*Девиз - "**Помехоустойчивая передача**"*

МУЛЬТИКОДОВАЯ СИСТЕМА ЗАЩИТЫ ДАННЫХ

2011

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

Передача информации в настоящее время осуществляется преимущественно в цифровой форме. Подобная передача сообщений обладает рядом преимуществ по сравнению с аналоговой:

- повышение точности передачи и обработки сигналов, которое не зависит от схемных и технологических решений аппаратуры;

- интеграция каналов электросвязи, источников и получателей сообщений, позволяющая проектировать развитые сети связи за счёт унификации методов передачи, обработки и распределения информации посредством использования однотипных цифровых сигналов и множественного доступа к передающей среде;

- возможность обеспечения скрытности передачи путём кодовой шифрации сообщений; нечувствительность цифровых каналов к эффекту накопления искажений при ретрансляциях;

- развитие систем связи, обеспечивающих эффективное использование дорогостоящих коммуникационных ресурсов;

- гибкость организации цифровых средств передачи и обработки данных, допускающая использование микроЭВМ, микросхем с большой степенью интеграции, цифровой коммутации.

Реализация цифровых систем связи на интегральных логических микросхемах позволяет создать гибкие, универсальные, компактные и недорогие устройства, обладающие заданными показателями верности передачи сообщений.

Одной из важнейших задач при построении аппаратуры передачи и защиты от ошибок является обеспечение помехозащищённости данных, поэтому в данной научно-исследовательской работе разрабатывается метод мультиководой защиты данных, позволяющий на практике улучшить характеристики систем передачи данных.

1 ОБЗОР ЛИТЕРАТУРЫ И ПОСТАНОВКА ЗАДАЧИ ИССЛЕДОВАНИЯ

1.1 Структура системы передачи данных и назначение ее элементов

Системой передачи данных (СПД) называется совокупность технических средств, обеспечивающих передачу сообщений от объекта к адресату [1]. Рассмотрим обобщенную структуру СПД однонаправленного действия, состоящую из оконечного оборудования (ООД), выполняющего функции отправителя (ООД-ОС) и получателя (ООД-ПС) сообщений, устройств сопряжения (УС), устройств защиты от ошибок (УЗО), устройств преобразования сигналов (УПС), устройств управления (УУ) и канала связи (КС) (рисунок 1.1).

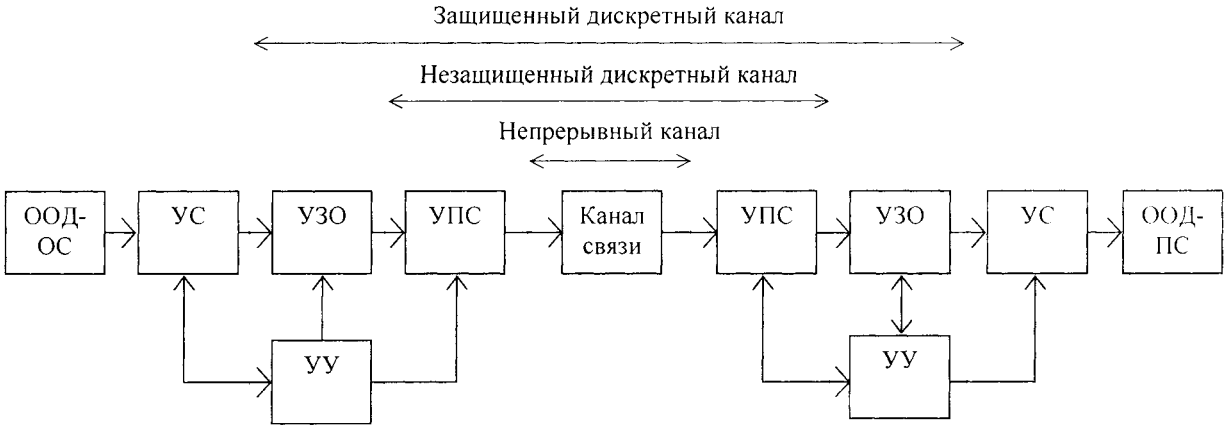


Рисунок 1.1 – Обобщённая структура СПД

В УЗО происходит кодирование-декодирование данных. УПС осуществляет преобразование сигналов данных в форму, удобную для передачи по каналу связи, а устройства сопряжения обеспечивают обмен информационными и управляющими сигналами между аппаратурой передачи данных (ПД) и ООД. Координация взаимодействия составных частей СПД обеспечивается специальными импульсами, вырабатываемыми

устройством управления. Совокупность непрерывного канала с включенными на его входе и выходе УПС называют незащищенным или дискретным каналом ПД, а объединение непрерывного канала с УЗО – защищенным от ошибок каналом ПД. Для двустороннего обмена информацией между абонентами используются две однонаправленные СПД, которые конструктивно могут быть выполнены в виде одной дуплексной СПД.

Пара УЗО передатчика и приемника существенно определяет степень защиты сообщений от ошибок в канале связи, причём кодер отображает последовательность, поступающую на его вход, в новую цифровую последовательность, а декодер производит обратное отображение. В совокупности эти отображения должны обеспечить устойчивость цифровой последовательности по отношению к возможным искажениям, что требует введения контролируемой избыточности при кодировании и её использование при декодировании [1, 2].

Пара УПС передатчика и приемника служит для согласования параметров сигнала с соответствующими параметрами КС с целью максимального противодействия помехам. Модулятор сопоставляет каждому символу или группе символов входной сигнал канала, демодулятор выполняет обратное преобразование [1, 2].

В КС действуют шумы и помехи, которые в дискретном канале проявляются в виде перехода одного значения символа в другое – ложное событие, состоящее в появлении ошибки, или неиспользуемое событие, которое называется стиранием. В зависимости от характера ошибок различают следующие дискретные каналы: симметричный (все ложные значения символов равновероятные), асимметричный (некоторые ложные значения символов обладают большей вероятностью), без памяти (искажение символов не зависит статистически от искажения другого выходного символа), с памятью (искажение символа выходной последовательности зависит статистически от искажения другого символа той же

последовательности), канал со стиранием (наряду с ошибками имеют место стирания символов) [2, 3].

1.2 Основные параметры системы передачи данных

Основными характеристиками, определяющими качество и эффективность передачи данных, являются скорость и верность передачи. Немаловажным показателем является сложность аппаратурной реализации, определяющая ее стоимость [1].

