

УДК 621.391.037

А.А. Гладких, Н.Ю. Чилихин, С.М. Наместников, Д.В. Ганин

УНИФИКАЦИЯ АЛГОРИТМОВ ДЕКОДИРОВАНИЯ ИЗБЫТОЧНЫХ КОДОВ В СИСТЕМЕ ИНТЕГРИРОВАННЫХ ИНФОРМАЦИОННО-УПРАВЛЯЮЩИХ КОМПЛЕКСОВ

Гладких Анатолий Афанасьевич, кандидат технических наук, окончил Военную академию связи им. С.М. Буденного, адъюнктуру ВАС, профессор кафедры «Телекоммуникации» Ульяновского государственного технического университета. Имеет монографию, учебные пособия, статьи и патенты РФ в области помехоустойчивого кодирования и защиты информации. [e-mail: a.gladkikh@ulstu.ru].

Чилихин Николай Юрьевич, окончил Ульяновский государственный технический университет, аспирантуру УлГТУ, преподаватель кафедры «Телекоммуникации» УлГТУ. Имеет статьи в области помехоустойчивого кодирования и защиты информации. [e-mail: n.chilikhin@gmail.com].

Наместников Сергей Михайлович, кандидат технических наук, окончил Ульяновский государственный технический университет, аспирантуру УлГТУ, доцент кафедры «Телекоммуникации» УлГТУ. Имеет статьи в области статистической обработки сигналов. [e-mail: sernam@ulstu.ru].

Ганин Дмитрий Владимирович, кандидат экономических наук, доцент, окончил Нижегородскую государственную сельскохозяйственную академию, заведующий кафедрой «Инфокоммуникационные технологии и системы связи» Нижегородского государственного инженерно-экономического университета. Имеет статьи в области инфокоммуникаций. [e-mail: ngiei135@mail.ru].

Аннотация

Возрастающие требования к управлению элементами интегрированных информационно-управляющих комплексов (ИУК) диктуют необходимость применения разнородных по организации протоколов обмена и длительности циклов управления. В этой связи для защиты информации реального времени от ошибок в подобных системах целесообразно использовать набор отличающихся по избыточности помехоустойчивых кодов, обрабатываемых на единой аппаратной платформе. Для реализации подобной концепции рационально использовать короткие блоковые коды, которые уместны при передаче малых по объему данных и которые могут быть легко трансформированы для защиты больших объемов данных с использованием технологии каскадного кодирования или на базе произведения кодов размерности 3D и более. Уменьшение длины кодовых последовательностей при заданных требованиях по достоверности данных приводит к необходимости гибкого синтеза сведений о сигналах, получаемых из непрерывного канала связи, и мягких итеративных алгоритмов обработки выбранных избыточных кодов. Этому требованию отвечают конструкции на основе полярных кодов (ПК). В целях сокращения интервала времени обработки комбинаций ПК предлагается использовать метод разбиения пространства разрешенных кодовых комбинаций на кластеры. Рассматривается механизм образования кластера и варианты защиты номера кластера от искажений при его передаче по каналу с помехами. Приводятся результаты испытаний имитационных моделей процедуры декодирования ПК с использованием различных алгоритмов, которые показывают преимущество предложенного метода обработки данных в условиях низких отношений сигнал/шум при сравнении с каноническими схемами декодирования избыточных кодов.

Ключевые слова: полярный код, мягкий декодер, итеративный процесс, кластер, каскадный код, стирание, списочное декодирование.

UNIFICATION OF REDUNDANT CODE DECODING ALGORITHMS IN INTEGRATED INFORMATION-MANAGEMENT SYSTEMS

Anatolii Afanasievich Gladkikh, Candidate of Engineering; graduated from the S.M. Budyonny Military Academy of Signal Corps; finished his post-graduate studies at the same Academy; Professor at the Department of Telecommunication at Ulyanovsk State Technical University; an author of a monograph, textbooks, articles, and patents in the field of noiseless coding and information security. e-mail: a.gladkikh@ulstu.ru.

Nikolai Iurievich Chilikhin, graduated from Ulyanovsk State Technical University; finished his post-graduate studies at the same University; Lecturer at the Department of Telecommunication at Ulyanovsk State Technical University; an author of articles in the field of noiseless coding and information security. e-mail: n.chilikhin@gmail.com.

Sergei Mikhailovich Namestnikov, Candidate of Engineering; graduated from Ulyanovsk State Technical University, finished his post-graduate studies at the same University; Associate Professor at the Department of Telecommunication at Ulyanovsk State Technical University; an author of articles in the field of statistical signal processing. e-mail: sernam@ulstu.ru.

Dmitrii Vladimirovich Ganin, Candidate of Economics, Associate Professor; graduated from Nizhny Novgorod State Agricultural Academy; Head of the Department of Infocommunication Technologies and Telecommunications at the Nizhny Novgorod State University of Engineering and Economics; an author of articles in the field of infocommunications. e-mail: ngiei135@mail.ru.

