УДК 004.056.4:004.422.632.4

Д.М. Романенко, Р.И. Белькевич
Белорусский государственный технологический университет

ЗАЩИТА ИНФОРМАЦИИ МЕТОДАМИ ИЗБЫТОЧНОГО КОДИРОВАНИЯ НА ОСНОВЕ МНОГОМЕРНЫХ СХЕМ

В настоящее время широкое распространение получили и продолжают быстро развиваться области, связанные с передачей и соответственно защитой информации в беспроводных (спутниковых) сетях, системах хранения данных.

Защита информации согласно СТБ ГОСТ Р 50922-2000 – это деятельность, направленная на предотвращение утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию. При этом под информации от непреднамеренного воздействия подразумевается деятельность, направленная на предотвращение воздействия на защищаемую информацию ошибок ее пользователя, сбоя технических и программных средств информационных систем, природных явлений или иных нецеленаправленных на изменение информации мероприятий, приводящих к искажению, уничтожению, копированию, блокированию доступа к информации, а также к утрате, уничтожению или сбою функционирования носителя информации.

Поэтому передаваемые сигналы подвергаются специальной обработке с помощью методов избыточного кодирования для эффективного обнаружения изменений данных в условиях помех без потери информации. В последние годы самым эффективным направлением в теории кодирования является использование методов комбинирования известных кодов, что позволяет приблизиться к оптимальной пропускной способности канала. Для этого необходимы компонентные коды с широким спектром скоростей, корректирующих возможностей и эффективные алгоритмы декодирования: Так для нейтрализации пакетов ошибок высокой кратности интересными являются коды Рида-Соломона или Файра, для исправления одиночных ошибок можно использовать коды Хэмминга, простые циклические или итеративные коды. Последние уже сами по себе являются примером комбинирования простых сверток по модулю 2 на основе кронекеровского произведение кодов [1]. Классический итеративный код [1] по сути и является прямым произведением двух сверток по модулю два. Развитием идеи комбинирования известных кодов стал трехмерный линейный итеративный код (ТЛИК) – код, полученный прямым произведением линейного итеративного кода и кода с простой проверкой четности [2]. При использовании трех и более кодов можно получить многомерные схемы кодирования, т.е. многомерные коды. Многомерные схемы итеративных кодов с числом

проверок 5 (ТЛИК5), 7 (ТЛИК7) и 9 (ТЛИК9) описаны [3]. Необходимо отметить, что наилучшем для многомерных итеративных кодов является многопороговый метод декодирования, который включает несколько стадий (итераций) с различными пороговыми значениями. Стадии декодирования выполняются последовательно друг за другом, а следовательно, обнаружение и исправление ошибок в кодовой последовательности выполняется несколько раз при различных пороговых значениях.

В теории избыточного кодирования также хорошо известна и широко применима на практике последовательная каскадная схема кодирования/декодирования. Каскадные схемы практически всегда обеспечивают гораздо более высокий энергетический выигрыш кодирования, чем исходные базовые кодеки, из которых формируются сами каскадные коды. Пример использования каскадного кода, состоящего из двух составляющих кодов, показан на рисунке 1 [4].

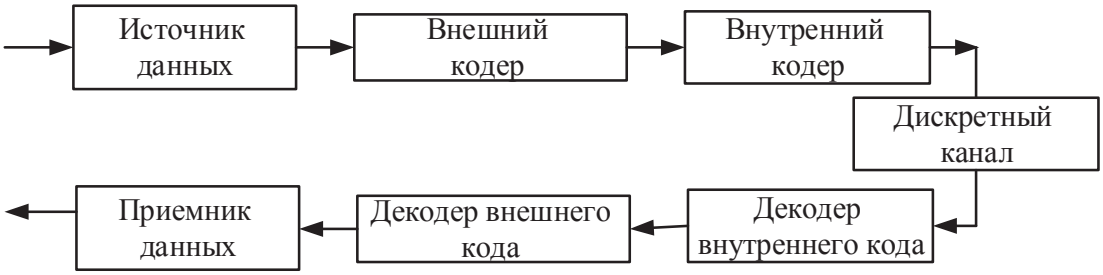

Рисунок 1 – Структурная схема последовательного каскадного кода с двумя компонентными кодами

На представленной схеме данные источника сначала кодируются внешним блочным (n_1, k_1) кодом. Затем закодированные символы внешнего кода кодируются кодером внутреннего (n_2, k_2) кода. Общая длина кодового слова каскадного кода оказывается равной $N = n_1 n_2$ двоичных символов, $K = k_1 k_2$, из них являются информационными. Результирующая кодовая скорость полученного каскадного кода будет равна $R = r_1 \cdot r_2$, где r_1, r_2 – кодовые скорости компонентных кодов.