Скорость передачи информации V равна количеству информации, передаваемой по КС за единицу времени, бит/с:

$$V = \frac{\log_2(m_c)}{\tau_0} \qquad (1.1)$$

где m_c – количество позиций сигнала;

τ_0 – длительность единичного элемента сигнала.

Для двухпозиционных сигналов на основании (1.1): $V = \frac{1}{\tau_0}$

Величина $1/\tau_0$ определяет количество элементов, передаваемых по КС в секунду, и носит название скорости модуляции B (*Бод*). Таким образом, для двоичных систем скорости передачи информации и модуляции совпадают. Применение многопозиционных сигналов позволяет при одной и той же скорости модуляции повысить, по сравнению с двухпозиционными системами, скорость передачи.

Верность передачи данных количественно оценивается вероятностями ошибочного приема единичных элементов P_o и кодовой комбинации $P_{кк}$, которые определяются следующим образом [1]:

$$P_o = \lim_{n\to\infty} \frac{n_{îø}}{n},$$

$$P_{êê} = \lim_{N\to\infty} \frac{N_{îø}}{N},$$

где $n_{ош}$, $N_{ош}$ – количество ошибочно принятых единичных элементов и кодовых комбинаций соответственно;

n, N – количество переданных единичных элементов и кодовых комбинаций соответственно.

В связи с ограниченным числом n и N на практике вместо вероятностей P_o и $P_{кк}$ используют коэффициенты ошибок по элементам K_o и по кодовым комбинациям $K_{кк}$

$$K_0 = \frac{n_{îø}}{n}, \qquad (1.2)$$

$$K_{êê} = \frac{N_{îø}}{N} \qquad (1.3)$$

Для телефонных каналов коэффициент $К_0$ нормируется рекомендацией МККТТ V53. Его величина зависит от типа канала, скорости модуляции. Значения $К_о$ приведены в таблице 1.1.

Коэффициент ошибки по кодовым комбинациям $К_{кк}$ независимо от типа канала и скорости передачи должен быть не более 10^{-6}.

Таблица 1.1 – Значения $Р_о$ и $К_о$ для разных каналов и скоростей модуляции

Тип канала связи	Скорость модуляции В, Бод	Вероятность $Р_о$ (коэффициент $К_о$) ошибки
Коммутируемый канал	300 600 1200	$1\cdot10^{-4}$ $1\cdot10^{-3}$ $1\cdot10^{-3}$
Некоммутируемый (выделенный) канал	300, 600, 1200	$5\cdot10^{-5}$

Существуют следующие подходы к борьбе с помехами [2]:

– использование подземных каналов связи, которые меньше зависят от внешних условий и имеют стабильные параметры;

– использование обратного канала в дуплексном режиме и решающей или информационной обратной связи;

– использование избыточных помехоустойчивых кодов, способных корректировать ошибки на приемном конце.

Последние два подхода характеризуются применением помехоустойчивых кодов, позволяющих обнаруживать и исправлять ошибки, возникающие при преобразованиях или передаче информации.

1.3 Постановка задачи исследования.

На основании литературного обзора и анализа вопросов, касающихся обеспечения качества передачи, можно сделать следующие выводы:

– кодовый метод защиты данных является достаточно эффективным, позволяющим существенно снизить временные издержки при переспросах ошибочно принятых кодовых комбинаций;

– параметры каналов связи и уровень помех в каналах являются нестабильными и могут меняться случайным образом;

– во множестве случаев каналы связи являются асимметричными, когда вероятности переходов ($0 \rightarrow 1$) и ($1 \rightarrow 0$) не равны друг другу;

– перспективным является использование в адаптивной системе передачи данных нескольких помехоустойчивых кодов, различающихся избыточностью и ошибкообнаруживающей способностью, применение которых в тот или иной момент зависит от уровня помех, присутствующих в канале, и требуемой скорости передачи данных.

Таким образом, проектируемая мультикодовая система защиты данных от ошибок должна обладать элементами адаптации по отношению к ошибкообнаруживающей и корректирующей способности в зависимости от уровня помех в КС.

2 МУЛЬТИКОДОВЫЙ МЕТОД ЗАЩИТЫ ДАННЫХ ОТ ОШИБОК

Различают две группы кодов: неизбыточные и избыточные (ошибкообнаруживающие и корректирующие). Первые не позволяют обнаруживать и исправлять искаженные элементы в своих комбинациях, вторые – обеспечивают возможность обнаружения или исправления искаженных в результате действия помех и искажений элементов кодовых комбинаций.

В избыточных кодах кодовые комбинации могут содержать информационные и проверочные элементы. Обе группы кодов подразделяются на равномерные и неравномерные, т.е. коды с постоянным и непостоянным числом разрядов. Избыточные коды делятся на непрерывные (рекуррентные) и блочные (блоковые). В непрерывных кодах процесс кодирования и декодирования носит непрерывный характер, в блочных – каждому сообщению соответствует кодовая комбинация (блок) из конечного числа элементов. Блоки кодируются и декодируются отдельно друг от друга.

Разделимые блочные коды, в свою очередь, делятся на систематические и несистематические.

Систематическим разделимым блочным кодом называется такой код, в кодовых комбинациях которого первые m позиций (разрядов) заняты информационными элементами, а последние $r = n - m$ позиций – проверочными. К несистематическим разделимым блочным кодам относятся коды, у которых информационные элементы не занимают все k первых позиций.

Разновидностью систематических кодов являются циклические коды.

При выборе кодов для передачи информации руководствуются требованиями к верности передаваемой информации и скорости передачи, которые определяются на основании характеристик кодов. К основным характеристикам кодов относятся [2, 3]:

– число информационных элементов m;

– число проверочных элементов r (для корректирующих кодов);

– длина (разрядность) n кода – число элементов (символов), составляющих кодовую комбинацию, n = m + r;

– мощность кода N_p – число разрешенных кодовых комбинаций, используемых для передачи сообщений;

– основание (алфавит) q кода;

– полное число кодовых комбинаций N – число всех возможных комбинаций, равное q^n (для двоичных кодов – $N = 2^n$);

– избыточность кода R_n:

$$R_{\text{è}} = 1 - \frac{\log_q N_{\text{ð}}}{\log_q N}, \qquad (1.4)$$

или при $N_p = 2^m$ и $N_p = 2^n$

$$R_{\text{è}} = 1 - \frac{m}{n} = \frac{r}{n}; \qquad (1.5)$$

– относительная скорость кода R, характеризующая степень использования в избыточном коде информационных возможностей его мощности,

$$R = \frac{\log_q N_{\text{ð}}}{\log_q N} \text{ или } R = \frac{m}{n} = 1 - R_{\text{è}};$$

