

Лохин Валерий Михайлович
Д.т.н.; профессор.

Манько Сергей Викторович
Д.т.н.; профессор.

Романов Михаил Петрович
Д.т.н.; профессор.

Makarov Igor' Mixajlovich
The State Educational Establishment of the Maximum Vocational Training "the Moscow State Institute of a Radio Engineering, Electronics and Automatics (Technical University)".
E-mail: cpd@mirea.ru; kpu-mirea@yandex.ru.
78, Vernadskogo Pr., Moscow, 119454, Russia.
Phone: +74954349232.
The Department "Problem of management"; Dr. of Eng. Sc.; Academician of the Russian Academy of Science.

Loxin Valerij Mixalovich
Dr. of Eng. Sc.; Professor.

Man'ko Sergej Viktorovich
Dr. of Eng. Sc.; Professor.

Romanov Mixail Petrovich
Dr. of Eng. Sc.; Professor.

УДК 004.41

Р.А. Нейдорф, С.П. Новиков, В.С. Чудаков

**ПРАКТИЧЕСКАЯ МЕТОДИКА РАСЧЕТА ДАННЫХ ДЛЯ ВЫБОРА
ПРИНЦИПОВ КОДИРОВАНИЯ И ИХ ПАРАМЕТРОВ В ЗАШУМЛЕННЫХ
КАНАЛАХ СВЯЗИ СЕТЕЦЕНТРИЧЕСКИХ СИСТЕМ**

Рассматривается методика расчета данных для выбора параметров систем кодирования в зашумленных каналах связи. В основу расчётов положено значение вероятности искажения одного бита информации как независимого случайного события. На основе этого подхода определены вероятности возникновения ошибки в кодовом слове в зависимости от его длины. Поскольку длина кодового слова определяет количество восстанавливаемых в нём ошибок для используемой системы кодирования, возникает возможность обоснованного выбора декодера и его параметров. Результаты расчетов приведены в таблицах и наглядно отображены диаграммами. Проведен анализ закономерностей формирования значений в зависимости от длины кодового слова и использованного декодера.

Канал связи; кодирование; методика расчета вероятности ошибок; помехоустойчивые коды.

R.A. Nejdorf, S.P. Novikov, V.S. Chudakov

**PRACTICAL DESIGN PROCEDURE OF THE DATA FOR THE CHOICE
OF PRINCIPLES OF CODING AND THEIR PARAMETERS
IN COMMUNICATION CHANNELS WITH NOISE OF
SETETSENTRICHESKY SYSTEMS**

This article describes a method for calculating the data for setting coding systems configuration in noisy communication channels. The calculation is based on probability of distortions of one bit of information as independent random events. Based on this approach identifies likelihood of errors in the code depending on its length. It should be possible to make informed choices of the decoder and its parameters, because length of typing keyword specifies the number of correctable

errors for encoding system, it should be possible to make informed choices of the decoder and its parameters. The results are presented in tables and displays charts graphically. Analysis of patterns formation of values depending on the length of code words and used decoder.

Communication channel; coding; a design procedure of probability of errors; noise proof codes.

Все реальные каналы связи подвержены воздействию помех, которые могут привести к искажению передаваемых по каналу сигналов и, как следствие, к частичной (или даже полной) потере связанной с ними информации. По этой причине одной из важнейших задач в теории связи является повышение надежности передачи информации путем построения и реализации различных помехоустойчивых кодов. В задачах построения систем связи, управления и автоматизации существенной является проблема выбора кодов передачи сигналов с возможностью их восстановления, а также параметров этих кодов, поскольку процессы дистанционной (особенно, беспроводной) передачи реализуются на фоне значительного спектра внешних помех. Это проблема тесно связана с шумовыми характеристиками каналов, для которых принято различать ситуации возникновения так называемых единичных и групповых ошибок.

В связи со сформулированной проблемой при проектировании каналов связи всегда приходится ориентироваться на результаты анализа наиболее распространенных, эффективных и просто реализуемых кодов на стойкость к пакетам ошибок.

Краткая характеристика кодов, исправляющих пакетные ошибки. Одни из давно известных помехоустойчивых кодов представлены семейством кодов Рида–Малера (*RM*-коды). Они представляют собой двухпараметрическое семейство блочных кодов с целыми неотрицательными параметрами m (порядок кодового слова) и r (длина кодируемого информационного слова в битах), для которых $0 \leq r < m$. Важнейшими характеристиками этих кодов являются: длина кодового слова ($n = 2^m$),

размерность кода – $k = \sum_{i=0}^r C_m^i$, минимальное кодовое расстояние: $d = 2^m - r$, коли-

чество гарантированно исправляемых кодом ошибок – $t = 2^m - r - 1$. *RM*-коды с параметрами m, r принято обозначать *RM*(r, m). Необходимо отметить, что восстанавливающая способность этих кодов невысока.

Классическим алгоритмом декодирования *RM*-кодов является мажоритарный алгоритм. Этот алгоритм полностью исправляет количество ошибок веса $w(t) \leq t$ (где t – количество гарантированно исправляемых кодом ошибок, $w(t)$ – вес Хэмминга, показывающий количество ошибок в кодовом слове). Отличительной особенностью мажоритарного декодера (МДК) является то, что по полученному из канала зашумленному кодовому слову восстанавливается не истинное кодовое слово (закодированная информация), а непосредственно исходное сообщение. Искомый информационный вектор $a = (a_1, a_2, \dots, a_k)$ представляется в блочном виде $(a_{(0)}, a_{(1)}, \dots, a_{(r)})$, длина j -го блока равна C_m^j . Декодирование производится по блокам справа налево, и при декодировании каждого следующего блока используются полученные ранее результаты [1]. Однако если число ошибок в кодовом слове превышает количество гарантированно исправляемых ошибок, то МДК практически перестает правильно декодировать кодовые слова.