Abstract

The increasing requirements for control of integrated information-management system elements are caused by the need of application of communication protocols that are heterogeneous in terms of organization and control cycle duration. Thereupon, it is reasonable to use a set of error-controlled codes differing in redundancy, and processed on a common hardware platform, in similar systems to prevent errors in real-time information. To implement this concept it is expedient to use short block codes. They are applicable in the process of small data transmitting and they can be easily transformed to protect a large bulk of data using the cascaded coding technology or on the basis of product codes in 3D or in higher dimensions. The code sequences shortening at specified requirements in terms of data adequacy leads to a need of the flexible synthesis of information on signals received from a continuous communications channel and of soft iterative algorithms of the selected redundant codes processing. Polar code constructions meet this requirement. The paper offers to use the proper code combinations space clustering in order to reduce the polar code combinations processing time interval. The text gives valuable information on a clustering mechanism and cluster number security variants when transmitting over a noisy channel. The authors present the results of polar code decoding simulation models testing using different algorithms that demonstrate the benefits of the proposed data processing method under conditions of low signal-to-noise ratios compared to canonical schemes required for redundant code decoding.

Key words: polar code, soft-decision decoder, iterative process, cluster, cascade code, erasure, list decoding.

ВВЕДЕНИЕ

Процесс интеграции разнородных информационно-управляющих комплексов (ИУК) может быть успешным только на основе консолидированной унификации программно-аппаратной платформы, составляющей множество разнородных элементов подобной системы. Наряду с передачей больших объемов данных, объективно возрастающие требования к оперативности управления современных и перспективных ИУК диктуют необходимость применения коротких циклов управления (ЦУ). В этой связи для защиты информации реального времени от ошибок в подобных системах целесообразно использовать короткие помехоустойчивые коды, которые оказываются универсальными относительно их длинных аналогов, поскольку они, с одной стороны, обеспечивают простую реализацию адаптивных режимов ИУК, с другой стороны, в случае обмена данными больших объемов такие коды легко трансформируются в многомерные каскадные конструкции [1, 2]. Уменьшение длины кодовых последовательностей при заданных требованиях по достоверности данных ЦУ приводит к необходимости гибкого синтеза сведений о сигналах, получаемых из непрерывного канала связи, и мягких итеративных алгоритмов обработки используемых избыточных кодов [3]. В полной мере этому требованию отвечают конструкции на основе полярных кодов (ПК) [4–6]. Применение концепции ПК обусловлено рядом положительных свойств данного класса блоковых кодов, а именно: достижением асимптотически возможной пропускной способности двоичного симметричного канала без памяти; возможностью свободного

выбора требуемого кодового расстояния в рамках метрики Хэмминга. Однако применение методов списочного декодирования ПК в настоящее время вызывает ряд трудностей, снижающих эффективность применения таких кодов в системах реального времени.

ЛЕКСИКОГРАФИЧЕСКОЕ РАЗБИЕНИЕ КОДОВОГО ПРОСТРАНСТВА

Современные телекоммуникационные технологии играют решающую роль в способах организации и структуре построения существующих и проектируемых мобильных ИУК или специализированных систем управления (СУ), призванных осуществлять сбор заданного набора сведений об управляемых объектах и, в соответствии с целевой функцией $F\{W, U, T\}$, выполнять управление этими объектами [7]. В СУ множество объектов W считается заданным, в то время как множество условий функционирования U может изменяться и оказывать влияние на достижение $F\{\bullet\}$ в требуемые интервалы времени T . Временные параметры СУ определяются длительностью цикла управления $T_{цу}$, выполнение которого является показателем эффективности достижения $F\{\bullet\}$. В условиях действия интенсивных мешающих факторов снижение параметра $T_{цу}$ может быть достигнуто только за счет применения интегрированных СУ и ИУК на основе материального носителя в виде системы связи, способной передавать не только короткие сигналы управления, но и большие объемы мультимедийных данных [7].

Наличие прямого и обратного каналов связи в классической СУ требует выполнения обязательного условия $k(T_{нк} + T_{ок}) \ll T_{ц}$, где k – коэффициент, определяющий число повторов данных в случае возникновения запросов; $T_{нк}$ и $T_{ок}$ – время нахождения управляющей информации в прямом и обратном каналах связи соответственно. Время $\Delta = T_{ц} - T_{cc}$, где $T_{cc} = k(T_{нк} + T_{ок})$, в СУ тратится на обработку данных и принятие решения как в управляемом объекте, так и в управляющем объекте, при этом $\Delta \neq 0$.

Постоянно растущие требования к скорости передачи разнородного контента мобильных СУ требуют комплексного подхода к решению задачи повышения спектральной эффективности широкополосных систем цифровой обработки сигналов. Известны несколько методов решения указанной задачи, среди которых целесообразно выделить два основных. Во-первых, направление, связанное с разработкой и совершенствованием средств обработки сигналов на физическом уровне, и, во-вторых, использование и развитие эффективных алгоритмов помехоустойчивого кодирования на канальном уровне. Объединение технологических особенностей указанных направлений обеспечивает инновационное развитие методов мягкого декодирования помехоустойчивых кодов, позволивших существенно приблизить возможности их обработки к асимптотическим оценкам [4]. В основе указанных методов лежит процедура сортировки индексов мягких решений (ИМР), которая в рамках обрабатываемого декодером кодового вектора носит лексикографический характер [7].

