УДК 519.725

С.Н. Кириллов, Д.С. Семин

МОДИФИЦИРОВАННЫЙ ПОМЕХОЗАЩИЩЕННЫЙ КОДЕР НА ОСНОВЕ БИХ-ФИЛЬТРА

Предложен модифицированный алгоритм помехозащищенного кодирования на основе БИХ-фильтров, и проведены исследования его помехоустойчивости. Показана возможность увеличения защищенности исходного кода при незначительном уменьшении помехоустойчивости на 0.2…0.8 дБ по сравнению с исходным кодом при числе ключей 10^{38}.

Ключевые слова: *помехозащищенный кодер, помехоустойчивый БЧХ код, БИХ-фильтр, рекурсивное кодирующее устройство, защита информации.*

Введение. Многоканальные телекоммуникационные системы должны обеспечивать как надежность, так и скрытность передаваемой информации. Предложено множество алгоритмов, позволяющих увеличить помехоустойчивость и защищенность передаваемой информации при раздельном выполнении данных процедур. Недостатком подобных методов являются высокие вычислительные затраты. Известны алгоритмы, позволяющие уменьшить вычислительные затраты за счет объединения этих процессов, например алгоритм Мак-Элис [1, 2] и стохастическое кодирование [3]. Однако и данные алгоритмы вычислительно затратны, особенно при высоких требованиях к помехоустойчивости, а при стохастическом кодировании необходимы большие объемы памяти. В [4] был предложен алгоритм кодирования на основе рекурсивных и нерекурсивных кодирующих устройств, но не представлены исследования свойств получаемых кодов и не учитываются требования к защите информации. На основе анализа этих алгоритмов был предложен и исследован модифицированный помехоустойчивый кодер на основе фильтров с бесконечной импульсной характеристикой (БИХ), позволяющий объединить в себе операции кодирования и защиты информации.

Цель работы. Разработка и исследование модификации алгоритма кодирования на основе БИХ-фильтров, обеспечивающего защиту передаваемой информации.

Обоснование структуры кодера. На рисунке 1 представлена схема кодирующего устройства на основе БИХ-фильтра, предназначенного для выполнения операции свертки двух сигналов (импульсной характеристики фильтра и входного сигнала), в котором все операции выполняются согласно арифметике полей Галуа.

Фильтр делится на две части: рекурсивную и нерекурсивную. Нерекурсивная часть выполняет операцию перемножения полиномов поля Галуа, а рекурсивная – деления. Кодирующее устройство, представленное на рисунке 1, было предложено в [4].

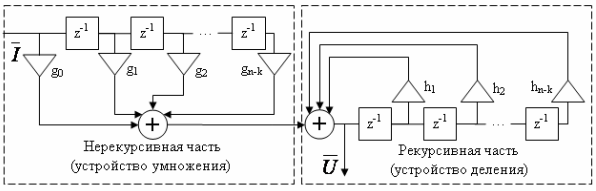

Рисунок 1 – Кодирующее устройство на основе БИХ-фильтра

Пусть задан бинарный вектор информации:

$$\overline{I} = (i_0, i_1, ..., i_k), \qquad (1)$$

где i_j принимает значения 0 или 1 ($j = \overline{0,k}$), k - число бит.

В арифметике полей Галуа информационный вектор можно записать в виде полинома:

$$I(x) = i_0 + i_1 x + ... + i_k x^k. \qquad (2)$$

В [4] показано, что кодирующее устройство изображенное на рисунке 1, выполняет операцию:

$$U(x) = I(x)G(x)/H(x), \qquad (3)$$

где полиномы $G(x) = g_0 + g_1 x + ,..., g_{n-k} x^{n-k}$ и $H(x) = 1 + h_1 x + h_2 x^2 + ,..., h_{n-k} x^{n-k}$ могут быть представлены в виде векторов коэффициентов фильтра нерекурсивной $\overline{G} = (g_0, g_1, ..., g_{n-k})$ и рекурсивной $\overline{H} = (h_1, h_2, ..., h_{n-k})$ частей. Коэффициенты фильтра также принимают значения

только 0 или 1, а сложение коэффициентов при одинаковых степенях x выполняется по модулю два.