В последнее время разработан ряд декодеров *RM*-кода, позволяющих с достаточной вероятностью восстанавливать искаженный кодовый вектор при числе ошибок больше, чем $d/2$. Одним из таких декодеров является вероятностный декодер Сидельникова–Першакова (СПД). В работе [2], предложен вероятностный алгоритм декодирования кодов Рида–Маллера при числе ошибок, превышающем значение t . При реализации алгоритма вводятся два целочисленных

параметра s и h , где $s \in [1, \dots, n]$, $h \geq 0$, которые отвечают за глубину перебора при поиске верных значений на одном из этапов алгоритма. Согласно [2] этот алгоритм имеет сложность порядка $n^2(m + hs^3)$ и позволяет почти всегда исправлять ошибки веса $t \leq (n - Cm^{1/4}n^{3/4})/2$ при $m \rightarrow \infty, C > \ln 4$.

Значительно более популярными на сегодняшний день являются коды Боуза–Чоудхури–Хоквингема (БЧХ). В теории кодирования БЧХ-коды – это широкий класс циклических кодов, применяемых для защиты информации от ошибок. Отличаются возможностью построения кода с заранее определёнными корректирующими свойствами, а именно, d_0 – минимальным кодовым расстоянием. Эти коды позволяют исправлять кратное число ошибок (две при $d_0 = 5$ и более – при $d_0 > 5$). Минимальное кодовое расстояние зависит от длины кодового слова (КС). Теоретически БЧХ-коды могут исправлять произвольное количество ошибок, но это требует существенного увеличения длины кодовой комбинации, что резко снижает скорость передачи данных.

Широко используемым подмножеством БЧХ-кодов является код Рида–Соломона. Это недвоичный циклический код, который обладает хорошей корректирующей способностью при сравнительно небольшой избыточности. Важнейшей характеристикой кода является количество восстанавливаемых ошибок, которое рассчитывается следующим образом: $t = (n - k)/2$, где n – длина кодового слова, k – длина информационного слова, $(n - k)$ – избыточность кода.

Коды БЧХ являются циклическими кодами, поэтому к ним применимы все методы, используемые для декодирования циклических кодов. Однако существуют гораздо более эффективные алгоритмы, разработанные именно для БЧХ-кодов:

- ◆ Алгоритм Берлекемпа–Мэсси (ВМА). По числу операций в конечном поле этот алгоритм обладает высокой эффективностью. ВМА обычно используется для программной реализации или моделирования кодов БЧХ и кодов Рида–Соломона;

Прямое решение (алгоритм Питерсона–Горенштейна–Цирлера (ПГЦ)). Этот алгоритм находит коэффициенты многочлена локаторов ошибок прямым решением, соответствующей системы линейных уравнений. В действительности, так как сложность этого алгоритма растёт как куб минимального расстояния d_0 , прямой алгоритм может быть использован только для малых значений d_0 , однако именно этот алгоритм лучше всего проясняет алгебраическую идею процесса декодирования.

Таким образом, в распоряжении проектировщиков каналов связи в настоящее время вполне достаточно подходов, методов кодирования и кодовых систем для решения конкретных задач. Однако при этом необходимо иметь в качестве одного из инструментов методику выбора параметров кодеков, удовлетворяющих условиям передачи сигналов и техническому заданию на канал. Эта методика должна опираться на характеристики помех в канале, предоставляя проектировщику информацию о наиболее вероятном (или максимальном) количестве ошибок, а также о связи его с параметрами кода, если такая имеется. Исследованию этой проблемы посвящён дальнейший материал данной статьи.

Теоретическое исследование связи вероятностей возникновения одиночных и пакетных ошибок. Как уже указывалось, отличительной особенностью большинства реальных каналов связи является возможность возникновения в них именно групповых ошибок. Это обстоятельство осложняет применение в таких каналах классических помехоустойчивых кодов, построенных на основе парадигмы независимости одиночных ошибок в канале, которые обычно имеют невысокую вероятность появления. Такие коды обладают невысокими восстанавливаемыми свойствами и оказываются совершенно неэффективными при использова-

нии в каналах с групповыми ошибками. В связи с этим коды, наряду с другими признаками, классифицируют по их способности эффективно исправлять либо независимые ошибки, либо пакеты ошибок. Если код оперирует элементами над полем большой размерности, то такие коды являются кодами, исправляющими пакеты ошибок, в силу того, что каждый элемент кодового слова, а также и каждый элемент накладываемого вектора ошибок можно представить в виде последовательности бит некоторой длины. При этом, естественно, код, исправляющий пакеты ошибок, является также и кодом, исправляющим независимые ошибки. Некоторые из таких кодов рассмотрены выше.

С другой стороны, параметры кодов, исправляющих пакетные ошибки, никак не связаны, ни со структурой пакета, ни с его положением в искажаемом кодовом слове. Таким образом, для современных кодовых систем значение имеет лишь количество ошибок на передаваемую информационную единицу, а структура не имеет значения.