Лексикографический порядок – это порядок, принятый в словарях. Пусть r -выборка $(A_1, B_1, C_1, \dots, R_1)$ предшествует r -выборке $(A_2, B_2, C_2, \dots, R_2)$, если k первых элементов (считая слева направо или справа налево, по соглашению) этих r -выборок равны, а $(k + 1)$ -й элемент первой предшествует $(k + 1)$ -му элементу второй. В общем случае лексикографический метод упорядочивания некоторых критериев соответствует последовательности, например, в которой $f(x_1) > f(x_2) > \dots > f(x_n)$, где $\{x_i\}$ – множество альтернатив среди заданных критериев. Под величинами x_i в контексте сортировки ИМР понимаются действительные числа, сопровождающие биты (жесткие решения) принятой кодовой комбинации. Задача заключается в том, чтобы из множества $C_{n,k}$ разрешенных комбинаций избыточного (n, k) -кода составить список комбинаций, в наибольшей степени совпадающих с принятым вектором. С учетом принятого из канала с помехами слова $V_{np} = V_{nep} \oplus e$, где e – вектор ошибок, а $V_{nep} \in C_{n,k'}$ составляется список $\{S\}$ множества слов, находящихся от слова V_{np} на расстоянии $d - 1$ и менее, где d – метрика Хемминга. Используя критерий максимального правдоподобия, декодер осуществляет замену слова V_{np} на вектор $C_{np} \in C_{n,k}$ из списка $\{S\}$, содержащего наибольшее число совпадающих позиций. В [7] показано, что, используя структурные признаки (алгебраические закономерности) в построениях практически любых помехоустойчивых ко-

дов, возможно разбиение пространства $C_{n,k}$ на кластеры. Каждый кластер содержит замкнутое множество комбинаций $\{c_i\} \in C_{n,k}$, где $i = 0, (2^f - 1)$, f – число одинаковых номеров разрядов для любой комбинации пространства $C_{n,k'}$ отводимых под признак (номер) кластера, при этом $f \leq k$ и $\{f\} \in GF(2^{k-f})$. Для получения номера i двоичное представление разрядов f_2 переводят в десятичную форму f_{10} . Упорядочение номеров i является лексикографической процедурой, позволяющей уменьшить время формирования списка в 2^f раз за счет однозначного выделения из $C_{n,k}$ комбинаций кластера с номером i , следовательно, $\{S_i\} = c_{i0}, c_{i1}, \dots, c_{i(2^k-1)}$. Полагая $2^k - 1 = \xi$, для всего множества $C_{n,k}$ получим:

$$\begin{aligned} i = 0 & \left\{ c_{00}, c_{01}, \dots, c_{0(2^k-1)} \right\}; \\ i = 1 & \left\{ c_{10}, c_{11}, \dots, c_{1(2^k-1)} \right\}; \\ & \dots \dots \dots \dots \dots \\ i = \xi & \left\{ c_{\xi 0}, c_{\xi 1}, \dots, c_{\xi(2^k-1)} \right\}. \end{aligned}$$

Кластер, у которого в качестве номера выбрано значение $i = 0$, составляет базис пространства кластеров. Действительно, если за номер кластера для всего множества $C_{n,k}$ приняты некоторые элементы a_1, a_2, \dots, a_f , то для каждого кластера с номером i эти элементы будут одинаковы. Складывая по mod 2 любые комбинации векторов из кластера с номером $i \neq 0$, получим нулевые значения на позициях номера кластера. Следовательно, любую комбинацию из множества $C_{n,k} \notin \{C_{i \neq 0j}\}$ путем сложения с любой другой комбинацией из этого кластера можно перевести в комбинацию базисного пространства $\{C_{i=0j}\}$. Это свойство кластеров актуально для рациональной организации работы декодера, поскольку позволяет исключить процедуру поиска обратных матриц эквивалентных кодов, снизить вычислительные затраты и повысить эффективность реализации декодера аппаратными средствами. Предлагаемый алгоритм перестановочного декодирования исключает процедуру поиска $\det G_{экг}$, однако требует надежного определения символов кластера a_1, a_2, \dots, a_f .

КЛАССИФИКАЦИЯ МЕТОДОВ ЗАЩИТЫ НОМЕРА КЛАСТЕРА

Для защиты номера кластера при его передаче по каналу с помехами может быть использовано несколько подходов. Классификация методов защиты кластера приведена на рисунке 1.

Защита номера кластера без введения дополнительной избыточности может быть выполнена за счет выделения тех разрядов кодового вектора, которые в кластере $\{C_{i=0j}\}$ оказываются линейно зависимыми. В совокупности из линейно зависимых разрядов невозможно сформировать полное поле элементов из $GF(2^{k-f})$. Это свойство

сохраняется для любого кластера кода. Гибридное кодирование предполагает размещение проверочных разрядов кода, защищающего номер кластера, на позициях линейно зависимых разрядов. Приемнику известны эти позиции, поэтому декодером такие позиции в рамках основного кода считаются ошибочными и могут быть заранее классифицированы как стирания с минимальными ИМР.