Отметим тот факт, что эти операции являются линейными:

$$(I(x)+e(x))\,G(x)= I(x)G(x) + e(x)G(x). \quad (4)$$

У каждого полинома $G(x)$ ($G(x)\neq 0$) есть обратный

$$F(x)=1/G(x);\ F(x)G(x)=1. \quad (5)$$

Причем

$$(I(x)+e(x))/\,F(x)= I(x)/F(x) + e(x)/F(x)= = I(x)G(x) + e(x)G(x). \quad (6)$$

Деление производится по неклассической схеме (без получения остатка), описанной в [4]. Причем полином $F(x)$ содержит бесконечное число членов, обладающих свойством периодичности. Также в [4] показано, что операции произведения полиномов и деления полиномов являются сверткой.

Для определения циклического кода необходимо задать полином $G(x)$, делящий x^n+1 без остатка [5, 6]. Определение разрешенной комбинации кода производится вычислением произведения генераторного и информационного полиномов. Если принять, что коэффициенты рекурсивной части схемы, показанной на рисунке 1, нулевые, то получим циклический кодер.

Операции умножения и деления полиномов можно использовать не только для кодирования, но и для защиты информации.

Рассмотрим более детально возможный принцип увеличения скрытности передаваемой информации. Зададимся массивом случайных ненулевых полиномов:

$$\boldsymbol{A}^k{}_m=(A_1(x), A_2(x), \ldots, A_m(x)), \quad (7)$$

где k – максимальная степень полиномов, m – число полиномов в массиве.

Исходный поток информации разобьём на блоки длиной не менее k бит:

$$\boldsymbol{I}^k = (I_1(x), I_2(x), \ldots, I_m(x), I_{m+1}(x), \ldots). \quad (8)$$

Тогда защищенный поток информации можно представить как последовательность

$$\boldsymbol{V}^k=(I_1(x)/A_1(x), I_2(x)/A_2(x), \ldots, I_m(x)/A_m(x), I_{m+1}(x)/A_1(x), \ldots) = = (V_1(x), V_2(x), \ldots, V_m(x), V_{m+1}(x), \ldots). \quad (9)$$

После вычисления операции деления $I_p(x)/A_p(x)$ могут получаться полиномы степени, большей, чем k, но для дальнейшего восстановления достаточно взять только k первых членов (число бит в исходном информационном векторе). Дешифрация производится путем перемножения соответствующих полиномов:

$$\boldsymbol{I}^k =(V_1(x)A_1(x), V_2(x)A_2(x), \ldots, V_m(x)A_m(x), V_{m+1}(x)A_1(x), \ldots)= =(I_1(x), I_2(x), \ldots, I_m(x), I_{m+1}(x), \ldots). \quad (10)$$

Степень закрытия информации определяется числом полиномов в массиве $\boldsymbol{A}^k{}_m(x)$. Если изменять коэффициенты полиномов $A_j(x)$ по квазислучайному алгоритму, получим, что $m\to\infty$, следовательно, если неизвестна структура кодирующего устройства, вскрыть такую систему простым перебором невозможно.

Зададим функцию формирования полинома $A_j(x)$ в виде

$$A_j(x)=F[p,\ \overline{K}], \quad (11)$$

где p – временной сдвиг, $\overline{K}$ – вектор начальных данных, необходимых для вычисления функции $F[\cdot]$, обеспечивающей формирование квазислучайных коэффициентов рекурсивной части кодера.

Для вскрытия системы связи при известной структуре кодера и алгоритме формирования квазислучайных коэффициентов рекурсивной части фильтра необходимо определить вектор $\overline{K}$ и временной сдвиг p случайной последовательности.