В силу рассмотренного обстоятельства в данном исследовании не делается акцент на свойствах помех, а считается, что дальнейшему рассмотрению подлежат лишь независимые ошибки, а пакеты суть результат их случайного попадания в интервал кодового слова. При этом единственным параметром, характеризующим свойства таких ошибок, является вероятность их возникновения. Однако в данном случае она должна оцениваться экспериментальными данными о вероятностях появления пакетных ошибок, и оцениваться величинами, делающими их адекватными результатам действия этих ошибок.

В парадигму настоящего исследования заложено предположение, что для расчета вероятности искажения некоторого заданного числа бит в кодовом слове (пакета ошибок) можно воспользоваться формулой Бернулли и принятой из технических, технологических или надёжных соображений заданной вероятностью искажения одного бита в канале связи. Эта формула применительно к задаче, где в качестве независимого случайного события B рассматривается появление ошибки в произвольном бите кодового слова, имеет следующий вид:

$$P_n(k) = C_n^k \cdot p^k \cdot (1-p)^{n-k} = \frac{n!}{k!(n-k)!} \cdot p^k \cdot (1-p)^{n-k}, \quad (1)$$

где $P_n(k)$ – вероятность появления k событий B в КС длиной n , передача каждого бита которого рассматривается как независимое испытание; p – вероятность появления события B при передаче одного бита.

Для расчета вероятности искажения КС пакетом длиной k в формуле (1) задается длина кодового слова n , теоретическая вероятность p искажения одного бита в канале и анализируемое количество k искаженных бит. Результатом вычисления будет искомая вероятность искажения требуемого количества бит в кодовом слове заданной длины.

Если число испытаний n в схеме независимых испытаний Бернулли растет, а вероятность p уменьшается, то точная формула Бернулли (1) практически непригодна из-за громоздких вычислений и возникающих погрешностей округления. В этом случае при условии, что $n \cdot p \cdot (1-p) < 9$ рекомендуется пользоваться приближенными формулами Пуассона, которые получены на основе доказанной им теоремы. Теорема Пуассона построена на том факте, что, если в схеме независимых испытаний Бернулли число испытаний $n \rightarrow \infty$, а $p \rightarrow 0$ таким образом, что $n \cdot p \rightarrow \lambda > 0$, то при любых $k = 0, 1, 2, \dots$ справедливо свойство

$$P_n(k) = C_n^k \cdot p^k \cdot (1-p)^{n-k} \rightarrow \frac{\lambda^k}{k!} \cdot e^{-\lambda}.$$

Таким образом, при соблюдении условий теоремы Пуассона вместо громоздких вычислений по точной формуле (1) можно использовать приближенную формулу

$$P_n(k) = \frac{(n \cdot p)^k}{k!} \cdot e^{-n \cdot p}, \quad (2)$$

т.е. использовать формулу Пуассона для $\lambda = n \cdot p$.

Как указано выше, на практике пуассоновским приближением пользуются при $n \cdot p \cdot (1 - p) < 9$.

Вычислительная эффективность формулы (2) выше, чем у (1). Однако она имеет тот недостаток, что при больших n и k скорость вычислений резко снижается. В этом случае можно воспользоваться приближенной формулой локальной теоремы Муавра-Лапласа. Согласно этой теореме, если величина параметрического

критерия удовлетворяет условию $\gamma = \left| \frac{k - n \cdot p}{\sqrt{n \cdot p \cdot (1 - p)}} \right| < \varepsilon > 0$, т.е. ограничена,

можно воспользоваться формулой

$$P_n(k) \approx \frac{e^{-\frac{\gamma^2}{2}}}{\sqrt{2 \cdot \pi \cdot n \cdot p \cdot (1 - p)}}. \quad (3)$$

На практике приближением Муавра-Лапласа пользуются при выполнении соотношения $n \cdot p \cdot (1 - p) > 9$. Точность формулы (3) растет как с ростом величин n и k , так и по мере приближения значения p (и соответственно $1 - p$) к 0,5.

Таким образом, при расчёте параметров действующего в канале пакетного фона ошибок необходимо учитывать величину $n \cdot p \cdot (1 - p)$. Для удобства выбора аппроксимирующих формул (2) или (3) можно воспользоваться табл. 1, в которой приведены результаты расчёта для различных стандартных длин КС и различных значений побитовой вероятности ошибки.

Таблица 1

Значения критерия выбора аппроксимирующей формулы вероятности пакетной ошибки

Вероятность	Длина кодового слова бит					
	32	64	128	256	512	1024
0,01	0,317	0,634	1,267	2,534	5,069	10,138
0,02	0,627	1,254	2,509	5,018	10,035	20,070
0,03	0,931	1,862	3,725	7,450	14,899	29,798
0,05	1,52	3,04	6,08	12,16	24,320	48,640
0,1	2,88	5,76	11,52	23,04	46,080	92,160
0,2	5,12	10,24	20,48	40,96	81,920	163,84
0,3	6,72	13,44	26,88	53,76	107,52	215,04

Практическое исследование связи вероятностей возникновения одиночных и пакетных ошибок. Результаты расчета вероятностей с использованием функций (1)–(3) проиллюстрированы столбчатыми диаграммами на рис. 1–6 и приведены в табл. 2–7, которые можно использовать при решении задач проектирования каналов связи. На диаграммах приведены иллюстративные данные расчета вероятностей появления пакетных ошибок различной величины для кодовых слов длиной от 32 до 1024 бит. В таблицах те же данные приведены в численном виде, и могут быть использованы для оценки вероятностей появления пакетных ошибок разной величины при использовании КС соответствующей длины.

