать новые неизученные типы кодов.

С целью анализа возможности адаптации РСПИ за счет выбора типа и параметров ПК, наиболее устойчивого к действию мешающих факторов, была разработана имитационная модель радиотракта. Исследования предложенной модели производились для радиолинии с ФМн-2 сигналами при действии различных шумов и помех в условиях идеальной синхронизации передатчика и приемника. Для анализа ПК были реализованы модели узкополосной помехи с шириной полосы, равной при-

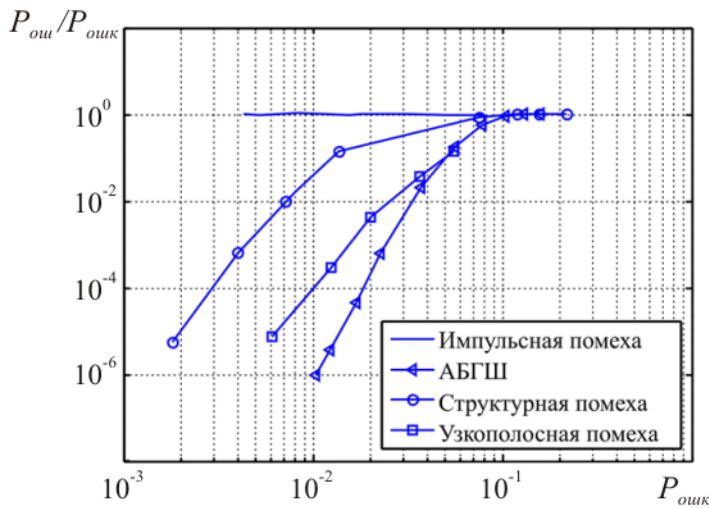


Рисунок 2

ное влияние на кодированный поток при вероятности ошибки в радиоканале $P_{ошк} = 10^{-2}$ независимо от используемого ПК оказывает импульсная помеха (отношение $P_{ош} / P_{ошк}$ больше на порядок по сравнению со структурной помехой), второй по степени воздействия является структурная помеха ($P_{ош} / P_{ошк}$ выше на два порядка по сравнению с узкополосной помехой), третьей – узкополосная помеха ($P_{ош} / P_{ошк}$ выше

на порядок по сравнению с АБГШ) и наименьшее воздействие оказывает АБГШ. Показано, что среди анализируемых ПК наиболее эффективным при воздействии помех рассмотренных типов является код РС, при действии структурных помех сверточные и БЧХ коды сравнимы по помехоустойчивости с данным типом ПК. Составные коды, образованные с использованием сверточного кода и ПК РС(127,111), при действии структурной и узкополосной помех обладают одинаковой исправляющей способностью и являются наименее помехоустойчивыми из всех рассмотренных типов ПК.

Для проведения адаптации системы помехоустойчивого кодирования РСПИ необходимы алгоритмы, позволяющие определять оптимальные параметры кодера и декодера по оценке характера и распределения шумов и/или помех, действующих в радиоканале. При этом в качестве изменяющихся параметров могут выступать: длина кодового слова (для блочных кодов), длина кодового ограничения (для сверточных кодов); кодовая скорость; глубина перемежения.

В предложенной процедуре адаптации системы ПК производится вычисление параметров помехоустойчивого кодера и перемежителя, обеспечивающих максимальную пропускную способность при заданной задержке передаваемых данных. При этом на первом этапе по дисперсии сигнала на выходе демодулятора производится грубая оценка вероятности ошибки в радиоканале. На втором этапе по известной вероятности ошибки выбираются ПК, способные исправить текущее число ошибок $t_{нкi}$ при длине кодового слова ПК $n_{нкi} \geq t_{нкi} / P_{ош}$, где $P_{ош}$ – оценка вероятности ошибки. На третьем этапе производится выбор ПК, параметры которого максимизируют значение кодовой скорости $r_{нкi} = k_{нкi} / n_{нкi}$ при заданной задержке сигнала $\Delta N_i = n_{нкi} / n_{нк\max}$:

$$r_{нкi} - a\Delta N_i \rightarrow \max_i, \quad (3)$$

для $i = \overline{1, N_C}$, где N_C – общее число ПК, используемых при адаптации, $n_{нк\max}$ – максимально возможная длина кодового слова, $a \in [0,1]$ – параметр, определя-

ющий вес задержки сигнала при декодировании (0 – задержка по времени не имеет значения для РСПИ, 1 – задержка имеет максимальное значение).