Циклические сдвиги данных целесообразно использовать в ходе применения циклических кодов. Для этого оценивается весовой спектр кода и выделяются представители каждого веса A_i , после чего они выражаются через примитивные элементы поля $GF(2^f)$ путем последовательного выделения в комбинации $f+j$ двоичных элементов, где $j = \overline{0, n}$. Например, комбинация двоичного циклического кода (15,5,7) вида 001111010110010 при $f=3$ может быть представлена в формате примитивных элементов поля $GF(2^3)$:

$\alpha^0 \alpha^3 \alpha^5 \alpha^5 \alpha^4 \alpha^6 \alpha^1 \alpha^6 \alpha^3 \alpha^4 \alpha^2 \alpha^0 \alpha^1 \alpha^2 0$, где $\alpha^0 \Rightarrow 001$ – первые три элемента двоичного представления комбинации, затем $\alpha^3 \Rightarrow 011$, $\alpha^5 \Rightarrow 111$ и далее с учетом сдвига на бит до $0 \Rightarrow 000$.

Для удобства выделим характерное сочетание элементов ... $\alpha^5 \alpha^5 \alpha^4 \alpha^6 \dots$, тогда расстояние от искаженного номера кластера α^0 до выделенной группы элементов составляет один шаг, а в альтернативном случае (в комбинации существует еще один элемент α^0) это расстояние составляет пять шагов. Используя эту разницу, можно точно определить номер кластера, к которому принадлежит комбинация. Метод не является надежным, поскольку группа характерных элементов может быть искажена. В этом случае в памяти приемника необходимо удерживать дополнительные признаки, что повышает сложность реализации приемника. Однако метод разбиения пространства $C_{n,k}$ на кластеры обладает интересной особенностью, которая заключается в том, что в любой кластер входят представители всех весов. Это позволяет существенно сократить объемы вычислений при изучении весового спектра кода. Необходимо вычислить комбинации, относящиеся только к одному из кластеров кода, вместо вычисления всего множества $C_{n,k}$.

Введение дополнительной избыточности за счет проверки четности разрядов кластера a_1, a_2, \dots, a_f похоже на метод гибридного кодирования, отличаясь только способом восстановления данных. Проверка четности может быть усилена итеративными преобразованиями данных, для реализации которых требуется сопровождение каждого символа значениями ИМР в виде действительных чисел $\pm\lambda$, для которых знак «+» соответствует жесткому решению «единица», а знак «-» соответствует решению «ноль». Если при первой передаче символа $a_k \in f$, где $k = \overline{1, f}$, приемник фиксирует λ_{k1} , то в ходе повторной передачи этого символа приемник фиксирует λ_{k2} . Очевидно, что символ четности λ_{nc} в условиях безыскаженной передачи λ_{k1} и λ_{k2} отвечает условию $\lambda_{nc} = 0$, а значение $\lambda_{nc} = \lambda_{max}$. В этом случае результат итеративного преобразования с номером j определяется соотношением:

$$\Omega_j = \begin{cases} \min(\text{sign}[L(\lambda_{k1}) + L(\lambda_{cork2})_j] \times \text{sign}L(\lambda_{nc})) \approx \text{sign}(\lambda_{cork2})_{j+1} \times (-1)^{1-m}; \\ \min(\text{sign}[L(\lambda_{k2}) + L(\lambda_{cork1})_j] \times \text{sign}L(\lambda_{nc})) \approx \text{sign}(\lambda_{cork1})_{j+1} \times (-1)^{1-m}. \end{cases} \quad (1)$$

В (1) λ_{cor} представляет значение ИМР, которое используется для коррекции ошибочного символа, а m определяет количество единичных элементов с высокими значениями ИМР, вычеркиваемых при увеличении числа повторов f более двух. Из (1) следует, что при большой разнице значений между $\min(\text{sign}[\bullet])$ и $\text{sign}L(\bullet)$ число итераций, требуемых для исправления ошибочного бита, возрастает. Расчеты показали, что в случае использования действительных значений λ требуется до 30 итераций, в то время как при целочисленных λ надежная коррекция символа происходит за 12–15 итераций.

Следует учитывать, что повтор данных является наиболее простым методом защиты последовательности a_1, a_2, \dots, a_f . При этом в зависимости от уровня мешаю-



Рис. 1. Классификация методов защиты номера кластера

ших факторов число дублирующих передач может изменяться.

Ошибочное определение номера кластера приводит к ошибочному выделению списка кодовых комбинаций, подлежащих дальнейшей обработке декодером. Поэтому вероятность искажения номера кластера P_f эквивалентна вероятности ошибочного декодирования кодовой комбинации P_0 . Пусть используемый в системе помехоустойчивый код обеспечивает режим исправления ошибок. При известном значении d_{min} ошибочное восстановление комбинации происходит, когда кратность ошибок превосходит значение $t = (d_{min} - 1)/2$. Оценим значения ошибки на комбинацию $P_0(n, t + 1)$ для некоторых кодов БЧХ и сравним вероятности ошибочного восстановления номера кластера для $f = 3$. Вероятное совпадение $|\lambda| = |-\lambda|$ в аналитической модели рассматривалось как ошибочное. При повторении данных номера кластера вероятность ошибки соответствует совпадению символов на одних и тех же позициях как при первой передаче, так и при повторной передаче значения f . Тогда

$$P_f(n, i) = p^2 \cdot (1 - p)^{n-2},$$

где $n = 2f$ при двукратной передаче номера кластера.