Главным недостатком последовательной каскадной схемы являются высокие временные затраты как на стадии кодирования, так и декодирования. Для увеличения скорости декодирования и уменьшения вероятности ошибочного декодирования были предложены параллельные каскадные схемы [5], структурная схема которого представлена на рисунке 2. Параллельный каскадный кодер содержит первый кодер и второй кодер, на вход которых поступает информационная последовательность из источника данных, а выходы составных кодеров 1 и 2 соответственно соединены с первым входом и вторым входом блока объединения, выход которого формирует составное кодового слово.

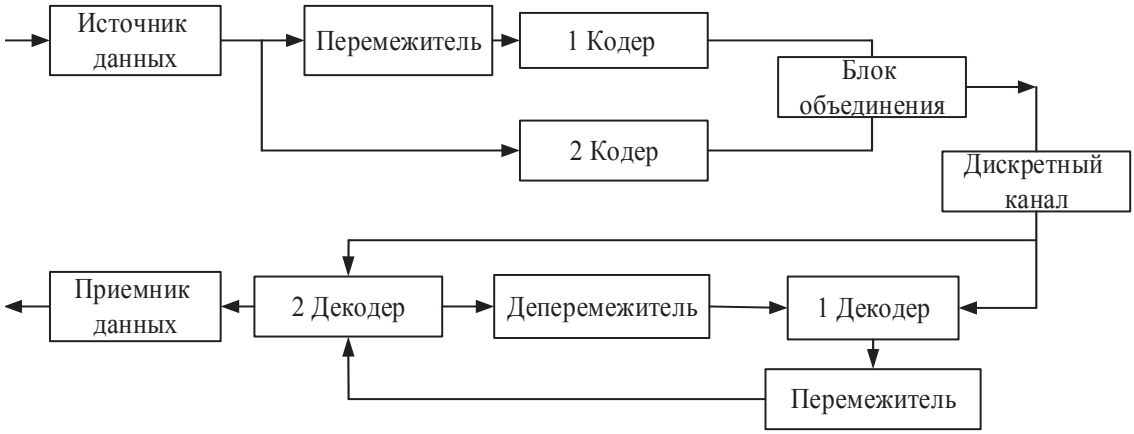

Рисунок 2 – Структурная схема параллельного каскадного кода с двумя компонентными кодами

При декодировании параллельного кода сначала выполняются несколько итераций декодирования составляющего кода 1, позволяющие примерно на порядок снизить вероятность ошибки в принятой из канала информационной последовательности, после чего в процесс декодирования включается оставшаяся часть кода 2. Самым распространенным случаем использования параллельных каскадных кодов являются турбо-коды, образующиеся при каскадировании двух или более составляющих систематических кодов.

В рамках данного исследования предлагается модифицировать каскадную схему кодирования, интегрировав ее в многомерную схему, представленную в виде многомерных итеративных кодов. Получим своего рода последовательно-параллельную схему кодирования/декодирования (рис. 3).

Поступающая на этап кодирования информационная последовательность (k) записывается в трехмерную структуру (куб или параллелограмм), при этом линейный адрес каждого информационного бита преобразуется в адрес с тремя координатами: номер плоскости, номер строки в плоскости, номер столбца в плоскости. На данном же этапе можно при необходимости осуществлять перемежение путем изменения последовательности записи бит. Далее из информационных бит формируется набор информационных последовательностей (k_1, k_2 … k_m), каждая из которых подается на блок кодирования, состоящий из m кодеров Используемые коды могут быть как одинаковые, так и отличаться. В блоке мультиплексирования осуществляется формирование итоговой кодовой последовательности (k+r, где $r = r_1 + r_2 + \ldots + r_m$) путем объединения информационных бит (k) и полученных корректирующих символов (r_1, r_2 … r_m).