Проведенное имитационное моделирование известной РСПИ при действии АБГШ и узкополосной помехи показало, что применение критериев (3) и (4) для выбора параметров системы ПК позволило снизить вероятность ошибки с уровня $1,1 \times 10^{-4}$ до уровня $6,7 \times 10^{-6}$ при использовании блочного перемежителя и кодов РС.

Таким образом, в первой главе обоснована структура универсального помехоустойчивого кодирующего устройства, проведены исследования устойчивости ПК при действии различных помех, а также предложен алгоритм адаптации, позволяющий производить выбор параметров ПК при изменении уровня помех.

Во второй главе проведен анализ возможности использования универсальных алгоритмов декодирования в интересах построения адаптивных РСПИ. Представлено сравнение данных алгоритмов по вычислительным затратам, необходимым для практической реализации. Среди универсальных алгоритмов были рассмотрены: алгоритм декодирования по максимуму апостериорной вероятности, списочный алгоритм декодирования на базе синдромов, алгоритм декодирования на базе упорядочивания статистики, а также алгоритм декодирования на базе минимальных кодовых слов.

Алгоритм декодирования по максимуму апостериорной вероятности является оптимальным алгоритмом декодирования для всех известных ПК с «мягким» входом и «мягким» выходом, позволяющим минимизировать апостериорную вероятность ошибки символов кодового слова. Преимуществами данного алгоритма декодирования являются оптимальность получаемого решения и возможность формирования «мягких» решений. Недостатками являются: высокие вычислительные затраты, экспоненциально зависящие от длины кодового ограничения для СК или числа информационных символов для БК, необходимость построения и хранения решетки состояний кодера для каждого из ПК, приводящая к значительным затратам памяти при практической реализации в РСПИ, использующих адаптацию или поддержку разных протоколов передачи информации. Анализ показал, что для реализации алгоритма требуется около $O_n = 9 \cdot 2^{k_{нк}-1} n_{нк}$ (для БК), $O_n = n_{нк} 9 \cdot 2^{d_{нк}-1}$ (для СК) элементарных операций и не более $M_n = 2^{n_{нк}-k_{нк}} n_{нк}$ (для БК), $M_n = 2^{d_{нк}} n_{нк}$ (для СК) ячеек памяти, где $d_{нк}$ – длина кодового ограничения СК.

Показано, что списочный алгоритм декодирования является оптимальным для блочных кодов и неоптимальным для сверточных, при этом позволяет использовать «жесткий» и «мягкий» вход. Применение принципа исправления ошибок в принятом кодовом слове по синдрому возможно только для линейных кодов. К достоинствам данного алгоритма декодирования относятся малые вычислительные затраты в сравнении с другими алгоритмами декодирования с «мягким» входом, оптимальность получаемого решения для блочных ПК, а также возможность быстрой перестройки между ПК. Недостатками алгоритма являются: необходимость построения списка для каждого из ПК, используемых в РСПИ, большие затраты памяти, неоптимальность получаемого решения,

в случае если список соответствия синдромов и векторов ошибок не является достаточно полным. Анализ показал, что для реализации алгоритма требуется около $O_n = 2n_{nk}k_{nk} + n_{nk}^2$ элементарных операций и не более $M_n = 2^{n_{nk}-k_{nk}}$ ячеек памяти.

