УДК 681.391

К.В. Вековищева, В.В.Костюченко

ИСПРАВЛЯЮЩАЯ СПОСОБНОСТЬ НЕКОТОРЫХ КОДОВ

Воронежский институт высоких технологий
Концерн радиостроения «Вега»

В данной работе рассматривается задача кодирования данных, которые могут храниться на носителях информации или передаваться по системам связи. Приведена структура систем связи, дано описание основных входящих в нее составляющих. Проведена классификация помехоустойчивых кодов. Дано описание программного продукта, с использованием которого демонстрируется работа помехоустойчивых кодов. Приведены результаты исследований исправляющих способностей кодов Хемминга, Боуза-Рой-Чоудхури-Хоквингема и Рида-Маллера для текстового файла, а также для файла, имеющего формат видео. Установлено, что на основе кода Хемминга можно хорошо исправлять одиночные ошибки, но он плохо работает для множественных. На основе кода Рида-Маллера, также исправляются разные ошибки, но в нем искажается меньше битов, чем для кода Боуза-Рой-Чоудхури-Хоквингема.

Ключевые слова: помехоустойчивое кодирование, система связи, алгоритм, обработка информации.

В существующих условиях можно наблюдать, как непрерывным образом идет рост объемов информации, которая как передается, так и принимается. Поэтому весьма актуальными являются проблемы, связанные с ее сохранением [1, 2]. В памяти компьютеров могут возникать ошибки вследствие того, существуют всплески напряжения в линии электропередач и в связи с другими причинами.

При передаче информации во многих случаях существуют помехи, также ведущие к ошибкам. Чтобы обеспечить борьбу с такими ошибками, была проведена разработка специальных способов, в рамках которых кодируется информация, они дают возможности для обнаружения и исправления возможных ошибок. На настоящий момент известно большое число разных типов помехоустойчивого кодирования.

Определенные из них являются настолько сложными, что для них требуется формировать специальный математический аппарат, для других же, можно сказать, что они являются простыми и понятными. Степень эффективности различных подходов кодирования существенным образом отличается.

Проведение изучения способов кодирования часто является проблемой вследствие того, что материал излишним образом математизирован и недостаточно нагляден [3].

Код представляет собой форму представления сообщений, которая не зависит от того какая их физическая суть. В этом отличие кодов от сигналов, которые дают определение физического представления сообщений в системах связи.

Историю теории кодирования, в рамках которой можно контролировать ошибки, связывают с тем, что Клод Шеннон в 1948 г. опубликовал свою статью [4]. Им было показано, что для каждого канала можно поставить в соответствие пропускную способность, она измеряется в битах в секунду. За счет применения кодов, которые контролируют ошибки, по данному каналу можно осуществить формирование такой системы связи, что значение вероятности ошибки, относящейся к выходу будет сколь угодно мало.

Затем был большой прорыв, основанный на том, что Боуз и Рой-Чоудхури и Хоквингем смогли определить большой класс кодов, в рамках которого идет исправление кратных ошибок (говорят о кодах БЧХ), а Рид и Соломон определили такой соответствующий класс кодов, имеющий связь с кодами БЧХ при недвоичных каналах.

Если в сообщениях существуют внутренние корреляционные связи, когда одно из сообщений определенным образом зависит от другого, мы можем это наблюдать при процессах передачи текста на естественном языке, тогда степень помехоустойчивости любого кода мы можем повысить вследствие того, что есть статистические связи между сообщениями.

В тех случаях, когда такие связи являются слабыми, или неизвестными, или мы их не можем применять для того, чтобы повысить помехоустойчивость, то тогда форму, в которой представляется сообщение, требуется делать избыточной.

Для определенных условий делают увеличение числа символов для кода сообщения, а среди кодовых символов делают введение искусственных корреляционных связей. Тогда помехоустойчивые коды имеют название избыточных. Вследствие того, что избыточность вводится в код, возникают возможности для того, что кроме того, что обнаруживаются и исправляются ошибки, повышается энергетическая эффективность линий связи, идет сужение частотного спектра передаваемого сигнала, сокращается время установления связи, поскольку повышается помехозащищенность тракта синхронизации, идет улучшение корреляционных свойств ансамбля сигналов, за счет простых средств реализуется разнесенный прием [5-7].