На рис. 2–4 представлены столбчатые диаграммы, иллюстрирующие зависимость вероятностей появления в 32–128-битных КС пакетных ошибок размером от 0 до 9 при вероятности искажения 1 бита $p=0,1$. Из диаграмм видно, что вероятностно значимая величина пакета для 32-битного КС не превышает 9, 64-битного – 16, а для 128-битного – 26.

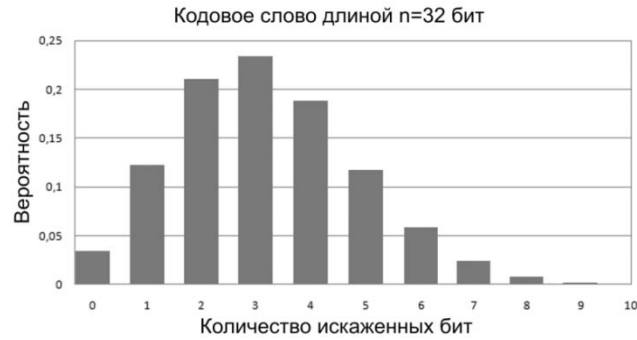


Рис. 2. Вероятностная диаграмма пакетных ошибок в 32-битном КС при $p=0,1$

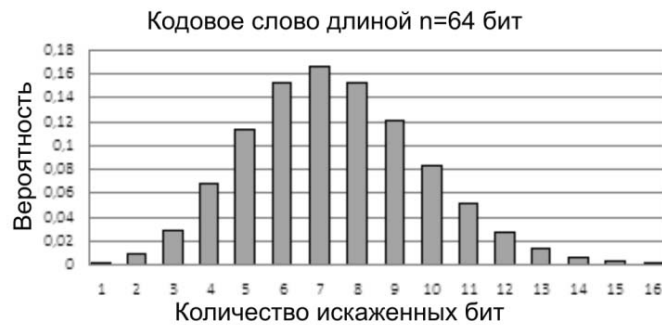


Рис. 3. Вероятностная диаграмма пакетных ошибок в 64-битном КС при $p=0,1$

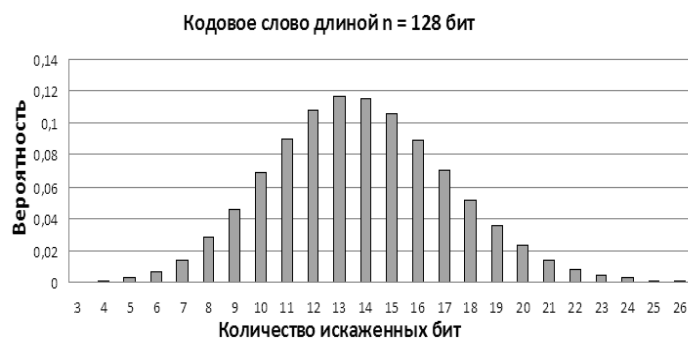


Рис. 4. Вероятностная диаграмма пакетных ошибок в 128-битном КС при $p=0,1$

Далее приведены вероятностные диаграммы для 256-, 512- и 1024-битных кодовых слов. Хорошо видно, что с ростом размерности КС вся диаграмма и её максимум смещаются в область больших значений ошибок, и увеличивается количество вероятностно значимых пакетов ошибок. Однако максимум вероятности пакетной ошибки при этом уменьшается. Это естественно, в связи с тем, что сумма вероятностей всех позиций диаграммы всегда равна единице.

Для стадии выбора и расчёта параметров кодирующей системы наиболее информативна правая нисходящая ветвь вероятностной диаграммы, по наибольшему

пакету ошибок этой ветви, вероятность которого входит в заданный проектировщиком диапазон. Так, из рис. 4 видно, что для 256-битного КС минимальный из максимальных пакет ошибок, вероятность появления которого не превышает 0,5 %, составляет 38. Исходя из этого значения следует выбирать кодек канала.

