ВИНОКУРОВ
Александр Владимирович -
кандидат технических наук, доцент, заместитель начальника кафедры филиала Военной академии связи
Адрес: 350035, г. Краснодар, ул. Красина, 4
e-mail: VAV73@rambler.ru

ОВЧАРЕНКО
Михаил Вячеславович -
адъюнкт филиала Военной академии связи
Адрес: 350035, г. Краснодар, ул. Красина, 4

Метод помехоустойчивого кодирования информации с обнаружением позиции искаженного символа сообщения при декодировании

В настоящее время основным способом обеспечения достоверности сообщений при их передаче по каналам связи при воздействии непреднамеренных помех и целенаправленных деструктивных воздействий со стороны злоумышленника является помехоустойчивое кодирование. Эффективность такого кодирования достигается за счет введения искусственной избыточности в передаваемое сообщение, что приводит к расширению используемой полосы частот и уменьшению информационной скорости передачи.

Многообразие существующих помехоустойчивых кодов делится на два класса: блочные и непрерывные коды. В блочных кодах передаваемая информационная последовательность разбивается на отдельные блоки с добавлением к каждому блоку определенного числа проверочных символов. Кодовые комбинации кодируются и декодируются независимо друг от друга. В непрерывных кодах, называемых также цепными, рекуррентными, конволюционными или сверточными, передаваемая информационная последовательность не разделяется на блоки, а проверочные символы размещаются в определенном порядке между информационными. Процессы кодирования и декодирования также осуществляются в непрерывном режиме. Сверточные коды эффективно работают в канале с белым шумом, но плохо справляются с пакетами ошибок.

Хорошим средством защиты информации от случайных искажений являются циклические избыточные коды, достоинства которых [1]:

- высокая достоверность обнаружения искажений, доля обнаруживаемых искажений не зависит от длины массива данных и составляет $1-2^{-N}$, где N - разрядность контрольного кода;
- зависимость контрольного кода не только от всех бит анализируемой информационной последовательности, но и от их взаимного расположения;
- высокое быстродействие, связанное с получением контрольного кода в реальном масштабе времени;
- простота аппаратной и программной реализации.

Недостатки:

- простое условие пропуска искажений делает циклический код принципиально непригодным для защиты от умышленных искажений информации;
- равенство полученных значений контрольных сумм не дает гарантии неизменности информации.

По возможности коррекции ошибок все избыточные коды делятся на:

- обнаруживающие ошибки;
- исправляющие ошибки.

Общим свойством является то, что они не учитывают семантическую избыточность языка и обеспечивают повышение достоверности сообщения за счет добавления структурной избыточности на уровне бит, что приводит к нерациональному использованию ресурсов информационной системы.

Для повышения достоверности сообщений предлагается новый подход согласованного использования избыточности языка и вводимой структурной избыточности при помехоустойчивом кодировании.

В данной работе представлены результаты разработки нового метода кодирования и декодирования информации на уровне кодовых слов (байт), позволяющего локализовать место обнаружения ошибки заданной кратности в блоке сообщения и в последующем ее устранить, используя семантическую избыточность языка.

Основу данного метода составляют алгоритмы, базирующиеся на математическом аппарате специальных функций с обратными связями не только по аргументу, как, например, применяемых в сверточном кодировании [2], но и по функции. Впервые такие функции упоминались как «функции с памятью» и применялись для за-

дач прогнозирования событий за счет имеющегося сходства с моделями авторегрессии [3].

Рассмотрим алгоритм рекуррентного кодирования информации на примере упрощенной типовой функция кодирования, имеющей следующий вид:

$$Y_i = \begin{cases} (X_i + B)/A, & i = 1 \\ (X_i + Y_{i-1})/X_{i-1}, & i > 1 \end{cases},$$

где: X_i - символ сообщения, подлежащий преобразованию (кодированию);

Y_i - преобразованный (закодированный) i-й символ сообщения;

A, B - установочные параметры алгоритма кодирования, предназначенные для задания начальных параметров на этапе кодирования первого блока символа криптограммы.