– вес кодовой комбинации (кода) ω (для двоичного кода определяется количеством единиц в кодовой комбинации);

– минимальное кодовое расстояние кода

$$d = \min_{ij} d_{ij}, \qquad (1.6)$$

определяемое как минимальное расстояние из всех полученных кодовых расстояний между парами кодовых комбинаций данного кода. Кодовое расстояние d_{ij} между i-й и j-й комбинациями этого кода определяется в соответствии с правилом

$$d_{ij} = \sum_{l=1}^{n} \left| a_{li} - a_{lj} \right|, \qquad (1.7)$$

где a_{li}, a_{lj} – элементы, стоящие на l-м месте в i-й и j-й комбинациях, то есть d_{ij} определяется числом одноименных разрядов с различными значениями;

– вероятность необнаруживаемой ошибки $P_{но}$ – вероятность такого события, при котором принятая кодовая комбинация отличается от переданной, а свойства данного кода не позволяют определить факт наличия ошибки;

– вероятность обнаруженной ошибки $P_{оо}$ – вероятность, при которой принятая кодовая комбинация отличается от переданной и благодаря свойствам данного кода устанавливается факт наличия ошибки в кодовой комбинации;

– вероятность исправляемой ошибки $P_{ио}$ – вероятность такого события, при котором кодовая комбинация отличается от переданной, и благодаря свойствам данного кода исправляется ошибка в кодовой комбинации;

– вероятность возникновения ошибки $P_{ош}$ – вероятность такого события, при котором принятая кодовая комбинация отличается от переданной ($P_{ош} = P_{но} + P_{оо}$);

– кратность ошибки v определяется кратностью обнаруживаемых $v_о$ и исправляемых $v_и$ ошибок;

– эффективность кода

$$r_{э} = \frac{N_{р}}{N} \frac{P_{ош}}{P_{ош} - \sum_{i=1}^{v} P_i},$$

где P_i – вероятность обнаруживаемой или исправляемой ошибки в зависимости от свойств данного кода.

Степень защиты информации от ошибок определенным методом кодирования зависит, главным образом, от минимального кодового расстояния d данного кода.

Различают три вида кодового расстояния: Хемминга, Ли и матричное. Наиболее широкое распространение в теории кодирования нашло кодовое

расстояние Хемминга, так как оно неразрывно связано с понятием веса кодовой комбинации [2]. Кодовое расстояние Хемминга d между двумя комбинациями одной длины n определяется как число из одноименных разрядов (позиций), содержащих неодинаковые элементы. Для двоичных кодов, поскольку в двоичной арифметике суммирование одинаковых элементов дает 0, а неодинаковых – 1, расстояние Хемминга между двумя кодовыми комбинациями можно определить их поразрядным суммированием по $\mathrm{mod}\,2$ и последующим подсчетом числа ненулевых элементов, то есть определением веса ω такой суммы.

Общее число комбинаций длины n равно 2^n, а число комбинаций, отстоящих от данной на расстояние d, равно числу сочетаний из n по d:

$$C_n^d = \frac{n!}{d!(n-d)!}$$

Чтобы определить комбинацию, отстоящую от данной на расстояние d, можно прибавить к данной комбинации любую комбинацию веса d (с d единицами и $(n-d)$ нулями). Сложение – поразрядное по $\mathrm{mod}\,2$.

Для обнаружения всех ошибок кратности v_o кодовое расстояние должно быть

$$d \geq v_0 + 1, \tag{1.8}$$

а для исправления ошибок кратности $v_и$ –

$$d \geq v_u + 1 \tag{1.9}$$

Для исправления и обнаружения ошибок кодовое расстояние

$$d \geq v_u + v_0 + 1 \tag{1.10}$$

Примерами ошибкообнаруживающих и корректирующих кодов, которые получили широкое распространение в ПД, могут служить код с одной проверкой на чётность, код с простым повторением, код Хэмминга, код с постоянным весом и плоскостной код.

Код с одной проверкой на чётность имеет d = 2 и позволяет обнаруживать все ошибки нечётной кратности. Получил очень широкое

распространение в системах связи из-за простоты своей реализации и малой избыточности.

Код с простым повторением имеет d = 2 и позволяет обнаруживать все ошибки, за исключением ошибок в элементах, стоящих на одной и той же позиции в первой и второй частях комбинации.

Код Хэмминга имеет d = 4 и позволяет исправлять все однократные ошибки и обнаруживать все двукратные ошибки.

Коды с постоянным весом (равновесный код) имеют преимущество при использовании в каналах, которые в значительной степени асимметричны (что во множестве случаев и встречается на практике). В асимметричном канале данные коды обнаруживают все ошибки нечётной кратности. Из чётных ошибок не выявляются только те, при которых происходит симметричное преобразование 0 в 1 в одном разряде и 1 в 0 в другом. Код с постоянным весом получил широкое распространение в СПД, но он не позволяет производить коррекцию ошибок. Для того, чтобы исправлять ошибки предлагается использовать плоскостной код с d = 4, что позволяет исправлять все однократные ошибки и обнаруживать все двукратные ошибки. Дополнительным его достоинством является то, что он так же как и код с постоянным весом является комбинаторным, а значит и преобразование равновесного кода в плоскостной будет происходить наиболее простым образом с минимальными аппаратурными затратами.

2.1 Выбор совокупности кодов для передачи данных

Согласно заданию на исследование адаптивная система защиты от ошибок должна обеспечить передачу четырехразрядных десятичных чисел, представленных с помощью двоично-десятичного кода (ДДК). Учитывая, что число десятичных цифр равно 10, то количество $n_{ддк}$ разрядов ДДК цифры

$$n_{ääê} = \lceil \log_2 10 \rceil = 4$$

В качестве кода, предназначенного для передачи числовых данных в условиях низкого уровня помех, выбирается код с одной проверкой на чётность (КПЧ), который позволяет обнаруживать все ошибки нечётной кратности. Формирование КПЧ основано на получении дополнительного бита y_n паритета путем сложения значений всех разрядов $x_3x_2x_1x_0$ двоично-десятичного кода цифры:

$$y_n = x_3 \oplus x_2 \oplus x_1 \oplus x_0 \qquad (1.11)$$

и прибавлении его к исходному коду. Комбинации КПЧ (согласно 1.11) и соответствующие им комбинации ДДК цифры приведены в таблице 1.2.