Тип помехоустойчивого кода определяется структурой систем связи, на Рисунке 1 можно увидеть ее обобщенную схему [8]. Мы подразумеваем системы связи, в которых идет передача лишь дискретных сообщений. Для современных систем, в которых передаются дискретные сообщения, идет поступление последних на вход систем, большей частью, от нескольких источников.

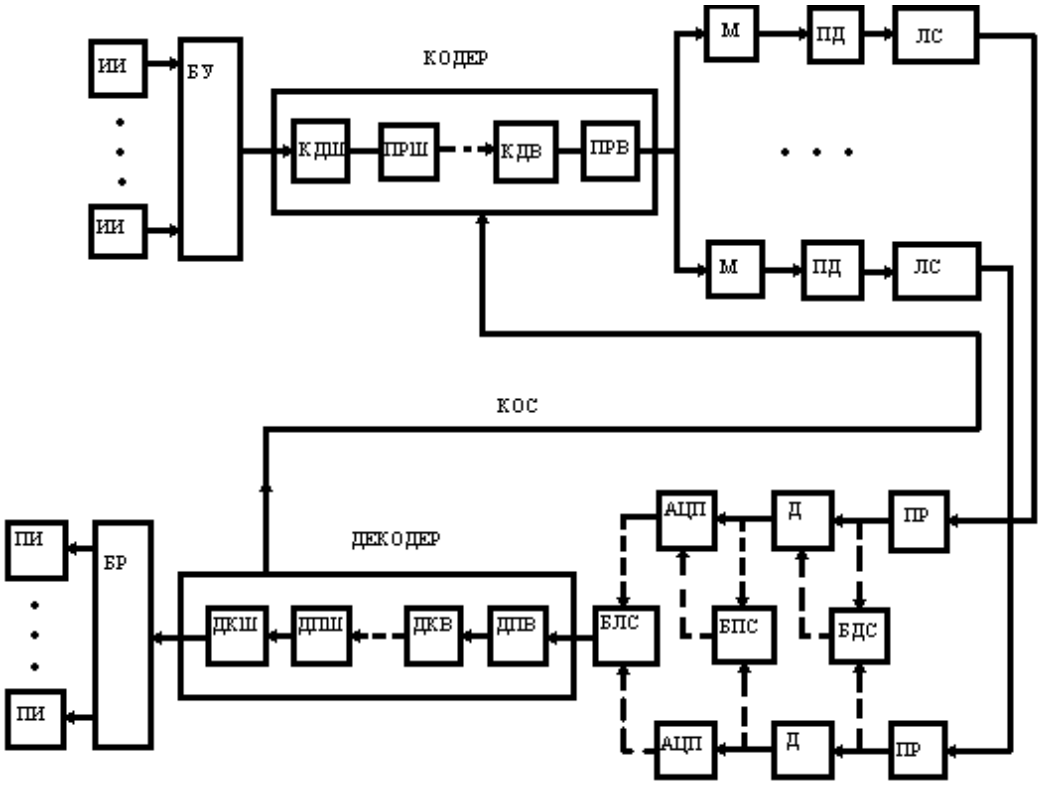

Рисунок 1 — Структура систем связи

ИИ является источником информации; БУ является блоком уплотнения сообщений; КДШ, КДВ являются внешним и внутренним кодером; ПРШ, ПРВ являются внешним и внутренним перемежителем; М обозначает модулятор; ПД является передатчиком; ЛС обозначает линию связи; ПР является приемником; Д обозначает демодулятор; АЦП является аналого-цифровым преобразователем; БДС, БПС, БЛС являются блоками, связанными с додетекторным, последетекторным, логическим сложением; ДПШ, ДПВ обозначают внешний и внутренний деперемежитель; ДКШ, ДКВ обозначает внешний и внутренний декодер; БР является блоком разуплотнения сообщений; ПИ обозначает получателя информации; КОС является каналом обратной связи.

Существуют случаи, когда возникающая ошибка для одного символа кода бут являться причиной ошибок для других смежных с ним символов, что определяет возникновение пакета ошибок для входа декодера, в котором идет исправление ошибок.