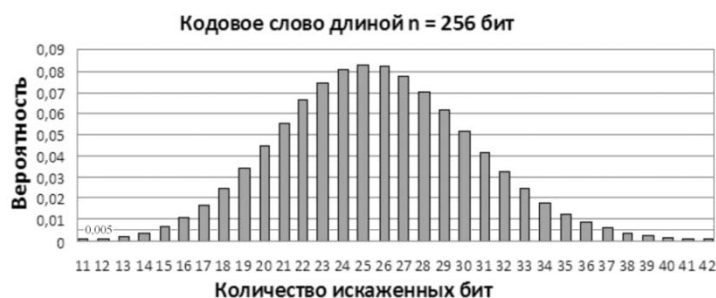


Рис. 5. Вероятностная диаграмма пакетных ошибок в 256 -битном КС при $p = 0,1$

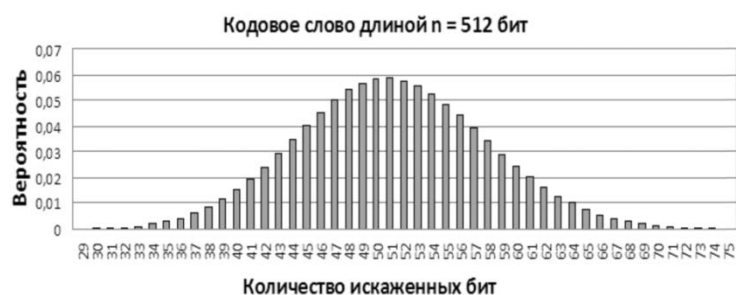


Рис. 6. Вероятностная диаграмма пакетных ошибок в 512 -битном КС при $p = 0,1$

Структурой приведённых ниже табл. 2–8 предусмотрено указание в заголовках столбцов теоретических значений вероятностей (p_i) искажения в сигнале одного бита кодового слова. При этом таблицы состоят из двух блоков – в верхнем помещены данные для побитовых вероятностей от 0,01 до 0,05, а в нижнем – для диапазона 0,06–0,1. В столбцах k указано количество бит, которые предположительно могут быть искажены в канале связи с битовой вероятностью помехи p_i , а в столбцах $P_i(k)$ – вероятность такого пакетного искажения. Значения k , расположенные по строкам, не идентичны. Они начинаются с количества ошибок, имеющих наибольшую вероятность появления пакетом, и заканчиваются при значениях пакетной вероятности менее 10^{-6} . Если расчетная вероятность искажения заданного количества бит не превышает этого значения, в ячейке таблицы проставляется 0.

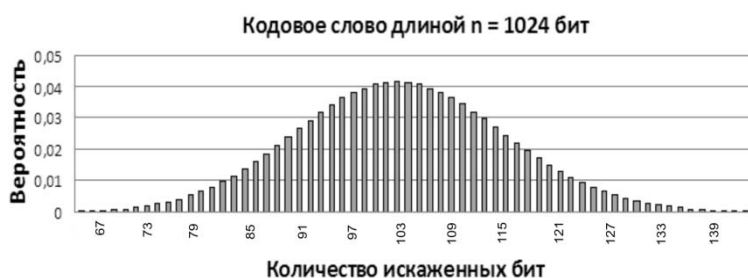


Рис. 7. Вероятностная диаграмма пакетных ошибок в 1024 -битном КС при $p = 0,1$

Таблица 2

Расчет вероятности искажения заданного числа бит
для длины кодового слова $n = 32$ бит

$p_1 = 0,01$		$p_2 = 0,02$		$p_3 = 0,03$		$p_4 = 0,04$		$p_5 = 0,05$	
k	$p_1(k)$	k	$p_2(k)$	k	$p_3(k)$	k	$p_4(k)$	k	$p_5(k)$
0	0,724980	0	0,523883	0	0,377308	1	0,361092	1	0,326251
1	0,234337	1	0,342128	1	0,373418	2	0,233205	2	0,266152
2	0,036689	2	0,108224	2	0,179010	3	0,097169	3	0,140080
3	0,003706	3	0,022087	3	0,055364	4	0,029353	4	0,053452
4	0,000271	4	0,003268	4	0,012414	5	0,006849	5	0,015754
5	0,000015	5	0,000373	5	0,002150	6	0,001284	6	0,003731
6	0,000001	6	0,000034	6	0,000299	7	0,000199	7	0,000729
7	0	7	0,000003	7	0,000034	8	0,000026	8	0,000120
8	0	8	0	8	0,000003	9	0,000003	9	0,000017
9	0	9	0	9	0	10	0	10	0,000002
$p_6 = 0,06$		$p_7 = 0,07$		$p_8 = 0,08$		$p_9 = 0,09$		$p_{10} = 0,1$	
k	$P_6(k)$	k	$P_7(k)$	k	$P_8(k)$	k	$P_9(k)$	k	$P_{10}(k)$
1	0,282010	2	0,275528	2	0,260194	2	0,237251	3	0,233622
2	0,279010	3	0,207387	3	0,226255	3	0,234644	4	0,188196
3	0,178091	4	0,113171	4	0,142639	4	0,168248	5	0,117100
4	0,082415	5	0,047702	5	0,069459	5	0,093183	6	0,058550
5	0,029459	6	0,016157	6	0,027180	6	0,041472	7	0,024163
6	0,008462	7	0,004517	7	0,008779	7	0,015234	8	0,008390
7	0,002006	8	0,001062	8	0,002385	8	0,004708	9	0,002486
8	0,000400	9	0,000213	9	0,000553	9	0,001242	10	0,000635
9	0,000068	10	0,000037	10	0,000111	10	0,000282	11	0,000141
10	0,000010	11	0,000006	11	0,000019	11	0,000056	12	0,000027
11	0,000001	12	0,000001	12	0,000003	12	0,000010	13	0,000005

Таблица 3

Расчет вероятности искажения заданного числа бит
для длины кодового слова $n = 64$ бит

$p_1 = 0,01$		$p_2 = 0,02$		$p_3 = 0,03$		$p_4 = 0,04$		$p_5 = 0,05$	
k	$p_1(k)$	k	$p_2(k)$	k	$p_3(k)$	k	$p_4(k)$	k	$p_5(k)$
0	0,525596	1	0,358470	1	0,281787	2	0,256701	3	0,227935
1	0,339780	2	0,230445	2	0,274524	3	0,221048	4	0,182948
2	0,108112	3	0,097194	3	0,175469	4	0,140457	5	0,115546
3	0,022569	4	0,030249	4	0,082760	5	0,070229	6	0,059800
4	0,003477	5	0,007408	5	0,030715	6	0,028774	7	0,026078
5	0,000421	6	0,001487	6	0,009341	7	0,009934	8	0,009779
6	0,000042	7	0,000251	7	0,002394	8	0,002949	9	0,003203
7	0,000004	8	0,000037	8	0,000527	9	0,000765	10	0,000927
8	0	9	0,000005	9	0,000102	10	0,000175	11	0,000240
9	0	10	0,000001	10	0,000017	11	0,000036	12	0,000056
10	0	11	0	11	0,000003	12	0,000007	13	0,000012
11	0	12	0	12	0	13	0,000001	14	0,000002
$p_6 = 0,06$		$p_7 = 0,07$		$p_8 = 0,08$		$p_9 = 0,09$		$p_{10} = 0,1$	
k	$P_6(k)$	k	$P_7(k)$	k	$P_8(k)$	k	$P_9(k)$	k	$P_{10}(k)$
3	0,206545	5	0,196065	5	0,182450	5	0,172531	6	0,166333
4	0,201051	6	0,177091	6	0,156008	6	0,167791	7	0,153132
5	0,153997	7	0,131073	7	0,112403	7	0,137499	8	0,121229
6	0,096658	8	0,081744	8	0,069641	8	0,096892	9	0,083813