Очевидно, что разрядность $n_{кпч}$ кода с битом четности

$$n_{êï\div} = n_{äää} + 1 = 4 + 1 = 5$$

Сложение по модулю 2 всех пятиразрядных кодовых комбинаций КПЧ друг с другом показывает, что минимальное кодовое расстояние для этого кода $d_{min} = 2$. Следовательно, в соответствии с (1.8) для используемого КПЧ

$$v_0 + 1 \le 2 \text{ или } v_0 \le 1,$$

то есть данный код может обнаруживать все однократные ошибки (с кратностью $v_o = 1$). Согласно (1.9) КПЧ не может исправлять обнаруженные однократные ошибки, поскольку $v_u < 1$.

Так как количество всех двоичных пятиразрядных комбинаций

$$N = 2^5 = 32$$

а разрешенных для КПЧ с четырьмя информационными разрядами

$$N_p = 2^4 = 16,$$

то ошибкообнаруживающая способность $Q_{кпч}$ рассматриваемого кода

$$Q_{êï\div} = 1 - \frac{N_p}{N} = 1 - \frac{16}{32} = 1 - 0,5 = 0,5$$

Это означает КПЧ может обнаруживать *50%* всех ошибок, возникаемых при передаче его комбинаций по КС. Избыточность такого кода по формуле (1.4)

$$R_{\hat{e}\acute{a}\ddot{i}} = 1 - \frac{\log_2 16}{\log_2 32} = 1 - \frac{4}{5} = 1 - 0,8 = 0,2,$$

а его относительная скорость (1.5)

$$S_{\hat{e}\ddot{i}\div} = 1 - R_{\hat{e}\ddot{i}\div} = 1 - 0,2 = 0,8.$$

Таблица 1.2 – Комбинации КПЧ и соответствующие им ДДК

Десятичная цифра	Двоично-десятичный код $x_3 x_2 x_1 x_0$	Бит y_n четности	Код с битом четности $y_3 y_2 y_1 y_0 y_n$
0	0000	0	00000
1	0001	1	00011
2	0010	1	00101
3	0011	0	00110
4	0100	1	01001
5	0101	0	01010
6	0110	0	01100
7	0111	1	01111
8	1000	1	10001
9	1001	0	10010

Доля обнаруживаемых ошибок для КПЧ невелика, поэтому для дальнейшего повышения качества передачи предлагается использовать равновесный код (РК), который можно применять для канала в условиях среднего уровня помех [3]. Равновесный код – это код с постоянным количеством единиц в каждой кодовой комбинации. Увеличение или уменьшение количества единиц в кодовой комбинации говорит о наличии ошибки. Число кодовых комбинаций в двоичных кодах с постоянным весом длиной в *n* символов

$$N_{\text{д}} = C_n^k = \frac{n!}{k! \cdot (n-k)!}, \qquad (1.12)$$

где k – число единиц в кодовой комбинации.

Чтобы обеспечить $N_p = 10$, необходимо взять число разрядов РК $n_{рк} = 5$, а число двоичных единиц $k = 2$. Действительно, по (1.12)

$$N_{\text{д}} = \frac{5!}{2! \cdot 3!} = 10.$$

Кодовые комбинации РК "2 из 5" представлены в таблице 1.3.

Таблица 1.3 – Равновесные комбинации и их соответствие комбинациям ДДК

Десятичная цифра	Двоично-десятичный код $x_3 x_2 x_1 x_0$	Комбинации равновесного кода "2 из 5" $y_4 y_3 y_2 y_1 y_0$
0	0000	00011
1	0001	00101
2	0010	01001
3	0011	00110
4	0100	01010
5	0101	01100
6	0110	10001
7	0111	10010
8	1000	10100
9	1001	11000

Сложение по модулю 2 всех пятиразрядных равновесных комбинаций друг с другом показывает, что минимальное кодовое расстояние для кода РК, как и для КПЧ, равно $d_{кр} = 2$.

Следовательно, в соответствии с (1.8) для РК

$$\nu_0 + 1 \le 2 \text{ или } \nu_0 \le 1,$$

то есть данный код может обнаруживать все однократные ошибки (с кратностью $v_o = 1$). Согласно (1.9) РК также, как и КПЧ, не может исправлять обнаруженные однократные ошибки, поскольку $v_u < 1$. Но ошибкообнаруживающая способность $Q_{рк}$ этого кода выше, поскольку число разрешенных равновесных кодовых комбинаций у него меньше:

$$Q_{\hat{e}\ddot{i}\div} = 1 - \frac{N_p}{N} = 1 - \frac{10}{32} = 1 - 0,66 = 0,34,$$

то есть приблизительно 69% ошибок РК позволяет обнаруживать. Избыточность такого кода по формуле (1.4)

$$R_{\eth\hat{e}} = 1 - \frac{\log_2 10}{\log_2 32} = 1 - \frac{3,3}{5} = 1 - 0,66 = 0,34,$$

а его относительная скорость (1.5)

$$S_{\hat{e}\ddot{i}\div} = 1 - R_{\hat{e}\ddot{i}\div} = 1 - 0,34 = 0,66$$

При большом числе ошибок частота переспросов возрастает и, следовательно, скорость передачи информации падает, а значит уменьшается производительность мультикодовой системы защиты от ошибок. С тем, чтобы не допустить существенного снижения скорости передачи для случая высокого уровня помех предлагается применить корректирующий комбинаторный плоскостной код (КПК).