Квазиоптимальный алгоритм декодирования на базе упорядочивания статистики основан на выделении из кодового слова ПК наиболее надежных символов и дальнейшем поиске кодовых векторов, наиболее близких к принятому. Применим для любых видов линейных бинарных и небинарных БК. Достоинством данного декодера является то, что при длине кодового слова более 150 символов данный алгоритм требует наименьшего числа операций в сравнении со всеми рассмотренными выше алгоритмами. Недостатком является неоптимальность получаемого на выходе решения. Анализ показал, что для реализации алгоритма требуется около $O_n = n_{nk}^2 + k_{nk}n_{nk}^2 + 2n_{nk}k_{nk} + 5n_{nk}$ элементарных операций и не более $M_n = 2n_{nk}k_{nk} + 4n_{nk}$ ячеек памяти.

Принцип работы алгоритма декодирования на базе минимальных кодовых слов сходен с градиентными методами оптимизации: на каждой итерации производится переход из одного разрешенного кодового слова в другое, до тех пор, пока не будет найдено кодовое слово, наиболее близко расположенное к принятой кодовой комбинации. Переход по решетке разрешенных состояний осуществляется путем добавления к текущему вектору одного из векторов, принадлежащих множеству минимальных кодовых слов. Минимальные кодовые слова формируются как кодовые комбинации, обладающие весом Хэмминга, равным расстоянию между наиболее близкими кодовыми словами. Алгоритм применим только для линейных бинарных и небинарных БК, так как использует свойство коммутативности пространства разрешенных кодовых слов. Достоинством данного алгоритма является значительно меньший объем памяти, требуемый для хранения минимальных кодовых слов, в сравнении со списочным алгоритмом декодирования. Недостатками являются необходимость предварительного расчета и хранения на приемной стороне для каждого ПК множества минимальных кодовых слов, а также неоптимальность получаемых решений для некоторых типов кодов. Анализ показал, что для реализации алгоритма требуется около $O_n = n_{nk}C_{k_{nk}}^{d_{\min}}$ элементарных операций и не более $M_n = 3n_{nk}C_{k_{nk}}^{d_{\min}}$ ячеек памяти, где $d_{\min}$ – минимальное расстояние Хэмминга между наиболее близкими кодовыми словами.

Проведенное сравнение представленных алгоритмов показало, что полностью универсальными, а также обеспечивающими наибольший эквивалентный энергетический выигрыш Δq являются алгоритм декодирования по максимуму апостериорной вероятности и списочный алгоритм. В качестве примера в таблице 2 представлены значения отношения сигнал-шум q в радиоканале и Δq при которых алгоритмы декодирования обеспечивают вероятность ошибки равную $P_{ош} = 10^{-5}$ для кода БЧХ(63,51).

Кроме того, показано, что по исправляющей способности наиболее эффективен алгоритм декодирования по максимуму апостериорной вероятности, так

Таблица 2

№ п\п	Название ПК	q , дБ	Δq , дБ
1	Алгоритм декодирования по максимуму апостериорной вероятности	3,8	5,8
2	Списочный алгоритм декодирования с «мягким» входом	3,8	5,8
3	Алгоритм на базе упорядочивания статистики	4	4,7
4	Алгоритм на базе минимальных кодовых слов	8	1,6

как данный алгоритм является устойчивым к действию узкополосных и структурных помех, а в случае действия импульсных помех целесообразно использовать перемежитель.

Произведена модификация списочного алгоритма декодирования, которая позволила за счет увеличения числа элементарных операций значительно снизить объем необходимой памяти, а также реализовать параллельную структуру

декодирующего устройства в интересах увеличения скорости вычислений. Применение предложенного алгоритма позволило уменьшить затраты памяти для кода БЧХ(127,113) в 1,3 раза и для кода БЧХ(63, 51) в 3 раза.

Алгоритм списочного декодирования и алгоритм на базе упорядочивания статистики сравнимы по порядку требуемого числа элементарных операций при длинах кодового слова более 150 символов, при этом для списочного алгоритма необходим больший объем памяти. Например, для декодирования ПК БЧХ(63,51) списочный алгоритм декодирования требует в 20 раз меньшего числа операций и в 1,6 раз меньшего объема памяти. Наиболее эффективным по суммарному объему затрачиваемой памяти и числу элементарных операций является алгоритм декодирования на базе упорядочивания статистики. Наименее эффективным суммарно по помехоустойчивости и необходимым вычислительным ресурсам является алгоритм декодирования на базе минимальных кодовых слов, требующий больших объемов вычислительных ресурсов и проигрывающий по помехоустойчивости всем представленным алгоритмам до 4,2 дБ.