На рисунке 2 приведены все полученные путем аналитического моделирования характеристики для трех кодов БЧХ: (15,5,7); (15,7,5); (15,11,3) – и указанных выше способов защиты кластера.

Анализ полученных данных показывает преимущество кода БЧХ с максимальной исправляющей способностью. Именно этот код обеспечивает наибольшую энергетическую эффективность систем связи, но этот код имеет низкое значение $R \approx 0,33$. Лучшие показатели для системы защиты кластера показывает система с повтором комбинации кластера. Эта система в области низких отношений сигнал/шум обеспечивает энергетический выигрыш относительно кода (15,5,7) до значения $E_b/N_0 = 1,5$ дБ. При

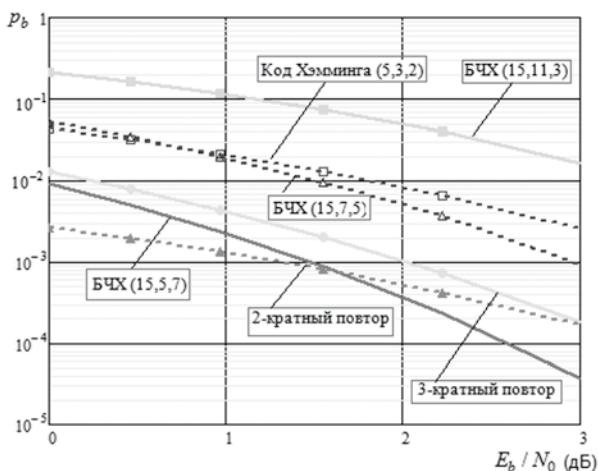


Рис. 2. Сравнительные данные для оценки искажения номера кластера

этом трехкратный повтор номера кластера по сравнению с кодом БЧХ неэффективен во всем диапазоне отношений сигнал/шум. Использование системы гибридного кодирования неэффективно даже по сравнению с кодом БЧХ, имеющим $R \approx 0,5$. При этом повторение данных кластера всегда оправдано относительно кодов (15,7,5) с $R \approx 0,47$ и (15,11,3) с $R \approx 0,73$.

РЕЗУЛЬТАТЫ ИМИТАЦИОННОГО МОДЕЛИРОВАНИЯ НЕКОТОРЫХ ТИПОВ ПК

В ходе имитационного моделирования были выполнены испытания моделей систем обмена данными с ПК в канале с независимым потоком ошибок. Параметры ПК (8,4); (16,5); (16,11) и (32,16) отвечали требованиям применения таких кодов в системе с короткими циклами управления. Полученные данные оценивались как для искажения комбинаций, так и для оценки вероятности искажения на бит. В последнем случае полученные данные сравнивались с результатами, полученными в работах Арикана [1, 2] и Тала-Варди [8, 9]. Длина кодовых комбинаций в рассматриваемой модели выбиралась из соображений рационального размера перестановочной матрицы и последующего использования ПК в основе каскадных конструкций. На рисунке 3 представлены результаты испытаний модели для ПК с параметрами (8, 4) с мультипликативным коэффициентом $\mu = 1$.

Анализ результатов испытаний имитационной модели показывает, что полученные характеристики обеспечивают энергетический выигрыш относительно лучшего из известных алгоритмов – алгоритма Тала-Варди в диапазоне от 0,9 до 1,6 дБ. При этом алгоритм АПД оказался лучшим относительно МРД. Для оценки тенденции поведения ПК в диапазоне от 0 до 3 дБ были испытаны модели с ПК, име-

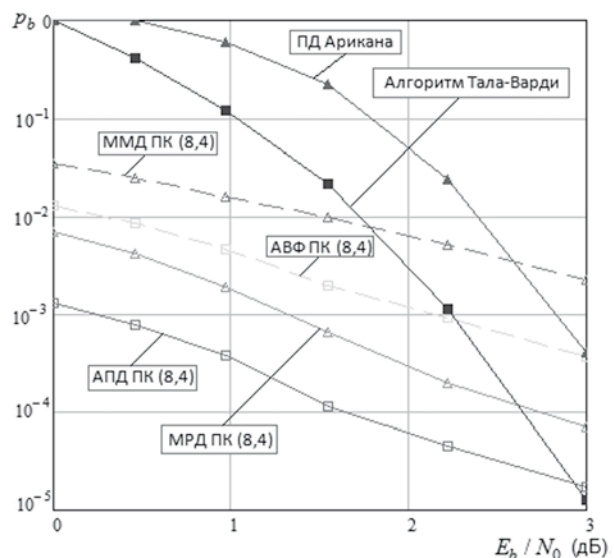


Рис. 3. Результаты моделирования системы с ПК (8, 4): ММД – метод мажоритарного декодирования; АВФ – алгоритм с весовой функцией; МРД – метод распространения доверия; АПД – алгоритм перестановочного декодирования

ющими иные характеристики, например, увеличивалась длина кодового блока. Результаты испытаний модели для кода (16,5) показаны на рисунке 4.