КПК использует возможность нахождения любой точки плоскости системой комбинаторных координат. В предлагаемом коде число контрольных символов r равно числу координат, а общее число информационных символов m – числу комбинаций из r по 2, то есть

$$m = C_r^2 = \frac{1}{2} r\,(r - 1).$$

В местах пересечения координатных шин будем располагать информационные, а у изгибов – проверочные символы, используя при этом принцип проверки на четность. Общее число символов $n_{кпк}$, составляющих кодовую группу, равно:

$$n_{\hat{e}\ddot{i}\ \hat{e}} = m + r = C_r^2 + r = \frac{1}{2} r\,(r+1).$$

Зная число информационных символов, всегда можно определить число проверочных символов. Решая квадратное уравнение $r^2 - r - 2m = 0$, получаем:

$$n_{\hat{e}\ddot{i}\ \hat{e}} = \left\lceil \frac{1}{2} + \sqrt{\frac{1}{4} + 2m} \right\rceil.$$

Зависимость общего числа символов в кодовой группе от числа информационных символов у плоскостных кодов примет вид:

$$n_{\hat{e}\ddot{i}\ \hat{e}} = \left\lceil \frac{1}{2} + m + \sqrt{\frac{1}{4} + 2m} \right\rceil. \qquad (1.13)$$

В целях максимально возможного повышения помехоустойчивости передачи в качестве информационных разрядов для КПК возьмем разряды РК. Таким образом, при $n = n_{кр} = 5$ из (1.13) получаем

$$n_{\hat{e}\ddot{i}\ \hat{e}} = \left\lceil \frac{1}{2} + 5 + \sqrt{\frac{1}{4} + 10} \right\rceil = \lceil 2{,}5 + \sqrt{10{,}25} \rceil = 9,$$

а число проверочных разрядов $r = n_{кпк} - n_{кр} = 4$.

Задача выявления позиции, на которой находится искаженный двоичный символ, решается для КПК согласно рисунку 1.4 [4].

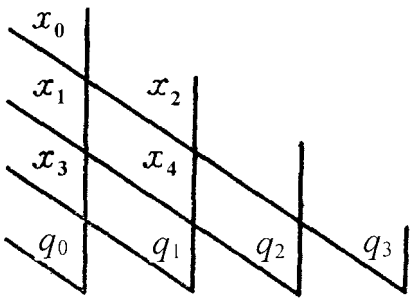


Рисунок 1.4 – Расположение информационных и проверочных разрядов в координатной решетке

Проверочные символы располагаются вдоль одной из трёх сторон матрицы на рисунке 1.4. Значения проверочных двоичных разрядов

определяются из проверок информационных символов, расположенных вдоль соответствующих координатных линий, на четность:

$$\begin{cases} q_0 = y_0 \oplus y_1 \oplus y_3 \\ q_1 = y_2 \oplus y_3 \oplus y_4 \\ q_2 = y_1 \oplus y_4 \\ q_3 = y_0 \oplus y_2 \end{cases}. \qquad (1.14)$$

Произведя последовательное считывание значений разрядов из матрицы, получим последовательность информационных и проверочных символов в передаваемой кодовой комбинации: $y_4 y_3 y_2 y_1 y_0 q_3 q_2 q_1 q_0$.

Если принятая кодовая комбинация не содержит ошибок, то результаты проверок на четность равны нулю:

$$\begin{cases} q_0 \oplus y_0 \oplus y_1 \oplus y_3 = 0 \\ q_1 \oplus y_2 \oplus y_3 \oplus y_4 = 0 \\ q_2 \oplus y_1 \oplus y_4 = 0 \\ q_3 \oplus y_0 \oplus y_2 = 0 \end{cases}.$$

Отображение двоичных разрядов, охваченных каждой проверкой на четность, приведено в таблице 1.4, из которой видно какие проверки на четность позволяют обнаружить ошибочные кодовые элементы.

Например, если первая, вторая и четвертая проверки на четность имеют 0, а третья 1, то это значит, что ошибка находится в третьем проверочном символе q_2. Если же результаты первой и третьей проверок равны 0, а второй и четвертой 1, то, следовательно, ошибка находится в информационном символе y_1. Комбинации КПК и их соответствие комбинациям ДДК приведены в таблице 1.5.

Сложение по модулю 2 всех девятиразрядных плоскостных комбинаций друг с другом показывает, что минимальное кодовое расстояние для кода КПК равно $d_{кпк} = 4$.

Следовательно, в соответствии с (1.8) для используемого КПК

$$\nu_0 + 1 \le 4 \text{ или } \nu_0 \le 2,$$

Таблица 1.4 – Соответствие ошибочных разрядов значениям проверочных разрядов

Номер проверки	Информационные символы					Проверочные символы			
	y0	**y1**	**y2**	**y3**	**y4**	**q0**	**q1**	**q2**	**q3**
1	▪	▪		▪		▪			
2			▪	▪	▪		▪		
3		▪			▪			▪	
4	▪		▪						▪

то есть данный код может обнаруживать все однократные, двукратные и трехкратные ошибки. Согласно (1.9) КПК может исправлять обнаруженные однократные ошибки, поскольку $v_u \le 1{,}5$. Ошибкообнаруживающая способность данного кода намного больше вышеприведенных КПЧ и РК. Так как $N = 2^9 = 512$, то

$$Q_{\hat{e}\ddot{i}\div} = 1 - \frac{N_p}{N} = 1 - \frac{10}{512} = 1 - 0,0195 = 0,98$$

то есть приблизительно *98%* ошибок КПК позволяет обнаруживать.

Избыточность такого кода по формуле (1.1)

$$R_{\hat{e}\ddot{i}\,\hat{e}} = 1 - \frac{\log_2 10}{\log_2 512} = 1 - \frac{3,3}{9} = 1 - 0,37 = 0,63,$$

а его относительная скорость (1.5)

$$S_{\hat{e}\ddot{i}\div} = 1 - R_{\hat{e}\ddot{i}\div} = 1 - 0,63 = 0,37$$

Таблица 1.5 – Комбинации КПК и соответствующие им ДДК и РК

Десятичная цифра	Двоично-десятичный	Комбинации равновесного кода "2 из	Комбинации плоскостного код

	код	5" $y_4 y_3 y_2 y_1 y_0$	$y_4 y_3 y_2 y_1 y_0 q_3 q_2 q_1 q_0$
0	0000	00011	00011 1100
1	0001	00101	00101 0011
2	0010	00110	00110 1111
3	0011	01001	01001 1010
4	0100	01010	01010 0110
5	0101	01100	01100 1001
6	0110	10001	10001 1111
7	0111	10010	10010 0011
8	1000	10100	10100 1100
9	1001	11000	11000 0101

2.3 Анализ помехоустойчивости используемых кодов

Анализ помехоустойчивости используемых кодов – РК и КПЧ – следует проводить на основе такого критерия как вероятность необнаруживаемой ошибки, обоснование применения которого приведено в работе [5].

В качестве модели канала передачи воспользуемся несимметричным каналом без памяти, в котором вероятности правильной передачи для двоичных нуля и единицы отличаются друг от друга: $p_{11} \neq p_{00}$. Такая модель канала представляет наибольший интерес, поскольку она наиболее часто используется для моделирования процессов в реальных каналах связи.