Исходя из вышеизложенного, можно сделать следующий вывод: при использовании в РСПИ как БК, так и СК с различными параметрами эффективным является использование алгоритма декодирования по максимуму апостериорной вероятности и списочного алгоритма декодирования, а в случае сокращения класса ПК возможно использование алгоритма на базе упорядочивания статистики.

В третьей главе производится обоснование процедуры проектирования системы помехоустойчивого кодирования по заданным показателям качества. Для этого проведен анализ исходных данных, необходимых для построения алгоритма проектирования и представлено обоснование показателей качества, позволяющих произвести выбор ПК по исходным данным, а также разработана структурная схема алгоритма проектирования системы помехоустойчивого кодирования и приведен пример работы предложенной процедуры.

Входные данные алгоритма проектирования можно разделить на две группы – это технические требования, предъявляемые к РСПИ, а также набор ПК и алгоритмов декодирования из которых производится выбор системы ПК. К техническим требованиям, которые могут быть предъявлены к РСПИ при про-

ектировании, отнесены: доступная ширина полосы частот ΔF_s , оценка минимального отношения сигнал-шум в канале q_k , максимально допустимая вероятность ошибки потока данных на выходе канального уровня РСПИ $P_{ош\ доп}$, скорость передачи данных r_d , максимальная задержка сигнала ΔT_s при декодировании, степень защищенности и скрытности информационного потока, вычислительные ресурсы, доступные для проведения цифровой обработки сигналов в кодере и декодере.

Для выбора системы ПК должны быть определены следующие исходные данные: параметры ПК, необходимые для формирования кода, кодовая скорость ПК $r_{нк\ j}$, длина кодового блока, защищенность. зависимости вычислительных затрат, устанавливающие взаимосвязь между длиной декодируемого блока и числом элементарных операций, а также объемом необходимой памяти.

Процедура проектирования системы ПК включает два основных шага: на первом производится отбор кодов, удовлетворяющих исходным данным, а на втором по методу последовательного применения критериев производится выбор ПК по заданным показателям качества.

Для перечисленных выше данных была обоснована процедура проектирования, включающая выбор ПК по следующим показателям качества:

- 1 Кодовой скорости, определяющей избыточность кодированного потока.
- 2 Исправляющей способности ПК, определяющей возможности кода и алгоритма декодирования устранять ошибки из информационного потока данных при действии различных шумов и помех.
- 3 Задержки, вносимой в сигнал системой ПК, зависящей от длины кодового блока.
- 4 Скрытности ПК, характеризующей степень структурной скрытности информации, переданной с использованием данного кода.

5 Вычислительной сложности помехоустойчивого кодера, определяемой оценкой числа элементарных операций и объема памяти, необходимых для выполнения процедуры декодирования.

Для предложенной процедуры проектирования системы ПК приведен пример работы со следующими исходными данными: минимально допустимая скорость передачи данных 512 кбит/с; максимальная скорость передачи данных 1024 кбит/с; вид модуляции ФМн-2; максимальная вероятность ошибки, допустимая при передаче данных, $P_{ош\ max} = 10^{-7}$; максимальная задержка сигнала $\Delta T_s = 10$ мс. При этом был задан следующий сценарий изменения параметров радиоканала:

- в течение всего времени сеанса передачи данных в канале действует АБГШ на уровне 20 дБ;
- в течение 25% времени действует узкополосная помеха при отношении сигнал - помеха 20 дБ;
- в течение 25% уровень узкополосной помехи в канале достигает значения 15 дБ.

По результатам работы представленной процедуры для указанных исходных данных получены следующие параметры ПК:

- при действии АБГШ на уровне 20 дБ выбран ПК БЧХ(255, 231);
- при действии узкополосной на уровне 20 дБ выбран ПК БЧХ(63, 57);
- при действии узкополосной помехи на уровне 15 дБ выбран сверточный ПК с длиной кодового ограничения 8 и кодовой скоростью $1/2$.