Схему, которую мы привели на Рисунке 1, представляют на практике разным образом, это определяется конкретной реализацией ее. Для каналов связи существуют искажения по сигналам, совокупность шумов, помех, для которых в дискретных каналах есть проявление как переход одних значений символов в другие - ложные (события, заключающиеся в том, что будут ошибки) или неиспользуемые (события, которые влекут стирание).

Даже если вероятность ошибок очень мала, значение скорости передачи будет меньше, чем пропускная способность. В присутствии ошибок в канале передачи максимальное значение скорости может быть достигнуто за счет того, что используется помехоустойчивое кодирование. При этом будет вводиться избыточность в передаваемые сигналы: для времени, частоты или амплитуды. Когда существует согласование кода и канала, то можно говорить о том, что введение избыточности будет оправданным. Когда нет согласования кода и канала, то ошибки не только не исправляются, но и идет их размножение кодами. То есть помехоустойчивое кодирование дает не пользу, а вред.

На Рисунке 2 приведена классификация помехоустойчивых кодов.

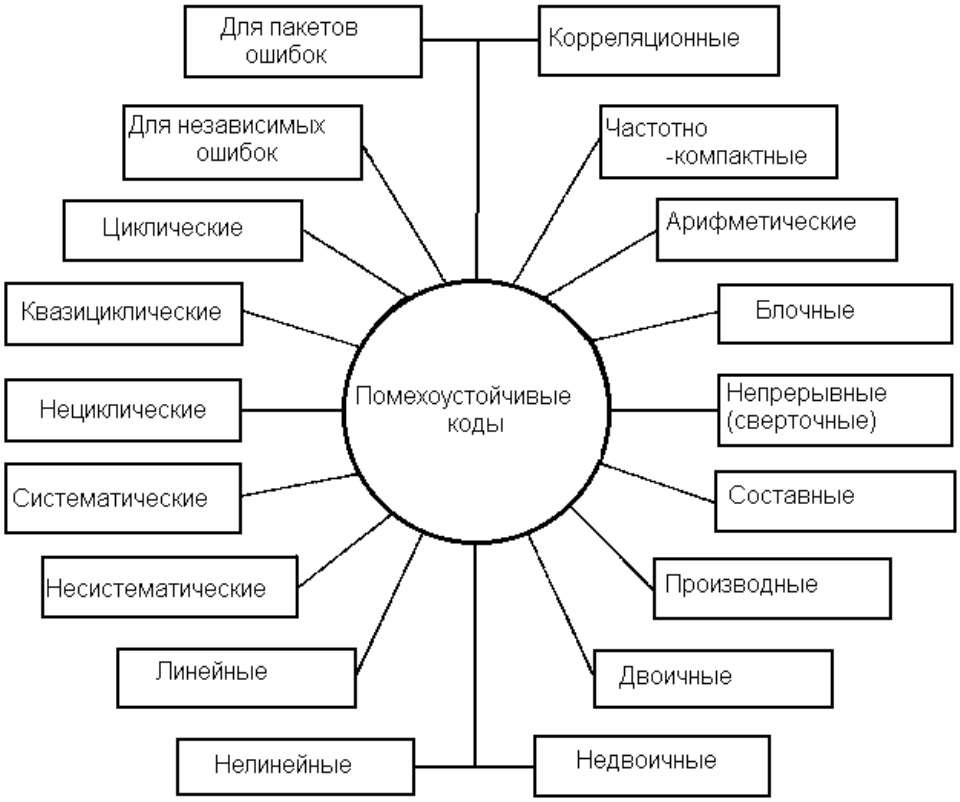

Рисунок 2 — Демонстрация классификации помехоустойчивых кодов

Рисунок 3 иллюстрирует схему связи, которая представляется общим образом [9].