Определение вероятности V_k необнаруживаемой ошибки при передаче информации с помощью равновесного кода осуществляется по следующей формуле [6]

$$V_k = \sum_{r=1}^{k} C_k^r \cdot C_{n-k}^r \cdot p_{01}^r \cdot p_{10}^r \cdot p_{00}^{n-k-r} \cdot p_{11}^{k-r} . \qquad (1.15)$$

где p_{01} – вероятность возникновения ошибки типа $0 \to 1$;

p_{10} – вероятность возникновения ошибки типа $1 \to 0$;

p_{00} – вероятность правильного перехода $0 \to 0$;

p_{11} – вероятность правильного перехода $1 \to 1$.

При этом должны соблюдаться следующие равенства:

$$p_{00} + p_{01} = 1,$$

$$p_{11} + p_{10} = 1,$$

обоснованием которых является то, что ошибка типа $0 \to 1$ и переход $0 \to 0$, а также ошибка типа $1 \to 0$ и переход $1 \to 1$, поотдельности есть полные группы событий.

Построим для равновесного кода графические зависимости $V_k = f\left(p_{11}, k\right)$ от изменения состояния КС, то есть p_{11} (или $p_{10} = 1 - p_{11}$), для различных значений числа $1 \le k \le 7$ двоичных единиц, длине равновесной комбинации n = 8 и $p_{00} = 0,999$ (рисунок 1.5).

Как показывает анализ графиков на рисунке 1.5 вероятность V_k необнаруживаемой ошибки существенно зависят как от числа двоичных единиц k равновесных комбинаций, так вероятности ошибки. Каждый из семейства графиков V_k $(2 \le k \le 7)$ имеет свой максимум, расположение которого по оси абсцисс зависит от асимметрии канала, то есть соотношения вероятностей p_{01} и p_{10}.

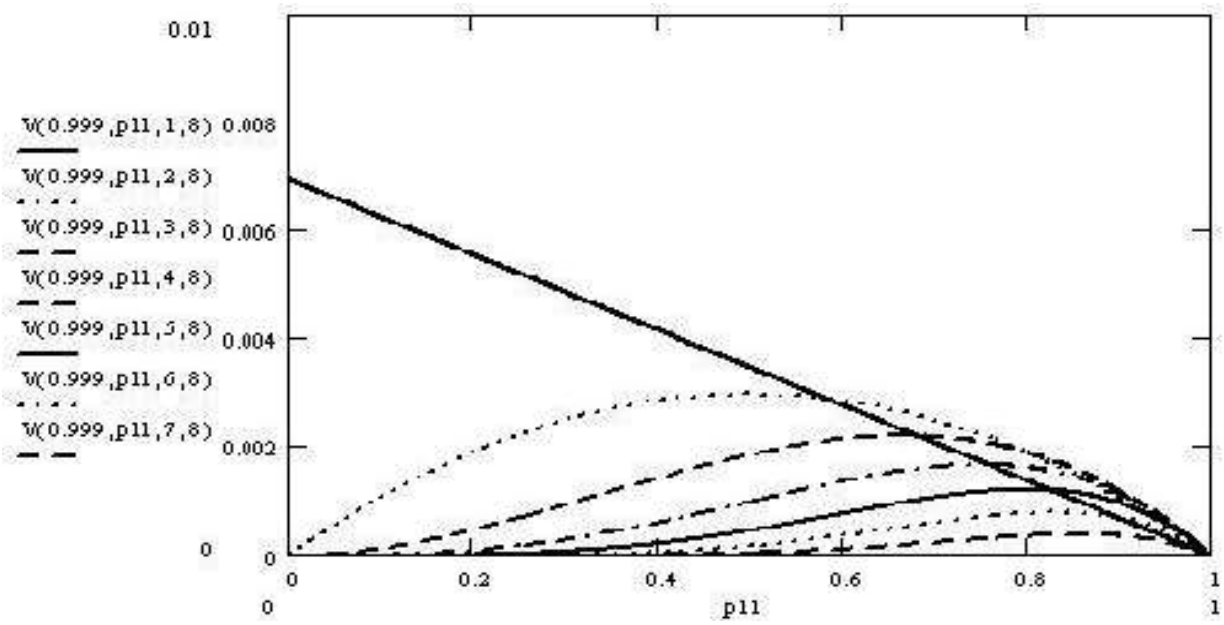


Рисунок 1.5 – Графики вероятности $V_k = f\left(p_{11}, k\right)$ необнаруживаемой ошибки для равновесного кода

Вычисление вероятности V_k необнаруживаемой ошибки для кода с проверкой на четность выполняется по следующей формуле [7]:

$$V_k = \sum_{\alpha=0}^{\left\lfloor \frac{m-1}{2} \right\rfloor} \sum_{\beta=0}^{\left\lfloor \frac{k-1}{2} \right\rfloor} C_m^{2\alpha+1} C_k^{2\beta+1} p_{00}^{\left[m-(2\alpha+1)\right]} p_{01}^{(2\alpha+1)} p_{11}^{\left[k-(2\beta+1)\right]} p_{10}^{(2\beta+1)} + \sum_{\alpha=0}^{\left\lfloor \frac{m}{2} \right\rfloor} \sum_{\beta=0}^{\left\lfloor \frac{k}{2} \right\rfloor} C_m^{2\alpha} C_k^{2\beta} p_{00}^{[m-2\alpha]} p_{01}^{2\alpha} p_{11}^{[k-2\beta]} p_{10}^{2\beta} - p_{00}^m p_{11}^k. \quad (1.16)$$

где m – число двоичных нулей в комбинациях КПЧ.

График функции (1.16) для кода с контролем по четности при различных значений k, длине комбинации КПЧ n = 8 и $p_{00} = 0{,}999$ приведен на рисунке 1.6.

Как показывает рисунок 1.6, вероятность V_k также существенно зависит от значений p_{10} и числа k двоичных единиц. При этом точки перегибов графиков определяются соотношением вероятностей p_{01} и p_{10}. Значение же самой вероятности V_k при соответствующих значениях p_{11} для КПЧ будет значительно выше, чем для РК.