Показано, что если производится перестроение параметров ПК в режиме реального масштаба времени при изменении условий функционирования РСПИ в соответствии с полученными рекомендациями, то выигрыш по кодовой скорости составит 1,6 раза в сравнении системой, использующей один фиксированный ПК.

В заключении диссертационной работы представлены основные результаты разработки процедуры проектирования системы ПК по заданным показателям качества, позволяющей осуществить выбор помехоустойчивого кода и алгоритма декодирования, удовлетворяющих исходным данным. При решении данной задачи в диссертационной работе получены следующие результаты:

1 Проведен анализ ПК, применяемых в современных РСПИ, и обоснована структура универсального кодирующего устройства, позволяющего формировать широкий класс циклических (коды БЧХ, РС, квадратично-вычетные, Голея, циклические LDPC, и др.) и сверточных кодов, а также составных ПК.

2 Предложен алгоритм увеличения защищенности информации на базе универсального кодирующего устройства, позволяющий обеспечить защищенность потока с заданной степенью стойкости (не менее 10^9 ключей). Проведенное имитационное моделирование показало, что увеличение защищенности информационного потока не менее чем на 10^9 ключей приводит к снижению помехоустойчивости (увеличению вероятности ошибки на выходе) не более чем на 0,7 дБ (при вероятности необнаруживаемой ошибки 10^{-5}).

3 Разработана имитационная модель анализа систем помехоустойчивого кодирования при действии узкополосных структурных и импульсных шумов в канале передачи данных. Проведены исследования по анализу устойчивости ПК к действию различных помех. Показано, что по степени воздействия на кодированный поток независимо от типа кодов мешающие сигналы можно упорядочить следующим образом – импульсная помеха, узкополосная помеха, структурная помеха, АБГШ. Наиболее устойчивыми к действию помех рассмотренных типов являются коды РС, при этом к действию структурных помех также устойчивы БЧХ и сверточные ПК. Использование блочного перемежителя позволило уменьшить число ошибок примерно на два порядка при действии импульсных помех и примерно на один порядок при действии узкополосных. Совместное использование кода РС (127, 65) и операции перемежения при воздействии импульсных помех привело к увеличению среднего числа ошибок в 2,7 раза, а при воздействии узкополосных помех – к снижению вероятности ошибок в 1,2 раза, в сравнении со случаем без использования перемежения.

4 Для предложенного универсального устройства помехоустойчивого кодирования разработан алгоритм адаптации системы ПК, позволяющий производить оценку вероятности и распределения ошибок в потоке данных, а также выбирать параметры кодера и перемежителя по критерию минимизации задержки и максимизации кодовой скорости при заданной помехоустойчивости.

Показано, что дисперсия оценки вероятности ошибок в канале передачи данных не превосходит $1,3 \cdot 10^{-3}$ для моделей с АБГШ, узкополосными и импульсными помехами. Результаты моделирования показали, что предложенный алгоритм адаптации параметров перемежения позволил снизить вероятность ошибки с уровня $1,1 \times 10^{-4}$ до уровня $6,7 \times 10^{-6}$.

5 Проведен анализ универсальных алгоритмов декодирования ПК: алгоритма декодирования по максимуму апостериорной вероятности, применимого для линейных блочных и сверточных ПК; алгоритмов списочного декодирования с «жестким» и «мягким» входами, применимых для блочных и сверточных кодов; алгоритма декодирования на базе упорядочивания статистики, применимого для линейных блочных ПК; алгоритма декодирования на базе минимальных кодовых слов, применимого для линейных блочных ПК.

6 Представлены результаты имитационного моделирования алгоритмов декодирования для блочных и сверточных кодов с различными параметрами при прохождении сигнала через канал с АБГШ. Показано, что наименее эффективным по помехоустойчивости является алгоритм декодирования на базе минимальных кодовых слов, а наиболее устойчивыми алгоритмы списочного декодирования с «мягким» входом и алгоритм декодирования по максимуму апостериорной вероятности.