Поскольку ПК (8,4) эквивалентен коду РМ с аналогичными параметрами, возникла целесообразность исследования ММД. В этом случае использовались сведения о жестких решениях символов. Использование ИМР в ММД позволило разработать алгоритм, в котором использовалась весовая функция или значения ИМР при мажоритарной обработке данных.

Все указанные алгоритмы и методы оказались эффективными относительно алгоритма Тала-Варди в диапазоне отношений сигнал/шум от 0 до 3 дБ. При более высоких значениях этого параметра предложенные алгоритмы теряют свою эффективность.

Анализ полученных результатов показывает, что увеличение размерности кода положительно сказывается на вероятностных характеристиках системы. Действительно, на уровне $P_b = 10^{-4}$ энергическая эффективность алгоритма АПД относительно алгоритма Тала-Варди составляет около 2 дБ, при этом преимущество АПД относительно АВФ и ММД сохраняется. Недостатком рассматриваемого кода является низкая скорость обмена данными. Значение $R \approx 0,3$. Увеличение относительной скорости кода R до значений 0,7 приводит к снижению корректирующих возможностей кода. Результаты испытаний модели с ПК (16,11) представлены на рисунке 5.

Увеличение параметров ПК до значений (32,16) по результатам испытания модели показали общую тенденцию изменения характеристик системы обмена данными с ПК. Результаты испытаний представлены на рисунке 6.

Применение ПК в системах обмена данными позволяет реализовать алгоритмы перестановочного декодирования с защитой номера кластера. Подобный подход важен

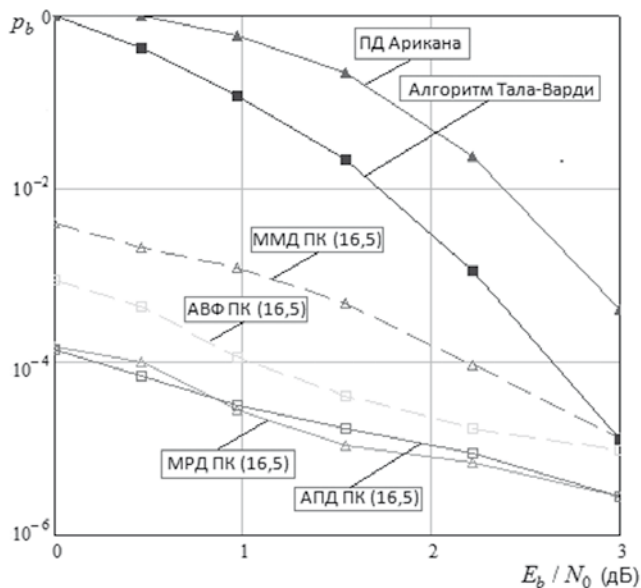


Рис. 4. Результаты испытаний модели с ПК (16,5)

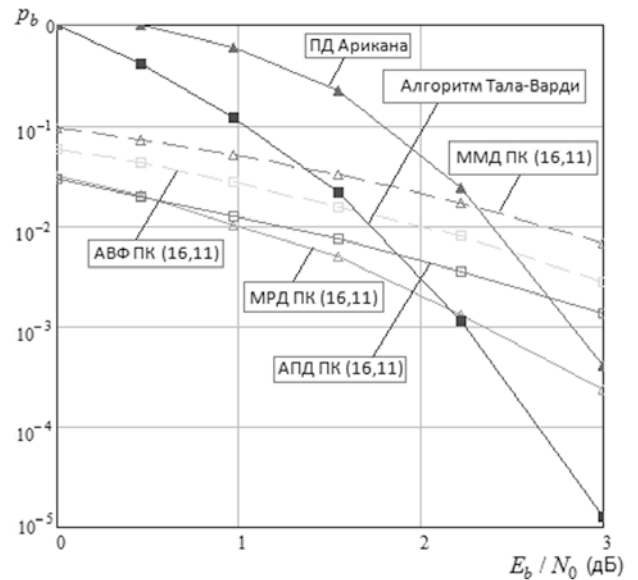


Рис. 5. Результаты испытаний модели с ПК (16,11)

в условиях применения каналов связи с эффектом группирования ошибок и каналов с нестационарными характеристиками.

Перестановочное декодирование обеспечивает выполнение двух важных условий:

- во-первых, гибкую систему защиты номера кластера, что позволяет оперативно реализовать преимущества параметрической адаптации за счет наращивания (снижения) числа повторов не всей комбинации, а ее части;
- во-вторых, в условиях концентрации ошибок среди младших разрядов кодовой комбинации получить дополнительные сведения о состоянии канала связи.