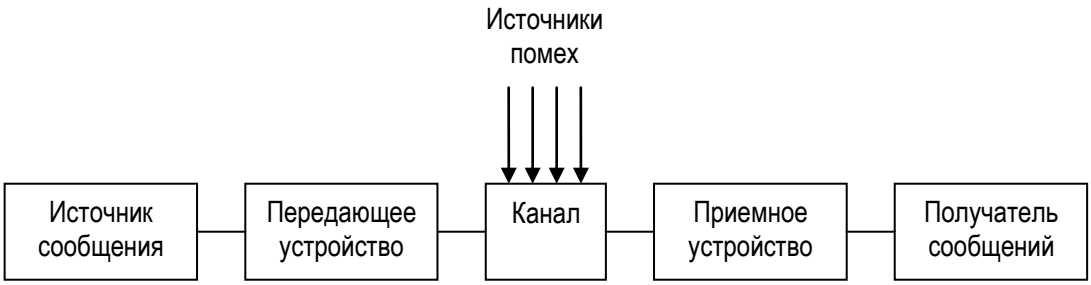

Рисунок 3 – Демонстрация схемы системы связи

Передающее устройство включает в себя всю аппаратуру, при помощи которой происходит процесс преобразования сообщений в соответствующие сигналы, приемное устройство – это аппаратура, при помощи которой происходит восстановление сообщения.

Нами был разработан программный продукт, с применением которого были проведены исследования по восстанавливающим способностям кодов [10-12].

Окна программы, относящиеся к анализу кода Хемминга, даны на Рисунке 4 и Рисунке 5.

В поле, которое относится к исходному тексту, нами вводится сообщение, которое требуется кодировать.

Поле, имеющее название «HEX», дает вывод в виде последовательности байтов, используется представление в виде шестнадцатеричной системы счисления.

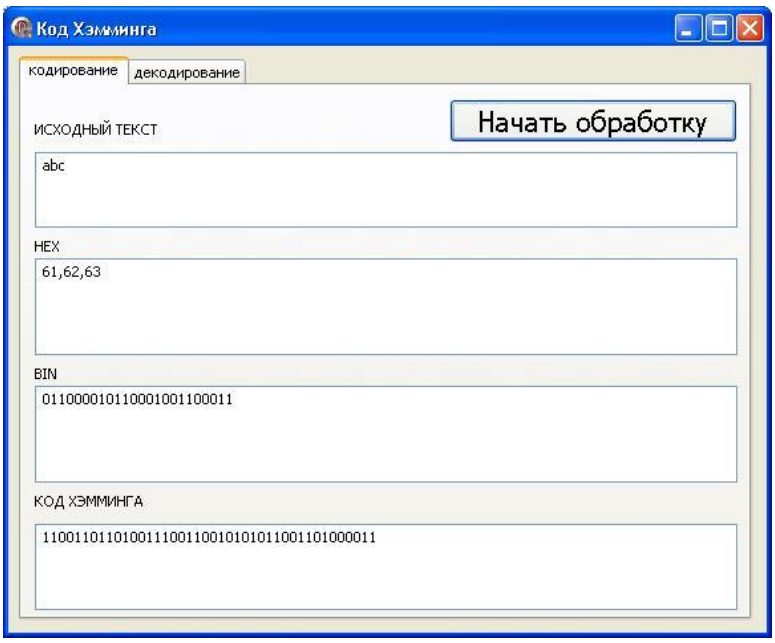

Рисунок 4 – Окно кодирования на основе кода Хемминга

Поле, имеющее название «BIN», дает вывод тексте как двоичный код.

Поле, имеющее название «Код Хемминга», дает вывод закодированного исходного сообщения.

Когда мы нажимаем кнопку «Начать обработку» то внутри поля «Код Хемминга» для вкладки «Декодирование» (Рисунок 5) идет вывод закодированного исходного сообщения. Для этого поля идет имитация помех, искажаются биты.

В поле, относящемуся к исходному тексту, идет вывод исправленного текста.

Над этим полем идет вывод числа найденных и исправленных ошибок.