7 Показано, что алгоритм списочного декодирования и алгоритм на базе упорядочивания статистики сравнимы по порядку сложности числа элементарных операций, при этом списочный алгоритм требует существенно более высокого объема памяти. Наиболее эффективным по суммарному объему затрачиваемой памяти и числу элементарных операций является алгоритм декодирования на базе упорядочивания статистики при длинах кодового слова более 150 символов, однако он проигрывает оптимальным декодерам до 1,7 дБ. При меньших длинах кодовых слов наилучшим является списочный алгоритм декодирования с «мягким» входом. Например, для декодирования ПК БЧХ(63,51) списочный алгоритм декодирования требует в 20 раз меньше операций и в 1,6 раз меньше объема памяти в сравнении с алгоритмом декодирования на базе упорядочивания статистики. Для декодирования кода БЧХ(255, 123) алгоритм на базе упорядочивания статистики требует меньшего числа операций на 33 порядка и на 34 порядка меньше объема памяти.

8 Анализ наиболее помехоустойчивого алгоритма декодирования по максимуму апостериорной вероятности, используемого в составе турбо-декодеров, при действии помех различного типа показал, что данный алгоритм является неэффективным при действии импульсных помех. Это связано с тем, что декодер, построенный для АБГШ, при изменении статистических свойств помех формирует не правильное решение.

9 Предложен модифицированный списочный алгоритм декодирования, позволяющий за счет увеличения числа элементарных операций уменьшить требуемые размеры объемов памяти. Применение данного алгоритма позволило уменьшить затраты памяти для кода БЧХ(127,113) в 1,3 и для кода БЧХ(63, 51) в 3 раза за счет увеличения числа элементарных операций в сравнении со списочным алгоритмом декодирования на базе синдромов с «мягким» входом.

10 Обоснованы показатели качества ПК, характеризующие кодовую скорость, исправляющую способность, временную задержку на выходе декодера, скрытность и защищенность, вычислительную сложность, позволяющие производить проектирование системы помехоустойчивого кодирования РСПИ. Представлена процедура проектирования системы ПК по заданным показателям качества, использующая для выбора необходимого кода метод последовательного применения критериев.

11 Показан пример работы процедуры проектирования системы ПК по заданным показателям качества при изменении условий функционирования. Моделирование проводилось для сценария при котором в радиоканале в течение 50% времени действовала узкополосная помех с изменяющейся мощностью. При этом адаптация параметров ПК позволила увеличить пропускную способность РСПИ в 1,6 раза при изменении уровня помех в радиоканале, в сравнении со случаем без адаптации при использовании кода, с наибольшей корректирующей способностью.

СПИСОК ОСНОВНЫХ ПУБЛИКАЦИЙ ПО ТЕМЕ ДИССЕРТАЦИИ

1. Кириллов С.Н., Дмитриев В.Т., Семин Д.С., и др. Перспективные алгоритмы совместного помехоустойчивого кодирования и защиты в радиосистемах передачи информации. //11-я МНТК и выставка «ЦОС и ее применение». Выпуск IX-2 Москва, 2009. - С. 534-537.

2. Кириллов С.Н., Семин Д.С. Помехозащищенный кодер на основе БИХ-фильтра. Вестник РГРТУ 2009 № 2 (выпуск 27). - С. 27-30.

3. Кириллов С.Н., Семин Д.С. Помехозащищенное кодирование на основе БИХ фильтров. // 34-я ВНТК Информационные и телекоммуникационные технологии. Подготовка специалистов для инфокоммуникационной среды. Рязань 2009 - С.350-351.

4. Семин Д.С. Многофункциональный помехозащищенный кодер на основе БИХ-фильтров. // Новые информационные технологии в научных исследованиях и в образовании. XIV ВНТК студентов, молодых ученых и специалистов. Рязанский государственный радиотехнический университет. Рязань 2009. - С. 143-144.