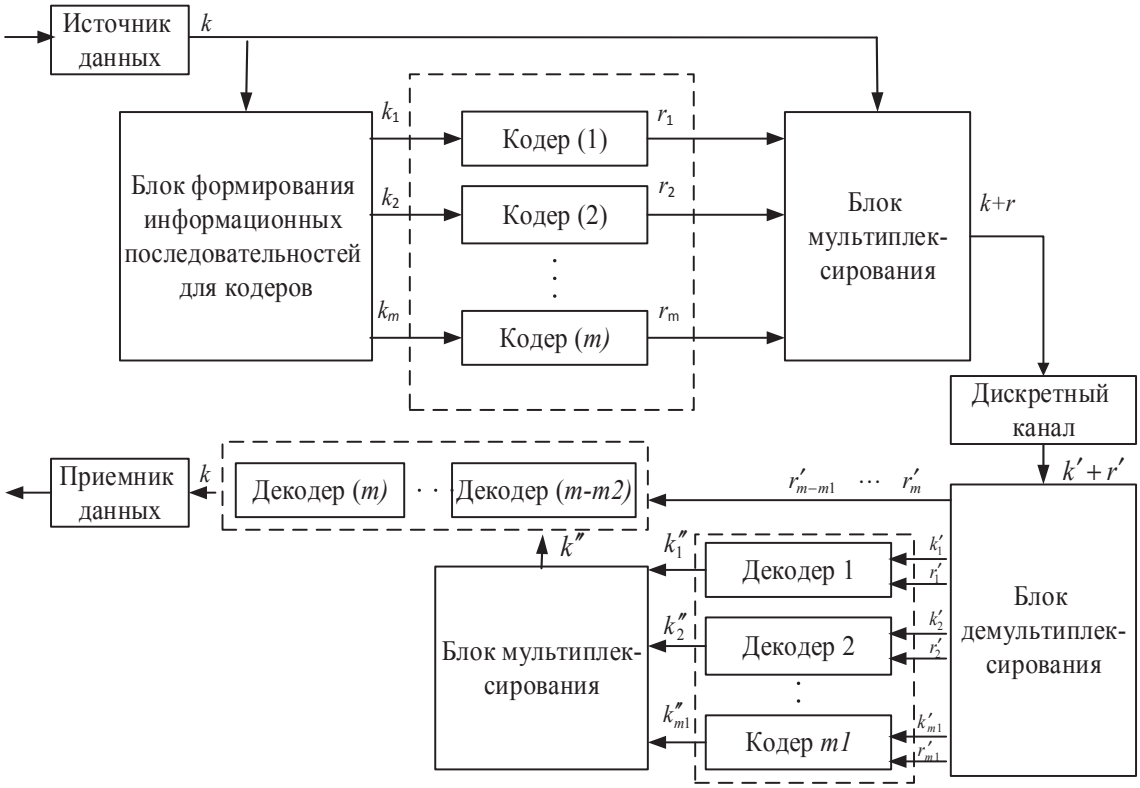

Рисунок 3 – Структурная схема последовательно-параллельной схемы кодирования с *m* компонентными кодами

После передачи данных на принимающей стороне осуществляется многостадийное декодирования принятой кодовой последовательности $k'+r'$, причем на первой стадии некоторое число декодеров (m_1) выполняют операции параллельно, а декодированная информационная последовательность (k'') отправляется на следующие стадии декодирования, количество которых равно m_2, выполняемые последовательно, как в классической каскадной схеме.

Таким образом можно предположить, что грамотный выбор компонентных кодов и последовательностей их применения позволит добиться высокой эффективности коррекции ошибок при сравнительно низких временных затратах, однако платой будет сложность технического исполнения всех элементов кодирования.

Список использованных источников

1. Скляр, Б. Цифровая связь. Теоретические основы и практическое применение / Скляр Б. – Изд. 2-е. – Москва: Изд. дом «Вильямс», 2003. – 1104 с.

2. Multithreshold majority decoding of LDPC-codes / P. Urbanovich, D. Romanenko, D. Shiman, M. Vitkova // Informatyka Automatyka Pomiary. – Poland, Lublinie. – R. 84, № 4a/2012. – 2012. – P. 22–24.

3. Виткова, М.Ф. Адаптивное многопороговое декодирование многомерных итеративных кодов / М.В. Виткова, Д.М. Романенко // Труды БГТУ. Сер. VI. Физ.-мат. науки и информ. – Минск. – Вып. XX. – 2012. – С. 134–138.

4. Золотарёв В. В., Овечкин Г. В. Помехоустойчивое кодирование. Методы и алгоритмы: Справочник / Под. ред. чл.-кор. РАН Ю. Б. Зубарева. – М.: Горячая линия-Телеком, 2004. – 126 с.

5. Золотарёв В.В. Параллельное кодирование в каналах СПД // Вопросы кибернетики. – 1986. – Вып. 120.

УДК 004.925.5

Д.М. Романенко, О.А. Новосельская, А.Н. Щербакова
Белорусский государственный технологический университет

ЗАЩИТА ЭЛЕМЕНТОВ ФИРМЕННОГО СТИЛЯ НА ОСНОВЕ АЛГОРИТМОВ ДИСКРЕТИЗАЦИИ ЦВЕТА

В настоящее время необходимость борьбы с фальсификацией стала еще более востребованной. Каковы бы сложны и эффективны не были средства защиты от фальсификации, со временем появляется способ их воспроизведения. Поэтому эффективность защиты напрямую зависит от новизны методов, что определяет постоянную потребность в новых средствах и технологиях защиты.

При разработке защиты для элементов фирменного стиля выполнен анализ возможных уровней защиты. Для элементов фирменного стиля как правило применяется полиграфическая защита, которая разделяется на три уровня. Уровень первый включает в себя защиты, которые в состоянии распознать неквалифицированный пользователь продукции. Второй уровень защиты предполагает использование простейшего детекторного оборудования, которое определяет наличие люминесцентных и метамерных красок и некоторых других защитных признаков. Экспертные организации могут диагностировать третий уровень защиты, проводя специальные исследования на более сложном оборудовании. Это определение наличия спецкрасок, некоторых скрытых изображений, кодированных магнитных меток и других подобных признаков. Это так называемые экспертные или арбитражные признаки, они известны только узкому кругу экспертов [1].

Есть еще один уровень – так называемая спящая защита. Это особый класс защитных признаков, вводимых в документ, целью которых