Окончание табл. 3

$p_6 = 0,06$		$p_7 = 0,07$		$p_8 = 0,08$		$p_9 = 0,09$		$p_{10} = 0,1$	
k	$P_6(k)$	k	$P_7(k)$	k	$P_8(k)$	k	$P_9(k)$	k	$P_{10}(k)$
7	0,051120	9	0,043839	9	0,037680	9	0,059626	10	0,051219
8	0,023249	10	0,020531	10	0,018021	10	0,032434	11	0,027938
9	0,009234	11	0,008500	11	0,007693	11	0,015747	12	0,013710
10	0,003242	12	0,003141	12	0,002954	12	0,006879	13	0,006093
11	0,001016	13	0,001044	13	0,001028	13	0,002721	14	0,002466
12	0,000286	14	0,000314	14	0,000326	14	0,000980	15	0,000913
13	0,000073	15	0,000086	15	0,000094	15	0,000323	16	0,000311
14	0,000017	16	0,000022	16	0,000025	16	0,000098	17	0,000098
15	0,000004	17	0	17	0,000006	17	0,000027	18	0,000028
16	0,000001	18	0	18	0,000001	18	0,000007	19	0,000008
17	0	19	0	19	0	19	0,000002	20	0,000002

Таблица 4

Расчет вероятности искажения заданного числа бит
для длины кодового слова $n = 128$ бит

$p_1 = 0,01$		$p_2 = 0,02$		$p_3 = 0,03$		$p_4 = 0,04$		$p_5 = 0,05$	
k	$p_1(k)$	k	$p_2(k)$	k	$p_3(k)$	k	$p_4(k)$	k	$p_5(k)$
1	0,357174	2	0,254994	3	0,204674	5	0,178730	6	0,162326
2	0,229096	3	0,218566	4	0,197817	6	0,152665	7	0,148901
3	0,097192	4	0,139392	5	0,151727	7	0,110864	8	0,118533
4	0,030679	5	0,070549	6	0,096198	8	0,069867	9	0,083181
5	0,007685	6	0,029515	7	0,051854	9	0,038815	10	0,052098
6	0,001591	7	0,010498	8	0,024256	10	0,019246	11	0,029414
7	0,000280	8	0,003241	9	0,010003	11	0,008602	12	0,015094
8	0,000043	9	0,000882	10	0,003681	12	0,003495	13	0,007089
9	0,000006	10	0,000214	11	0,001221	13	0,001299	14	0,003065
10	0,000001	11	0,000047	12	0,000368	14	0,000445	15	0,001226
11	0	12	0,000009	13	0,000102	15	0,000141	16	0,000456
12	0	13	0,000002	14	0,000026	16	0,000041	17	0,000158
13	0	14	0	15	0,000006	17	0,000011	18	0,000051
14	0	15	0	16	0,000001	18	0,000003	19	0,000016
15	0	16	0	17	0	19	0,000001	20	0,000004
16	0	17	0	18	0	20	0	21	0,000001

$p_6 = 0,06$		$p_7 = 0,07$		$p_8 = 0,08$		$p_9 = 0,09$		$p_{10} = 0,1$	
k	$P_6(k)$	k	$P_7(k)$	k	$P_8(k)$	k	$P_9(k)$	k	$P_{10}(k)$
7	0,148279	9	0,136627	10	0,129896	11	0,123234	12	0,116777
8	0,143152	10	0,122377	11	0,121168	12	0,118833	13	0,115779
9	0,121832	11	0,098811	12	0,102729	13	0,104870	14	0,105671
10	0,092540	12	0,072514	13	0,079709	14	0,085197	15	0,089233
11	0,063364	13	0,048703	14	0,056935	15	0,064038	16	0,070023
12	0,039434	14	0,030112	15	0,037627	16	0,044730	17	0,051259
13	0,022460	15	0,017225	16	0,023108	17	0,029145	18	0,035122
14	0,011776	16	0,009157	17	0,013238	18	0,017775	19	0,022593
15	0,005713	17	0,004541	18	0,007099	19	0,010178	20	0,013681
16	0,002575	18	0,002108	19	0,003574	20	0,005486	21	0,007818
17	0,001083	19	0,000918	20	0,001694	21	0,002790	22	0,004225
18	0,000426	20	0,000377	21	0,000757	22	0,001342	23	0,002163
19	0,000158	21	0,000146	22	0,000320	23	0,000612	24	0,001052
20	0,000055	22	0,000053	23	0,000128	24	0,000265	25	0,000486
21	0,000018	23	0,000019	24	0,000049	25	0,000109	26	0,000214