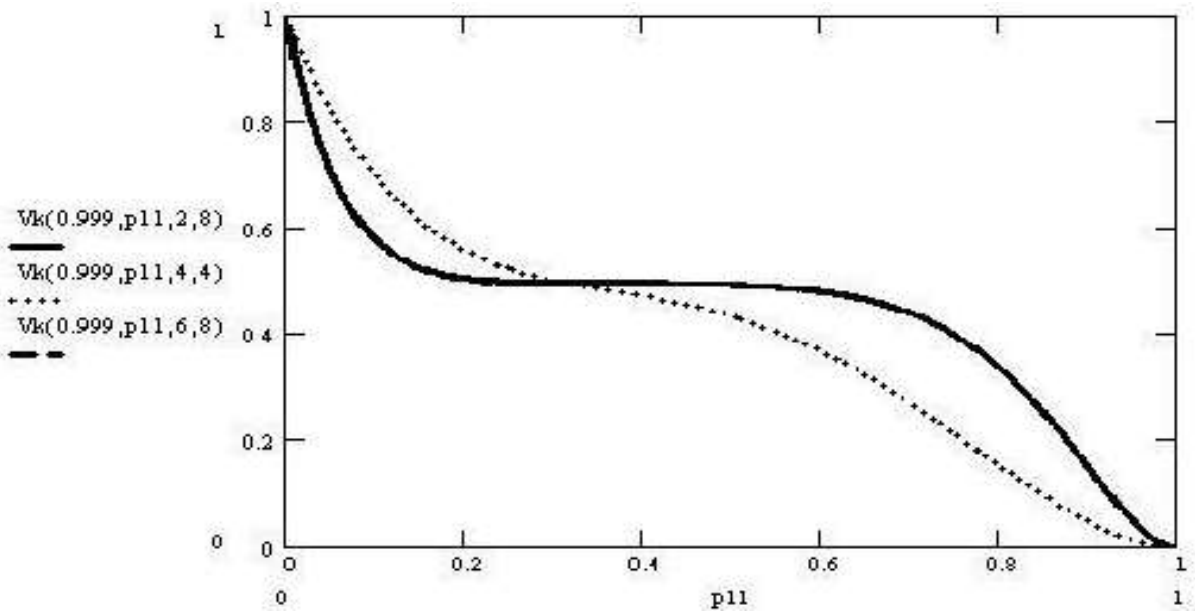


Рисунок 1.6 – График вероятности $V_k = f\left(p_{11}, k\right)$ необнаруживаемой для кода с контролем по четности

Таким образом, по результатам исследования эффективности применения совокупности ошибкообнаруживающих и корректирующих кодов можно сформулировать следующие выводы:

1) в целях повышения скорости передачи информации следует применять адаптивный кодовый способ передачи, основанный на использовании нескольких помехоустойчивых кодов;

2) выбор того или иного кода следует осуществлять на основе оценки состояния канала связи;

3) для передачи данных по малозашумленному каналу возможно применение кодов с невысокой ошибкообнаруживающей способностью, например кодов с битом паритета;

4) для передачи данных по среднезашумленному каналу следует применять код с более высокой ошибкообнаруживающей способностью, например равновесный код;

5) для передачи данных по сильнозашумленному каналу следует применять код с исправлением ошибок, снижая тем самым частоту обращений к передающему устройству.

3 ПРАКТИЧЕСКАЯ РЕАЛИЗАЦИЯ МУЛЬТИКОДОВОГО МЕТОДА ЗАЩИТЫ ДАННЫХ

3.1 Алгоритм работы системы передачи данных на основе мультикодовй защиты данных

В качестве элемента адаптации для проектируемой МКСЗ предлагается рассмотреть процедуру выбора нескольких кодов, различающихся между собой ошибкообнаруживающей и корректирующей способностями. Число ошибок в принимаемом приемником информационном пакете находится в прямо пропорциональной зависимости от уровня помех в КС. Следовательно, рассматриваемая МКСЗ должна осуществлять выбор кода в зависимости от числа искаженных двоичных разрядов, зафиксированных принимающей системой. Информацию о числе ошибок, присутствующих в данных, необходимо передавать в МКСЗ регулярно. Такое сообщение от приемника должно поступать после передачи всех разрядов числа. Таким образом, должна быть обеспечена информационная обратная связь с проектируемой системой. В целях экономии аппаратурных затрат и простоты алгоритма передачи информационный обмен необходимо проводить в полудуплексном режиме.

В качестве кодов, используемых в МКСЗ для передачи, предлагается применить следующие: ошибкообнаруживающий код с проверкой на четность (нечетность); ошибкообнаруживающий равновесный код; корректирующий плоскостной код.

Код с проверкой на четность предназначен для передачи информации в условиях невысокого уровня помех в КС, другими словами для "хорошего" канала. Равновесный код служит для передачи данных в условиях среднего уровня помех, или для "среднего" канала, а также для несимметричного КС.

Плоскостной код предназначен для передачи информации в условиях высокого уровня помех, то есть для "плохого" канала.

В результате алгоритм работы МКСЗ выглядит следующим образом (рисунок 1.7). Внешнее устройство (ВУ) при необходимости передачи числовых данных, выполняя шаг 1, загружает в проектируемую МКСЗ десятичный разряд числа, представленный в двоичном виде. Далее, действиями