Алгоритм кодирования следующий:

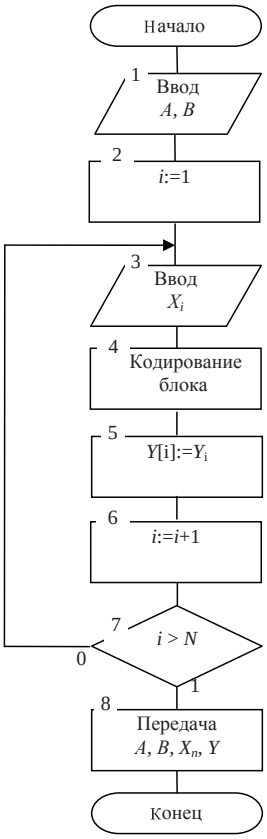

Рис. 1. *Схема алгоритма кодирования информационного блока*

1. Сообщение разбивается на информационные блоки длиной n в виде последовательности символов X_i.

2. Каждый информационный блок подлежит преобразованию в соответствии с функцией кодирования.

3. Кодированные блоки подлежат передаче по каналу связи, при этом в заголовке сообщения добавляются значения A, B, а в каждый информационный блок - X_n.

Процесс кодирования в виде алгоритма представлен на **рис. 1.**

На приемной стороне осуществляется декодирование сообщения в соответствии с формулами, имеющими вид:

$X_1^* = Y_1 A - B$;

$X_2^* = Y_2 X_1^* - Y_1$;

и т. д.,

где: X_i^* - символ, полученный в результате декодирования сообщения.

Если последний декодированный символ X_n^* сообщения совпадает с переданным X_n, то блок передан без искажений. При условии $X_n^* \neq X_n$ делается вывод о наличии ошибки и применяется процедура обнаружения места ошибки, заключающаяся в декодировании информационного блока в обратном направлении (реверсный режим):

$X_{n-1}^* = (X_n^* + Y_{n-1})/Y_n$;

$X_{n-2}^* = (X_{n-1}^* + Y_{n-2})/Y_{n-1}$

и т. д.

Процесс декодирования информационного блока в виде алгоритма представлен на **рис. 2**.

Практическая значимость рассмотренного метода кодирования подтверждена техническими решениями и программной реализацией алгоритмов кодирования и декодирования информации [4-6].

За основу технической реализации **(рис. 3)** берутся структуры непрерывного сверточного кодирования, но отличающиеся преобразованием на уровне кодовых слов, введением дополнительной обратной связи с выхода кодера и последующей поблочной передачей с проверочными символами.

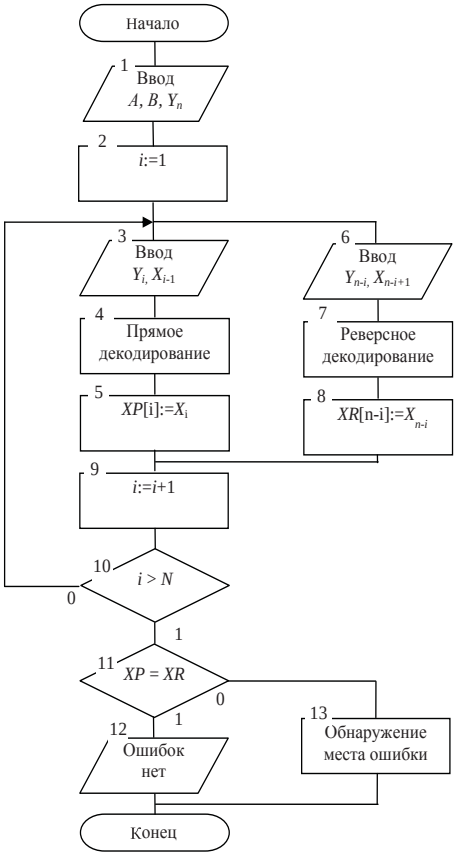

Рис. 2. *Схема алгоритма декодирования информационного блока*

Использование специальных функций позволило получить код, обладающий свойствами непрерывного сверточного кода (рекуррентная формула преобразования) и циклического избыточного кода (разбиение сообщения на блоки и добавление аналога контрольной суммы). За счет применения рекуррентных функций при декодировании обеспечивается обнаружение ошибок, включая выпадения и вставки символов с фиксацией мест искажения, при этом размножения ошибок не происходит.