5. Семин Д.С., Покровский П.С. Телемедицинские системы дистанционного мониторинга и диагностики самочувствия //Биотехнические, медицинские и экологические системы и комплексы. Биомедсистемы - 2009. Международная конференция с элементами научной школы молодежи. Рязань: РГРТУ, 2009. - С. 474-479.

6. Кириллов С.Н., Покровский П.С., Семин Д.С. Универсальный помехозащищенный тракт передачи информации // 12-я Международная конференция и выставка "ЦОС и ее применение - DSPA-2010", Москва, 2010. - С. 281-283.

7. Кириллов С.Н., Семин Д.С. Унифицированный алгоритм помехозащищенного кодирования //16-я МНТК Проблемы передачи и обработки информации в сетях и системах телекоммуникаций. Рязань 2010. - С. 95-96.

8. Семин Д.С. Адаптивный алгоритм помехозащищенного кодирования // Новые информационные технологии в научных исследованиях и образовании. НИТ-2010. XV ВНТК студентов, молодых ученых и специалистов. Рязань

2010.- С 138-139.

9. Семин Д.С., Ватутин В.И., Снегирев В.М., и др. Алгоритмы совместного помехоустойчивого кодирования и защиты информации в космических системах связи. Ракетно-космическое приборостроение и информационные технологии. 2009-2010. Труды II ВНТК "Актуальные проблемы ракетно-космического приборостроения и информационных технологий", 2009 г. / под. ред. Ю.М. Урличича, А.А. Романова. М.: Радиотехника, 2010. - 272 с. - С. 54-56.

10. Кириллов С.Н., Слесарев А.С., Покровский П.С., Семин Д.С. Реализация программно управляемого формирователя радиосигналов телекоммуникационных систем на основе прямого цифрового синтеза //13-я МНТК "ЦОС и ее применение DSPA -2011". Выпуск XIII - 2, Доклады. Москва. - С 267-270.

11. Кириллов С.Н., Ревуцкий В.А., Семин Д.С., и др. Алгоритм распознавания типа и параметров помехоустойчивых кодов. //13-я МНТК "ЦОС и ее применение DSPA -2011". Выпуск XIII - 2, Доклады. Москва. - С 30-33.

12. Семин Д.С. Универсальный алгоритм помехозащищенного кодирования на базе нелинейного преобразования в поле Галуа // Информационные технологии. Межвузовский сборник научных трудов. Рязань. 2011. - С. 133-136.

13. Семин Д.С., Кириллов С.Н., Ревуцкий В.А., Ватутин В.М., и др. Алгоритм распознавания типа и параметров помехоустойчивых кодов // Тезисы докладов IV ВНТК «Актуальные проблемы ракетно-космического приборостроения и информационных технологий» М.: Радиотехника - 2011. - С. 122-123.

14. Семин Д.С., Кириллов С.Н., Слесарев А.С., Покровский П.С., и др. Программно-управляемый формирователь радиосигналов космических систем передачи информации // Тезисы докладов IV ВНТК «Актуальные проблемы ракетно-космического приборостроения и информационных технологий» М.: Радиотехника - 2011 г. С. 183-184.

15. Кириллов С.Н., Семин Д.С. Алгоритм помехозащищенного кодирования на базе нелинейного преобразования в полях Галуа // Перспективные технологии в средствах передачи информации: Материалы 9-ой МНТК.- Владим. гос. университет; редкол.: А.Г. Самойлов (и др.). - Владимир: ВлГУ, т.3 - 2011. - 86 с. - С.57-60.

16. Семин Д.С., Покровский П.С. Алгоритм адаптации помехоустойчивого кодера на основе апостериорной информации о частоте битовых ошибок // Новые информационные технологии в научных исследованиях: материалы XVI ВНТК студентов, молодых ученых и специалистов. Рязань. 2011. 354 с.

17. Семин Д.С., Покровский П.С. Вероятностные модели воздействия различных типов помех на бинарный кодированный поток при современных видах модуляции радиосигнала // Новые информационные технологии в научных исследованиях: материалы XVI ВНТК студентов, молодых ученых и специалистов. Рязань. 2011. 354 с.