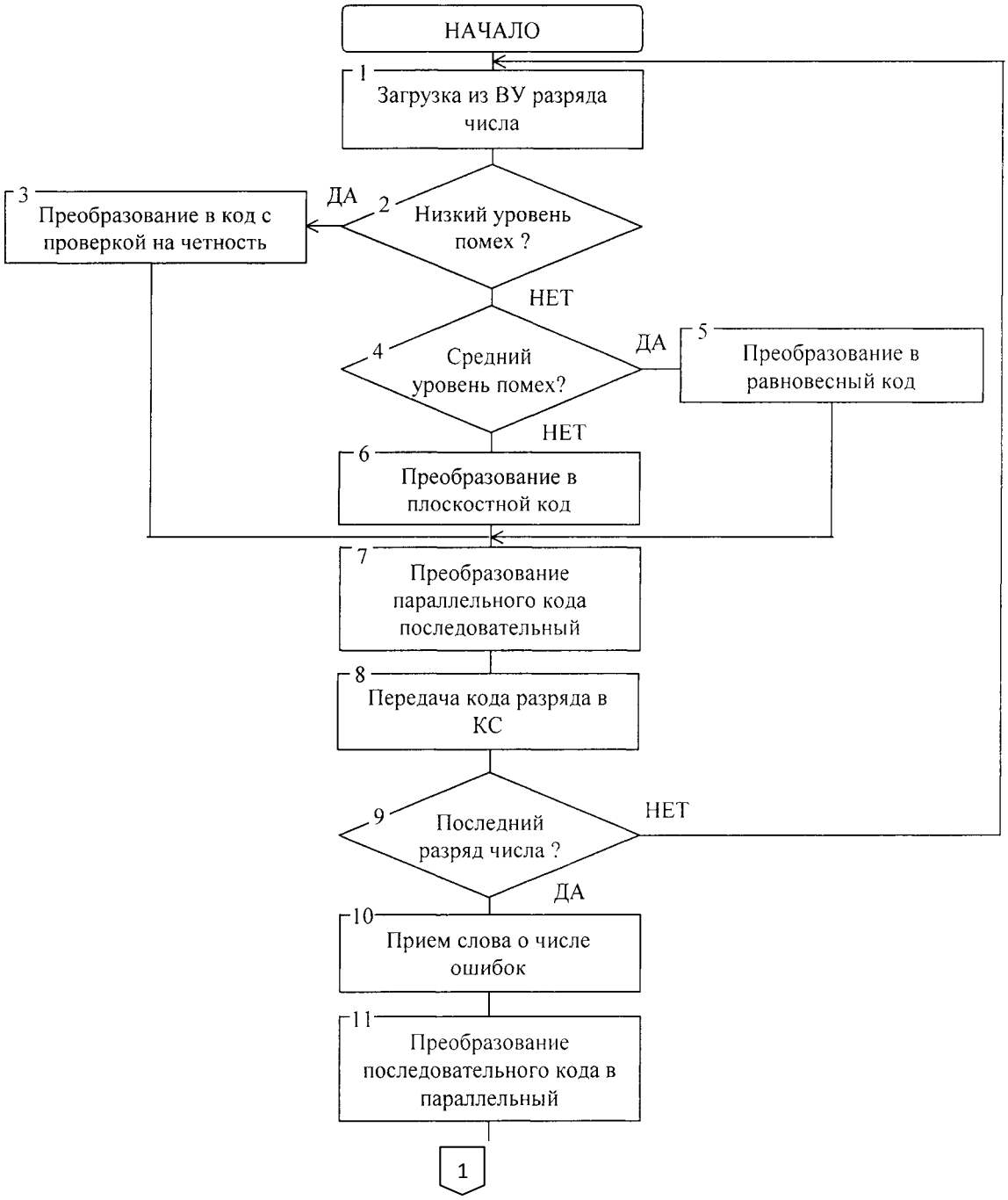
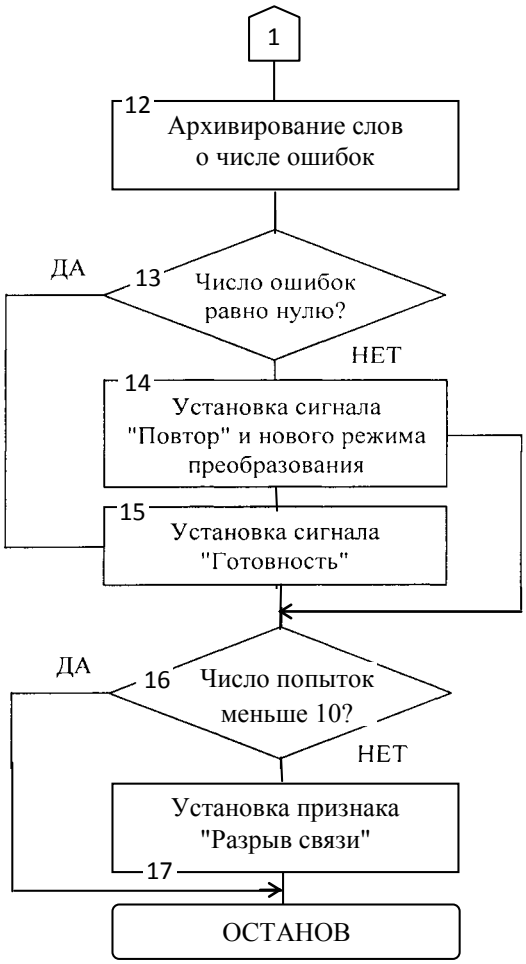


Рисунок 1.7 – Алгоритм работы МКСЗ



Продолжение рисунка 1.7

ЗАКЛЮЧЕНИЕ

Результатом проведенного исследования был разработан методо мультикодовой защиты данных от ошибок, предназначенная для повышения качества передачи числовой информации по последовательному каналу связи и повышения производительности систем связи. На основании данного метода разработан алгоритм работы системы передачи данных, которая выполняет следующие функции:

– выбор помехоустойчивого кода в зависимости от уровня помех в канале связи;

– помехоустойчивое кодирование числовых данных на основе кода с битом паритета, равновесного кода "2 из 5", комбинаторного плоскостного кода;

– обеспечение полудуплексного режима передачи числовых данных;

– обеспечение синхронного способа передачи числовых данных;

– архивирование данных о состоянии канала передачи и режимах кодопреобразования;

– контроль и сигнализация обрыва связи между передатчиком и приемником.

СПИСОК ЛИТЕРАТУРЫ

1. Чернега В.С., Василенко В.А., Бондарев В.Н. Расчет и проектирование технических средств обмена и передачи информации: Учеб. пособие для вузов. – М.: Высшая школа, 1990. – 224 с.
2. Жураковский Ю.П. Передача информации в ГАП: Учеб. пособие. – К.. Выща школа, 1991. – 216 с.
3. Березюк Н.Т., Андрущенко А.Г., Мощицкий С.С. Кодирование информации (двоичные коды). – Харьков: Выща школа, 1978. – 252 с.
4. Кувырков П.П., Темников Ф.Е. Комбинаторные системы. – М.: Энергия, 1975. – 152 с.
5. Борисенко А.А., Онанченко Е.Л. Оценка помехоустойчивости неразделимых кодов / Вісник Сумського університету 1994, № 2 – с 64-68.
6. Борисенко А.А., Бережная О.В., Кулик И.А. Оценка помехоустойчивости системы передачи данных на основе равновесных кодов / Вісник Сумського університету 1999, № 1(12) – с. 79-82.
7. Кулик И.А. Ошибкообнаруживающая способность кода с битом паритета / Тезисы докладов "Современные методы кодирования в электронных системах" 2002 – с. 38-39.