Практический результат предложенного метода повышения достоверности информации достигается не за счет увеличения избыточности кода, а путем усложнения

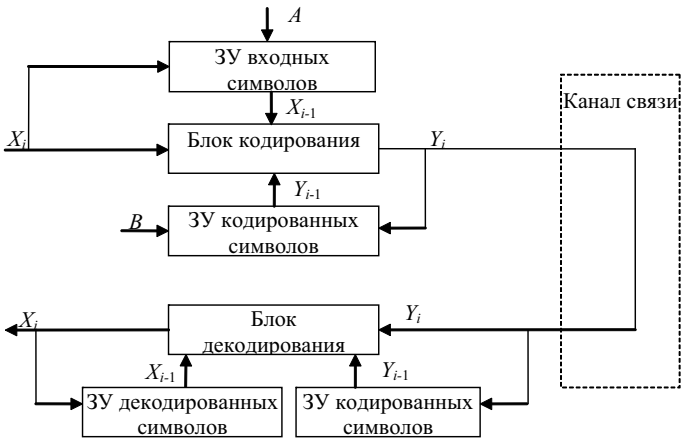

Рис 3. *Функциональная схема устройства рекуррентного кодирования и декодирования информации*

формулы кодирования, введения дополнительной обратной информационной связи между символами на выходе кодера и нового метода декодирования с начала и конца сообщения.

Эффект обнаружения места ошибки соответствует эффекту от применения кода с исправлением ошибки, но с меньшей введенной избыточностью кодера. Для оценки эффективности метода рекуррентного кодирования в сравнении с циклическим избыточным кодом предлагается использование коэффициента выигрыша, оцениваемого как отношение вероятности правильного приема сообщения без ошибок к вероятности правильного приема сообщения с одной ошибкой.

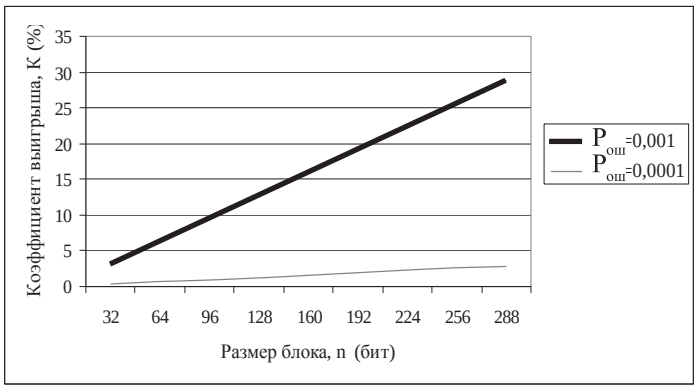

Рис. 4. *Графики сравнительного выигрыша К (в процентах) за счет обнаружения одной ошибки*

Представленные **(рис. 4)** графики показывают, что при $P_{ош}=10^{-4}$ выигрыш составляет 2,8 процента (n=288 бит), но при ухудшении качества канала связи ($P_{ош}=10^{-3}$) выигрыш увеличивается в 10 раз и составляет 28 процентов.

Предлагаемый метод помехоустойчивого кодирования обладает следующими классификационными признаками:

- по результату кодирования - обнаружение ошибки, с локализацией места;
- по принципу построения - несистематический нелинейный блочный с рекуррентной формулой построения.

Таким образом, особенности метода рекуррентного кодирования, заключающиеся в его направленности на результат обнаружения позиции ошибок, состоят в том, что новая рекуррентная формула преобразования информации и блочный принцип формирования кодовой последовательности позволяют его выделить в отдельный класс кодов, что можно охарактеризовать вкладом в науку.

Литература:

1. Sarwate, D.V., Computation of Cyclic Redundancy Checks via Table Look-Up, Communications of the ACM, 31(8), pp. 1008-1013.

2. Никитин Г.И. Сверточные коды: Учеб. пособие / СПбГУАП. СПб, 2001. - 80 с.

3. Аветисов А.Г., Сухарев М.Г., Кравец М.А. Оперативное прогнозирование газопотребления методом «функций с памятью» // Газовая промышленность. - 2007. - Сентябрь. - С. 60-62.

4. Винокуров А.В. Алгоритмы рекуррентного кодирования и декодирования цифровой информации / А.В. Винокуров, М.В. Овчаренко // Информационная безопасность - актуальная проблема современности. Совершенствование образовательных технологий подготовки специалистов в области информационной безопасности: Сборник трудов II-III Всероссийских научно-технических школ-семинаров. - Краснодар: ФВАС, 2011. - С. 98-101.

5. Винокуров А.В., Крупенин А.В., Овчаренко М.В. Рекуррентное кодирование цифровой информации. РОСПАТЕНТ. Свидетельство № 2012614612 от 24.05.2012 г.

6. Овчаренко М.В. Техническая реализация алгоритмов рекуррентного кодирования и декодирования цифровой информации // Информационная безопасность - актуальная проблема современности. Совершенствование образовательных технологий подготовки специалистов в области информационной безопасности: Сборник трудов IV-V Всероссийских научно-технических школ-семинаров. - Краснодар: ФВАС, 2012.