18. Кириллов С.Н., Семин Д.С., Роговской С.Г., и др. Помехозащищенный кодер канала передачи данных на базе рекурсивного фильтра. Ракетно-космическое приборостроение и информационные технологии. 2010. Труды III ВНТК "Актуальные проблемы ракетно-космического приборостроения и информационных технологий" / под ред. Ю.М. Урличича, А.А. Романова. М.: Радиотехника, 2011.- 624 с. - С 281-284.

19. Кириллов С.Н., Семин Д.С. Недвоичный биномиальный помехоустойчивый кодек с "мягким" алгоритмом декодирования. Проблемы передачи и обработки информации в сетях и системах телекоммуникаций: Материалы 17-й МНТК Рязань: РГРТУ, 2012. - 136 с., часть 1. С. - 65-67.
20. Кириллов С.Н., Семин Д.С. Алгоритмы кодирования и декодирования недвоичных биномиальных помехоустойчивых кодов // Вестник РГРТУ. № 1 (выпуск 39). Часть 1. Рязань, 2012. - С. 5-9.
21. Семин Д.С., Кириллов С.Н., Ревуцкий В.А., и др. Алгоритм распознавания типа и параметров помехоустойчивых кодов. Ракетно-космическое приборостроение и информационные технологии. 2011. Труды IV ВНТК "Актуальные проблемы ракетно-космического приборостроения и информационных технологий" (15-17 июня 2011 г.)/ Под ред. Ю.М. Урличича, А.А. Романова. М.: Радиотехника, 2012. - С 302-308.
22. Семин Д.С., Кириллов С.Н., Слесарев А.С., и др. Программно-управляемый формирователь радиосигналов для командных радиолиний систем спутниковой связи на основе прямого цифрового синтеза. Ракетно-космическое приборостроение и информационные технологии. 2011. Труды IV ВНТК "Актуальные проблемы ракетно-космического приборостроения и информационных технологий" (15-17 июня 2011 г.)/ Под ред. Ю.М. Урличича, А.А. Романова. М.: Радиотехника, 2012. - С. 391-398.
23. Семин Д.С., Слесарев А.С. Формирователь радиосигналов унифицированных средств контроля радиотехнических изделий. Вестник Рязанского радиотехнического университета, № 3. Выпуск 41. Рязань, 2012. - С. 49-53.
24. Кириллов С.Н., Семин Д.С. Недвоичный биномиальный помехоустойчивый кодек с "мягким" алгоритмом декодирования. Проблемы передачи и обработки информации в сетях и системах телекоммуникаций: Материалы 17й МНТК. Рязань: РГРТУ, 2012. - С. 65-67.
25. Семин Д.С. Биномиальные помехоустойчивые коды // Новые информационные технологии в научных исследованиях: материалы XVII ВНТК студентов, молодых ученых и специалистов. РГРТУ. 2012. - С. 151-152.
26. Семин Д.С. Алгоритм кодирования и декодирования недвоичных помехоустойчивых кодов // Методы и средства обработки и хранения информации. Межвузовский сборник научных трудов. Рязань 2012,- С. 173-176.
27. Семин Д.С., Яшин А.Ю. Списочный алгоритм декодирования на базе синдромов с «мягким» входом блочных помехоустойчивых кодов // Вестник Рязанского радиотехнического университета, № 3. Выпуск 45. Рязань, 2013. - С. 41-45.
28. Семин Д.С., Ревуцкий В.А. Анализ устойчивости к вскрытию универсального алгоритма помехозащищенного кодирования. X Международная научная конференция «Перспективные технологии в средствах передачи информации – ПТСПИ-13». Владимир, 2013. – С.148-150.

Соискатель

 / Д.С. Семин /

Семин Дмитрий Сергеевич

Универсальное устройство помехоустойчивого кодирования, адаптивное к
изменению условий функционирования радиосистемы
передачи информации

Подписано в печать 05.11.2013
Формат бумаги 60х84 1/16
Тираж 100 экз. Заказ № 293
Отпечатано в ООО «Полиграф»
390025 г. Рязань, ул. Нахимова д.13