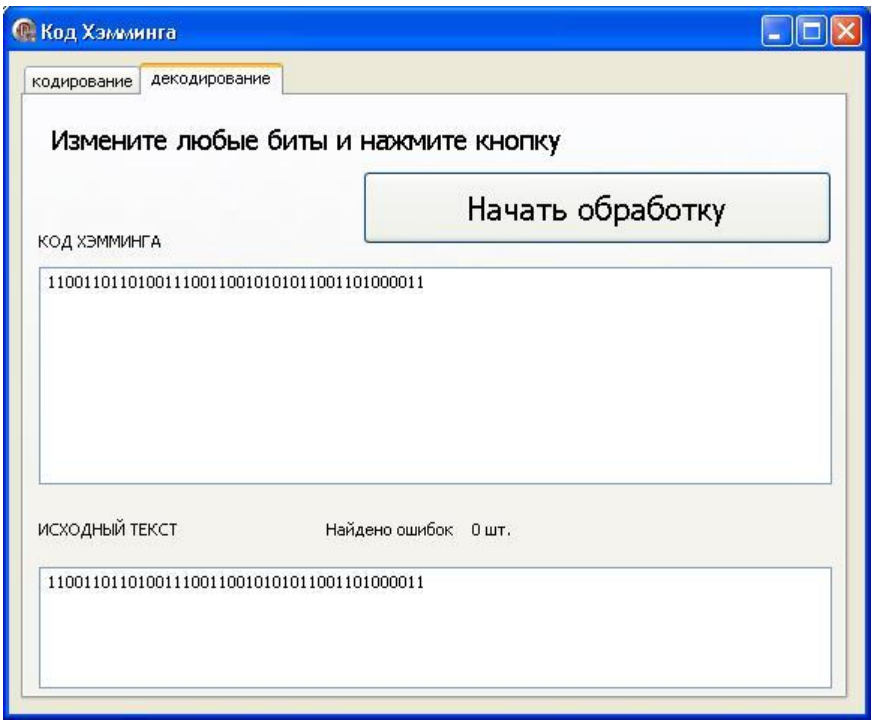

Рисунок 5 – Окно декодирования на основе кода Хемминга

Когда мы убираем контрольные биты (1,2,4,8), то будет получено исходное сообщение.

В программе предусмотрена реализация кодов БЧХ и Рида-Маллера.

Было проведено сравнение исправляющей способности кодов.

Для кодов мы выбрали такие характеристики:

в коде Хемминга – 8;5 (5 информационных бита, 3 контрольных);

код БЧХ - длина информационного слова – 16, длина кодового слова – 31, минимальное расстояние кода, количество исправляемых ошибок – 3;

код Рида-Маллера - длина информационного слова – 17, длина кодового слова – 32, минимальное расстояние кода, количество

исправляемых ошибок – 4, порядок кода Рида-Маллера – 2, определяет значение длины кодового слова – 5.

Результаты исследований исправляющих способностей кодов Хемминга, БЧХ и Рида-Маллера даны в Таблицах 1-3. В ходе испытаний рассматривались файлы, в которых содержался исходный текст, который дан в этих таблицах.

Таблица 1 – Исправляющая способность кода Хемминга

	Данные по исходному тексту	Число возникших ошибок	Число исправленных ошибок	Число битов, подвергшихся искажению в исходном тексте	Значение искаженных битов, %
1	20	1	1	0	0
2	Table	1	1	0	0
3	Ceiling	1	1	0	0
4	30	2	2	0	0
5	Table	2	2	0	0
6	30	2	0	2(2)	15
7	Table	3	0	3(1)	15
8	Table	4	1	3(0)	15

Таблица 2 – Исправляющая способность двоичного кода БЧХ

	Данные по исходному тексту	Число возникших ошибок	Число исправленных ошибок	Число битов, подвергшихся искажению в исходном тексте	Значение искаженных битов, %
1	20	1	1	0	0
2	Table	1	1	0	0
3	Ceiling	1	1	0	0
4	30	2	2	0	0
5	Table	2	2	0	0
6	30	2	2	0	0
7	Table	3	3	0	0
8	Table	4	0	4	17

Таблица 3 – Исправляющая способность кода Рида-Маллера

	Данные по исходному тексту	Число возникших ошибок	Число исправленных ошибок	Число битов, подвергшихся искажению в исходном тексте	Значение искаженных битов, %
1	20	1	1	0	0
2	Table	1	1	0	0
3	Ceiling	1	1	0	0
4	30	2	2	0	0
5	Table	2	2	0	0
6	30	2	2	0	0
7	Table	3	3	0	0
8	Table	4	4	2	9

Как видно были взяты несколько видов ошибок: одиночные, а также последовательные множественные. В 1, 2, 3, 4, 5 было проведено рассмотрение одиночных ошибок, в для остальных случаев – множественных.

Исследовалась избыточность кодов БЧХ и РМ для разных файлов.