Окончание табл. 4

$p_6 = 0,06$		$p_7 = 0,07$		$p_8 = 0,08$		$p_9 = 0,09$		$p_{10} = 0,1$	
k	$P_6(k)$	k	$P_7(k)$	k	$P_8(k)$	k	$P_9(k)$	k	$P_{10}(k)$
22	0,000006	24	0,000006	25	0,000018	26	0,000043	27	0,000090
23	0,000002	25	0,000002	26	0,000006	27	0,000016	28	0,000036
24	0	26	0,000001	27	0,000002	28	0,000006	29	0,000014
25	0	27	0	28	0,000001	29	0,000002	30	0,000005
26	0	28	0	29	0	30	0,000001	31	0,000002
27	0	29	0	30	0	31	0	32	0,000001

Таблица 5

Расчет вероятности искажения заданного числа бит
для длины кодового слова $n = 256$ бит

$p_1 = 0,01$		$p_2 = 0,02$		$p_3 = 0,03$		$p_4 = 0,04$		$p_5 = 0,05$	
k	$p_1(k)$	k	$p_2(k)$	k	$p_3(k)$	k	$p_4(k)$	k	$p_5(k)$
2	0,254150	5	0,176949	7	0,146328	10	0,127250	12	0,114041
3	0,217354	6	0,151069	8	0,140860	11	0,118574	13	0,112656
4	0,138865	7	0,110109	9	0,120046	12	0,100870	14	0,102915
5	0,070695	8	0,069941	10	0,091705	13	0,078885	15	0,087387
6	0,029873	9	0,039332	11	0,063429	14	0,057051	16	0,069277
7	0,010777	10	0,019827	12	0,040052	15	0,038351	17	0,051476
8	0,003388	11	0,009049	13	0,023250	16	0,024069	18	0,035973
9	0,000943	12	0,003770	14	0,012481	17	0,014158	19	0,023716
10	0,000235	13	0,001444	15	0,006228	18	0,007833	20	0,014791
11	0,000053	14	0,000512	16	0,002901	19	0,004088	21	0,008749
12	0,000011	15	0,000168	17	0,001267	20	0,002019	22	0,004919
13	0,000002	16	0,000052	18	0,000520	21	0,000945	23	0,002634
14	0	17	0,000015	19	0,000202	22	0,000421	24	0,001346
15	0	18	0,000004	20	0,000074	23	0,000178	25	0,000657
$p_6 = 0,06$		$p_7 = 0,07$		$p_8 = 0,08$		$p_9 = 0,09$		$p_{10} = 0,1$	
k	$P_6(k)$	k	$P_7(k)$	k	$P_8(k)$	k	$P_9(k)$	k	$P_{10}(k)$
15	0,105097	17	0,097109	20	0,091952	23	0,086873	25	0,083057
16	0,101044	18	0,097051	21	0,089858	24	0,083412	26	0,081992
17	0,091054	19	0,091504	22	0,083465	25	0,076556	27	0,077605
18	0,077170	20	0,081616	23	0,073841	26	0,067270	28	0,070522
19	0,061701	21	0,069037	24	0,062336	27	0,056674	29	0,061606
20	0,046670	22	0,055506	25	0,050303	28	0,045842	30	0,051794
21	0,033477	23	0,042505	26	0,038863	29	0,035645	31	0,041955
22	0,022825	24	0,031060	27	0,028787	30	0,026675	32	0,032778
23	0,014823	25	0,021695	28	0,020473	31	0,019233	33	0,024721
24	0,009185	26	0,014508	29	0,013996	32	0,013375	34	0,018016
25	0,005441	27	0,009303	30	0,009209	33	0,008979	35	0,012697
26	0,003086	28	0,005727	31	0,005838	34	0,005824	36	0,008660
27	0,001678	29	0,003389	32	0,003570	35	0,003654	37	0,005722
28	0,000876	30	0,001930	33	0,002107	36	0,002218	38	0,003664
29	0,000440	31	0,001059	34	0,001202	37	0,001305	39	0,002276
30	0,000212	32	0,000560	35	0,000663	38	0,000744	40	0,001372
31	0,000099	33	0,000286	36	0,000354	39	0,000411	41	0,000803

Таблица 6

Расчет вероятности искажения заданного числа бит
для длины кодового слова $n = 512$ бит