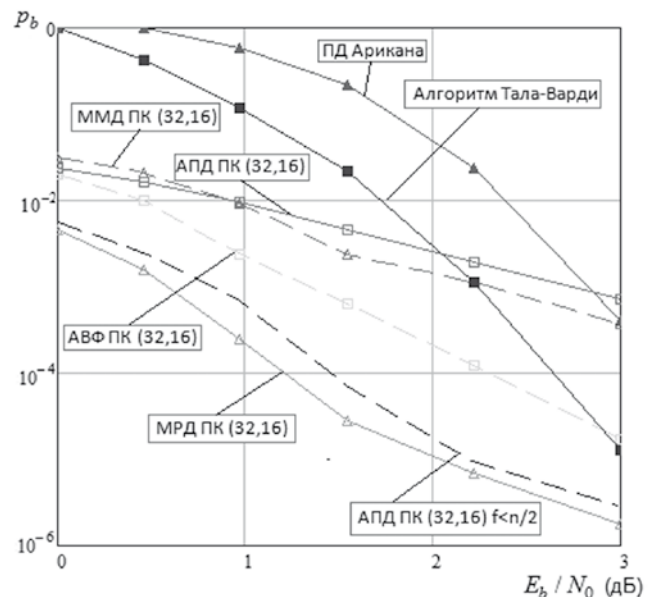


Рис. 6. Результаты испытаний модели с ПК (32,16)

СИНТЕЗ СИСТЕМЫ ОБМЕНА ДАННЫМИ НА ОСНОВЕ ПК

Представленные результаты обработки ПК показывают, что самостоятельное применение в ИУК таких кодов не в полной мере обеспечивает известные требования по достоверности данных. Для сравнения на рисунке 7 представлены результаты аналитического моделирования (АМ) кода Хэмминга с проверкой на четность (8,8,4) и ПК с адекватными параметрами. Одновременно с этими данными на рисунке представлены результаты испытаний имитационной модели (ИМ) для кода ПК (заимствованы из рисунка 3), которые показывают результаты, уступающие результатам АМ на порядок.

На рисунке 8 показаны результаты аналитического моделирования схем каскадного кодирования, когда на внешней ступени обработки данных используется не двоичный код Рида-Соломона (РС) над полем $GF(2^4)$, на внутренней ступени – подходящий ПК. При этом для ПК был выбран худший вариант из представленных на рисунке 7.

Один из алгоритмов декодирования кода РС был выбран как алгоритм провокации стирания (АПС), позволяющий декодеру максимально использовать введенную в код избыточность [2]. Представленные результаты показывают, что комплексное применение кодов РС и ПК обеспечивает выполнение требований по достоверности при использовании коротких кодов, когда возможна передача в одном пакете команды объемом до 40 бит. Предложенная схема эффективна с точки зрения борьбы с группирующимися ошибками в системах с радиointерфейсом, при этом исключаются временные задержки из-за перемежителей и демультиплексоров.

ЗАКЛЮЧЕНИЕ

В условиях интенсивных помех для передачи данных, используемых в ИУК, применение коротких помехоустойчивых кодов оправдано с точки зрения унификации алгоритмов декодирования таких кодов как в системах с масштабируемой избыточностью, адаптивных системах с повторением данных, так и в системах обработки команд, критичных к длительности ЦУ.

Показана возможность декодирования коротких ПК методом кластерного разбиения, что позволяет в полной мере реализовать введенную в код избыточность. Показано преимущество предложенных алгоритмов относительно рекурсивных методов обработки данных. Представлена классификация методов защиты номера кластера при его передаче по каналу с помехами и получены сравнительные характеристики по вероятности ошибочного приема различных конструкций представления номера кластера. Показано, что использование целочисленных ИМР позволяет в 3–4 раза сократить время производства итеративных преобразований, что отвечает требованиям функционирования ИУК реального времени.

Применение для ПК метода перестановочного декодирования в сочетании с одним из методов защиты кластера является продуктивным в диапазоне отношений сигнал/шум от 0 до 3 дБ.