В Таблице 4 можно увидеть результаты таких исследований – каким образом размеры файла и его вид оказывают влияние на характеристики избыточности.

Таблица 4 – Характеристики избыточности кодов

Текстовый файл txt

	Размер файла (Количество бит)	Процент восстановления
Исходный файл	205032	100
Использование кода БЧХ	609573	35,41
Использование кода Рида-Маллера	407360	51,86

Видеофайл, формат avi

Исходный файл	155768	100
Код БЧХ	477504	34
Код Рида-Маллера	351736	51,97

Выводы. На основе кода Хемминга можно хорошо исправлять одиночные ошибки, но он плохо работает для множественных. Помимо этого, код Хемминга оказывает влияние на искажение тех битов, для которых не было искажения. На основе кода БЧХ хорошо исправляются

разные ошибки, больший процент ошибок наблюдается для множественных. На основе кода Рида-Маллера, также исправляются разные ошибки, но в нем искажается меньше битов, чем для кода БЧХ. Избыточность кода растет при увеличении размера исходных файлов.

ЛИТЕРАТУРА

1. Пахомова А.С.Целенаправленные угрозы компьютерного шпионажа: признаки, принципы и технологии реализации / А.С.Пахомова, О.Н.Чопоров, К.А.Разинкин // Информация и безопасность. 2013. Т. 16. № 2. С. 211-214.
2. Львович И.Я. Снижение количества ошибок распознавания сканированных рукописных текстов / И.Я.Львович, Я.Е.Львович, А.А.Мозговой, А.П.Преображенский, О.Н.Чопоров // Цифровая обработка сигналов. 2016. № 4. С. 43-47.
3. Преображенский А.П. Особенности помехоустойчивого кодирования в каналах связи / А.П.Преображенский // Вестник Воронежского института высоких технологий. 2016. № 3 (18). С. 75-77.
4. Shannon C. E. A Mathematical Theory of Communication / C.E.Shannon // Bell System Technical Journal. 1948. Т. 27. С. 379-423, 623-656.
5. Воронов А.А. Обеспечение системы управления рисками при возникновении угроз информационной безопасности / А.А.Воронов, И.Я.Львович, Ю.П.Преображенский, В.А.Воронов // Информация и безопасность. 2006. Т. 9. № 2. С. 8-11.
6. Попов Е.А. Риск-анализ информационно-телекоммуникационных систем при аддитивном характере параметра нергулярности / Е.А.Попов, Н.Н.Корнеева, О.Н.Чопоров, А.В.Заряев // Информация и безопасность. 2013. Т. 16. № 4. С. 482-485.
7. Ермилов Е.В. Риск-анализ распределенных систем на основе параметров рисков их компонентов / Е.В.Ермилов, Е.А.Попов, М.М.Жуков, О.Н.Чопоров // Информация и безопасность. 2013. Т. 16. № 1. С. 123-126.
8. Калашников А.О. Атаки на информационно-технологическую инфраструктуру критически важных объектов: оценка и регулирование рисков / А.О.Калашников, Е.В.Ермилов, О.Н.Чопоров, К.А.Разинкин, Н.И.Баранников // монография / под ред. чл.-корр. РАН Д.А. Новикова. Воронеж, Издательство: ООО "Издательство "Научная книга", 2013, 159 с.
9. Львович И.Я. Основы информатики / И.Я.Львович, Ю.П.Преображенский, В.В.Ермолова / учебное пособие, Воронеж, Издательство: Воронежский институт высоких технологий, 2014, 339 с.

10. Финк Л.М. Теория передачи дискретных сообщений / Л.М.Финк // Издательство "Советское радио", 1970, 728 с.
11. Харкевич А.А. Борьба с помехами / А.А.Харкевич // Издательство "Наука", главная редакция физико-математической литературы. Москва, 1965. 275 с.
12. Блейхуд Р. Теория и практика кодов контролирующих ошибки / Р.Блейхуд // Пер. с англ.- М.: Мир, 1986. 576 с.