$p_1 = 0,01$		$p_2 = 0,02$		$p_3 = 0,03$		$p_4 = 0,04$		$p_5 = 0,05$	
k	$p_1(k)$	k	$p_2(k)$	k	$p_3(k)$	k	$p_4(k)$	k	$p_5(k)$
5	0,176078	10	0,125985	15	0,103515	20	0,090089	25	0,080932
6	0,150289	11	0,117336	16	0,099446	21	0,087944	26	0,079785
7	0,109735	12	0,099975	17	0,089737	22	0,081781	27	0,075586
8	0,069970	13	0,078474	18	0,076323	23	0,072596	28	0,068908
9	0,039579	14	0,057082	19	0,061373	24	0,061631	29	0,060529
10	0,020109	15	0,038676	20	0,046789	25	0,050126	30	0,051291
11	0,009270	16	0,024518	21	0,033903	26	0,039121	31	0,041973
12	0,003909	17	0,014599	22	0,023402	27	0,029341	32	0,033206
13	0,001519	18	0,008193	23	0,015419	28	0,021176	33	0,025421
14	0,000547	19	0,004347	24	0,009717	29	0,014726	34	0,018849
15	0,000183	20	0,002187	25	0,005866	30	0,009879	35	0,013549
16	0,000058	21	0,001046	26	0,003398	31	0,006400	36	0,009448
17	0,000017	22	0,000476	27	0,001892	32	0,004008	37	0,006397
18	0,000005	23	0,000207	28	0,001013	33	0,002429	38	0,004209
19	0,000001	24	0,000086	29	0,000523	34	0,001426	39	0,002692
20	0	25	0,000034	30	0,000260	35	0,000811	40	0,001676
21	0	26	0,000013	31	0,000125	36	0,000448	41	0,001015
22	0	27	0,000005	32	0,000058	37	0,000240	42	0,000599
23	0	28	0,000002	33	0,000026	38	0,000125	43	0,000345
24	0	29	0,000001	34	0,000011	39	0,000063	44	0,000193
25	0	30	0	35	0,000005	40	0,000031	45	0,000106
26	0	31	0	36	0,000002	41	0,000015	46	0,000057
$p_6 = 0,06$		$p_7 = 0,07$		$p_8 = 0,08$		$p_9 = 0,09$		$p_{10} = 0,1$	
k	$P_6(k)$	k	$P_7(k)$	k	$P_8(k)$	k	$P_9(k)$	k	$P_{10}(k)$
30	0,074186	35	0,068958	41	0,064825	46	0,061538	51	0,058749
31	0,073626	36	0,068772	42	0,063215	47	0,060344	52	0,057871
32	0,070640	37	0,066594	43	0,060083	48	0,057816	53	0,055808
33	0,065584	38	0,062655	44	0,055689	49	0,054147	54	0,052708
34	0,058977	39	0,057318	45	0,050363	50	0,049589	55	0,048768
35	0,051412	40	0,051016	46	0,044460	51	0,044428	56	0,044220
36	0,043481	41	0,044206	47	0,038332	52	0,038954	57	0,039307
37	0,035705	42	0,037313	48	0,032290	53	0,033438	58	0,034262
38	0,028488	43	0,030698	49	0,026589	54	0,028110	59	0,029293
39	0,022101	44	0,024629	50	0,021410	55	0,023151	60	0,024574
40	0,016681	45	0,019279	51	0,016865	56	0,018685	61	0,020232
41	0,012258	46	0,014732	52	0,013001	57	0,014784	62	0,016352
42	0,008774	47	0,010994	53	0,009812	58	0,011470	63	0,012978
43	0,006121	48	0,008017	54	0,007253	59	0,008729	64	0,010117
44	0,004165	49	0,005714	55	0,005252	60	0,006518	65	0,007747
45	0,002765	50	0,003983	56	0,003727	61	0,004777	66	0,005830
46	0,001792	51	0,002715	57	0,002592	62	0,003436	67	0,004312
47	0,001134	52	0,001812	58	0,001768	63	0,002428	68	0,003135
48	0,000701	53	0,001184	59	0,001183	64	0,001684	69	0,002242
49	0,000424	54	0,000757	60	0,000777	65	0,001148	70	0,001576
50	0,000250	55	0,000475	61	0,000501	66	0,000769	71	0,001090
51	0,000145	56	0,000292	62	0,000317	67	0,000506	72	0,000742

Анализ закономерностей формирования значений, приведенных в таблицах, показал, что при практическом применении данных методик исследования существует возможность сразу оценить вероятность возникновения ошибки в кодовом слове в зависимости от его длины и использованного декодера. При этом «пакетность» ошибок и их расположения в коде не влияют на результаты декодирования.

Следует отметить, что данные таблиц указывают на однозначный характер влияния числа ошибок, параметров кода и вероятностного декодера на вероятность корректного восстановления кодового слова. Это указывает на полезность проведённых исследований и необходимость более тщательного анализа рассматриваемых алгоритмов и явлений.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. *Мозилевская Н.С., Скоробогат В.Р., Чудаков В.С.* Экспериментальное исследование декодеров кодов Рида–Маллера второго порядка // Вестник ДГТУ. – 2008. – № 3 (38), Т. 8.
2. *Сидельников В.М., Першаков А.С.* Декодирование кодов Рида–Маллера при большом числе ошибок // Проблемы передачи информации. – 1992. – № 3 (28). – С. 80–94.

Статью рекомендовал к опубликованию д.т.н., профессор А.Р. Гайдук.

Нейдорф Рудольф Анатольевич

Донской государственный технический университет.

E-mail: ran_pro@mail.ru.

344000, г. Ростов-на-Дону, пл. Гагарина, 1.

Тел.: 88632738727.

Кафедра программного обеспечения вычислительной техники и автоматизированных систем; зав. кафедрой; д.т.н., профессор.

Новиков Сергей Петрович

E-mail: n_serg7@mail.ru.

Кафедра программного обеспечения вычислительной техники и автоматизированных систем; ст. преподаватель; аспирант.

Чудаков Виктор Сергеевич

E-mail: victor.chudakov@gmail.com.

Кафедра программного обеспечения вычислительной техники и автоматизированных систем; магистрант.

Nejdorf Rudolf Anatolevich

Don state technical university, Rostov-on-Don.

E-mail: ran_pro@mail.ru.

1, Gagarin Square, Rostov-on-Don, 344000, Russia.

Phone: +78632738727.

The Department of the Software of Computer Facilities and the Automated Systems; Head the Department; Dr. of Eng. Sc., Professor.

Novikov Sergei Petrovich

E-mail: n_serg7@mail.ru.

The Department of the Software of Computer Facilities and the Automated Systems; Postgraduate Student.

Chudakov Viktor Sergeevich

E-mail: victor.chudakov@gmail.com.

The Department of the Software of Computer Facilities and the Automated Systems; Undergraduate.