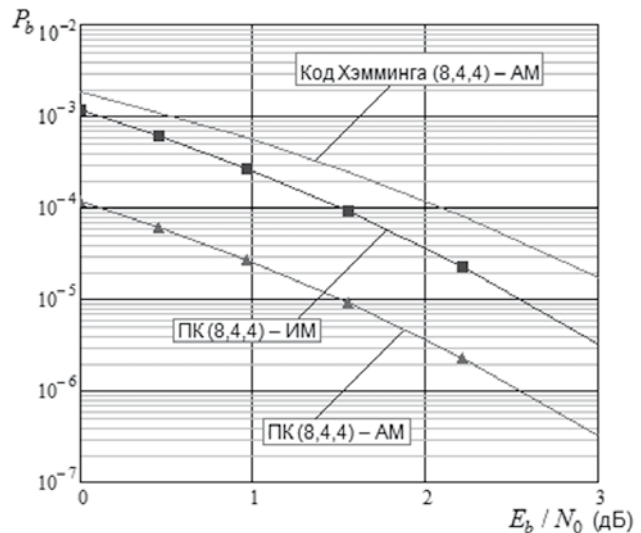


Рис. 7. Сравнительные данные результатов АМ и ИМ для кода Хэмминга и ПК

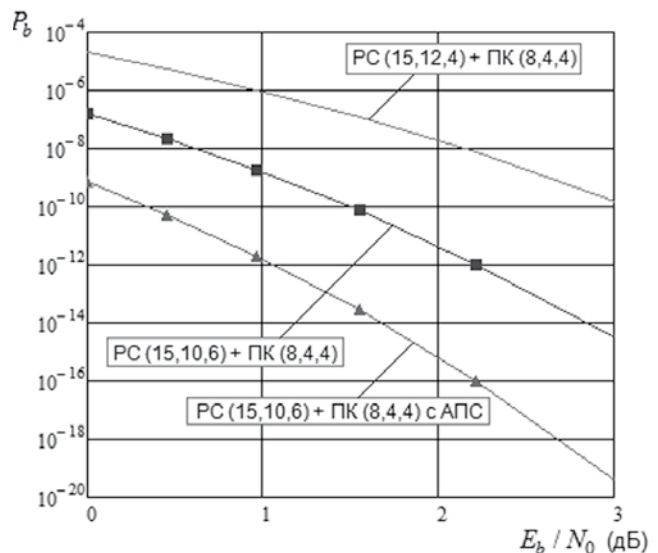


Рис. 8. Результаты АМ каскадного кода

Раскрыты новые возможности кластерного разбиения пространства разрешенных кодовых комбинаций систематических блочных кодов, позволяющие оценить весовой спектр кода для точного определения характеристик кода по исправлению ошибок.

СПИСОК ЛИТЕРАТУРЫ

1. Гладких А.А. Применение метода гиперкодирования в системах передачи данных // Автоматизация процессов управления. – 2011. – № 3 (25). – С. 77–81.
2. Эффективное декодирование не двоичных кодов с провокацией стертых элементов / А.А. Гладких [и др.] // Автоматизация процессов управления. – 2013. – № 2 (32). – С. 87–93.
3. Гладких А.А., Линьков И.С. Оптимизация процедуры итеративных преобразований данных // Автоматизация процессов управления – 2012. – № 3 (29). – С. 3–7.

4. Arikan E. Channel polarization: A method for constructing capacity-achieving codes for symmetric binary-input memoryless channels // *IEEE Transactions on Information Theory*. 2009. – № 7(55). – pp. 3051–3073.

5. Arikan E., Telatar E. On the rate of channel polarization // *Proc. IEEE Int'l Symp. Inform. Theory (ISIT'2009)*. – Seoul, South Korea. – 2009. – pp. 1493–1495.

6. Гладких А.А., Чилихин Н.Ю. Моделирование алгоритмов совместной обработки полярных кодов в системе производства кодов // *Радиотехника*. – 2014. – № 7. – С. 111–115.

7. Гладких А.А. Основы теории мягкого декодирования избыточных кодов в стирающем канале связи. – Ульяновск : УлГТУ, 2010. – 379 с.

8. Tal I., Vardy A. List decoding of polar codes // *IEEE Int. Symp. Inf. Theory (ISIT)*. – August 2011.

9. Tal I., Vardy A. How to construct polar codes // *IEEE Trans. Inform. Theory*. – October 2013. – Vol. 59, № 10. pp. 6562–6582.

REFERENCES

1. Gladkikh A.A. Primenenie metoda giperkodirovaniia v sistemakh peredachi dannykh [Use of Hyper-Coding Method in Data-Transfer Systems]. *Avtomatizatsiia protsessov upravleniia* [Automation of Control Processes], 2011, no. 3 (25), pp. 77–81.

2. Gladkikh A.A., Baskakova E.S., Maslov A.A., Tamrazian G.M. Effektivnoe dekodirovanie nedvoichnykh kodov s provokatsiei stertogo elementa [Effective Decoding of Non-Binary Codes Using Erased Element Provocation Method].

Avtomatizatsiia protsessov upravleniia [Automation of Control Processes], 2013, no. 2 (32), pp. 87–93.

3. Gladkikh A.A., Linkov I.S. Optimizatsiia protsedury iterativnykh preobrazovaniia dannykh [An Optimization of Iterative Data-Transform Procedure]. *Avtomatizatsiia protsessov upravleniia* [Automation of Control Processes], 2012, no. 3 (29), pp. 3–7.

4. Arikan E. Channel Polarization: A Method for Constructing Capacity-Achieving Codes for Symmetric Binary-Input Memoryless Channels. *IEEE Transactions on Information Theory*, 2009, vol. 55, no. 7, pp. 3051–3073.

5. Arikan E., Telatar E. On the Rate of Channel Polarization. *Proc. IEEE Int'l Symp. Inform. Theory (ISIT'2009)*. Seoul, South Korea, 2009, pp. 1493–1495.

6. Chilikhin N. Yu., Gladkikh A.A. Modelirovanie algoritmov sovmestnoi obrabotki poliarnykh kodov v sisteme proizvedeniia kodov [Simulation Algorithms Coprocessing Polar Codes in a Product Code]. *Radiotekhnika* [Radio-Engineering], 2014, no. 7, pp. 111–115.

7. Gladkikh, A.A. *Osnovy teorii miagkogo dekodirovaniia izbytochnykh kodov v stiraushchem kanale svyazi* [Soft-Decision Decoding Essentials of Redundant Codes in Erasure Communications Channel]. Ulyanovsk, UISTU Publ., 2010. 379 p.

8. Tal I., Vardy A. List Decoding of Polar Codes. *IEEE Int. Symp. Inf. Theory (ISIT)*, August 2011.

9. Tal I., Vardy A. How to Construct Polar Codes. *IEEE Trans. Inform. Theory*, October 2013, vol. 59, no. 10, pp. 6562–6582.