K. V. Vekovischeva, V.V.Kostyuchenko

CORRECTING CAPABILITIES OF SOME CODES

Voronezh Institute of high technologies
Radio engineering Corporation "VEGA"

In this paper we consider the problem of coding the data that can be stored on data carriers or transmitted over communication systems. The structure of communication systems, a description of the main constituent components. The classification of error-correcting codes. This description of a software product, which demonstrates how error-correcting codes. The results of research abilities-correcting codes, Hamming, Bose-Roy-Chowdhury-Hoquinghem and reed-Muller for the text file and for a file with the video format. Found that based on the Hamming code can be good to correct single errors, but it does not work for multiple. On the basis of the reed-müller code, also corrected various errors, but it is distorted less bits than code Bose-Roy-Chowdhury-Hoquinghem.

Keywords: error-correcting coding, communication system, algorithm, information processing.

REFERENCES

1. Pakhomova A.S.Tselenapravlennye ugrozy komp'yuternogo shpionazha: priznaki, printsipy i tekhnologii realizatsii / A.S.Pakhomova, O.N.Choporov, K.A.Razinkin // Informatsiya i bezopasnost'. 2013. Vol.16. No. 2. pp.211-214.
2. L'vovich I.Ya. Snizhenie kolichestva oshibok raspoznavaniya skanirovannykh rukopisnykh tekstov / I.Ya.L'vovich, Ya.E.L'vovich, A.A.Mozgovoy, A.P.Preobrazhenskiy, O.N.Choporov // Tsifrovaya obrabotka signalov. 2016. No. 4. pp.43-47.
3. Preobrazhenskiy A.P. Osobennosti pomekhoustoychivogo kodirovaniya v kanalakh svyazi / A.P.Preobrazhenskiy // Vestnik Voronezhskogo instituta vysokikh tekhnologiy. 2016. No. 3 (18). pp.75-77.
4. Shannon C. E. A Mathematical Theory of Communication / C.E.Shannon // Bell System Technical Journal. 1948. Vol.27. pp.379-423, 623-656.
5. Voronov A.A. Obespechenie sistemy upravleniya riskami pri vozniknovenii ugroz informatsionnoy bezopasnosti / A.A.Voronov, I.Ya.L'vovich,

Yu.P.Preobrazhenskiy, V.A.Voronov // Informatsiya i bezopasnost'. 2006. Vol.9. No. 2. pp. 8-11.

6. Popov E.A. Risk-analiz informatsionno-telekommunikatsionnykh sistem pri additivnom kharaktere parametra nergulyarnosti / E.A.Popov, N.N.Korneeva, O.N.Choporov, A.V.Zaryaev // Informatsiya i bezopasnost'. 2013. Vol.16. No. 4. pp.482-485.
7. Ermilov E.V. Risk-analiz raspredelennykh sistem na osnove parametrov riskov ikh komponentov / E.V.Ermilov, E.A.Popov, M.M.Zhukov, O.N.Choporov // Informatsiya i bezopasnost'. 2013. Vol.16. No. 1. pp.123-126.
8. Kalashnikov A.O. Ataki na informatsionno-tekhnologicheskuyu infrastrukturu kriticheski vazhnykh ob"ektov: otsenka i regulirovanie riskov / A.O.Kalashnikov, E.V.Ermilov, O.N.Choporov, K.A.Razinkin, N.I.Barannikov // monografiya / pod red. chl.-korr. RAN D.A. Novikova. Voronezh, Izdatel'stvo: OOO "Izdatel'stvo "Nauchnaya kniga", 2013, 159 p.
9. L'vovich I.Ya. Osnovy informatiki / I.Ya.L'vovich, Yu.P.Preobrazhenskiy, V.V.Ermolova / uchebnoe posobie, Voronezh, Izdatel'stvo: Voronezhskiy institut vysokikh tekhnologiy, 2014, 339 p.
10. Fink L.M. Teoriya peredachi diskretnykh soobshcheniy / L.M.Fink // Izdatel'stvo "Sovetskoe radio", 1970, 728 s.
11. Kharkevich A.A. Bor'ba s pomekhami / A.A.Kharkevich // Izdatel'stvo "Nauka", glavnaya redaktsiya fiziko-matematicheskoy literatury. Moskva, 1965. 275 p.
12. Bleykhud R. Teoriya i praktika kodov kontroliruyushchikh oshibki / R.Bleykhud // Per. s angl.- M.: Mir, 1986. 576 p.