Рассмотрим практическую реализацию предложенного модифицированного алгоритма (рисунок 2), позволяющего объединить шифрацию и помехоустойчивое кодирование.

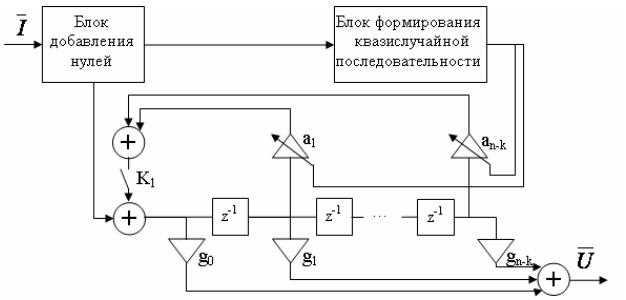

Рисунок 2 – Модернизированный помехозащищенный кодер циклических кодов

Шифрование осуществляется в рекурсивной части схемы, а кодирование производится блочным циклическим кодом, где n – общая длительность закодированного слова, а $\overline{g}=(g_0, g_1, \ldots, g_{n-k})$ – генераторный вектор в нерекурсивной части. В блоке добавления нулей информационный поток разбивается на пакеты длительностью k бит, разделенные нулевыми последовательностями (число нулей совпадает с числом проверочных символов n-k). Данная последовательность подается на вход кодера. На тактах от 1 до k осуществляются одновременное кодирование и закрытие информации (деление информационного полинома на полином $A_j(x)$ и умножение на полином $G(x)$). На $k+1$- м такте ключ K_1 размыкается и происходит кодирование про-

верочных символов до n-такта. Далее происходит смена коэффициентов ($a_1, a_2, \ldots, a_{n-k}$), генерируемых в блоке формирования квазислучайной последовательности. После этого значения бит, хранящиеся в памяти линии задержки, обнуляются и цикл повторяется.

Декодирования производится в два этапа. На первом этапе в принятом сообщении исправляются ошибки с помощью алгоритма Бэрлекэмпа-Мэсси [5], на втором происходит дешифрация путем пропускания сигнала через фильтр с конечной импульсной характеристикой с коэффициентами ($1, a_1, a_2, \ldots, a_{n-k}$) (умножение на соответствующий полином $A_j(x)$).

Результаты моделирования. Целью экспериментальных исследований является определение помехоустойчивости и скрытности в предложенном модифицированном кодере на основе БИХ-фильтров. Имитационное моделирование проводилось для канала с аддитивным белым гауссовским шумом (АБГШ) с использованием сигналов с относительной фазовой манипуляцией. Случайная информационная кодовая последовательность ***I*** формировалась алгоритмом В.В. Золотарева (Институт космических исследований РАН). Результаты исследований помехоустойчивости предложенного модифицированного кодирующего устройства на основе БИХ-фильтра с использованием БЧХ кода и исходных кодов БЧХ представлены на рисунке 3.

Как следует из анализа рисунка 3, увеличение скрытности передаваемой информации сопровождается некоторым уменьшением помехоустойчивости примерно 0.2-0.8 дБ (при вероятности ошибки 10^{-5}). Величина проигрыша зависит от длины информационной части k и от отношения сигнал-шум. Это объясняется тем, что при появлении необнаруживаемой ошибки на этапе дешифрации возникают дополнительные искажения информационной последовательности.

При вычислении коэффициентов рекурсивной части кодера использовалась квазислучайная последовательность, для формирования которой необходимо 128 бит. Таким образом, при известной структуре кодера для вскрытия последовательности методом перебора необходимо $2^{128}-1 = 3{,}7\cdot10^{38}$ комбинаций. Кроме того, требуется правильно определить начало случайной последовательности, в противном случае декодирование является невозможным. Для дополнительного увеличения скрытности передаваемой информации можно использовать несколько разных алгоритмов формирования квазислучайной последовательности A^k_m.

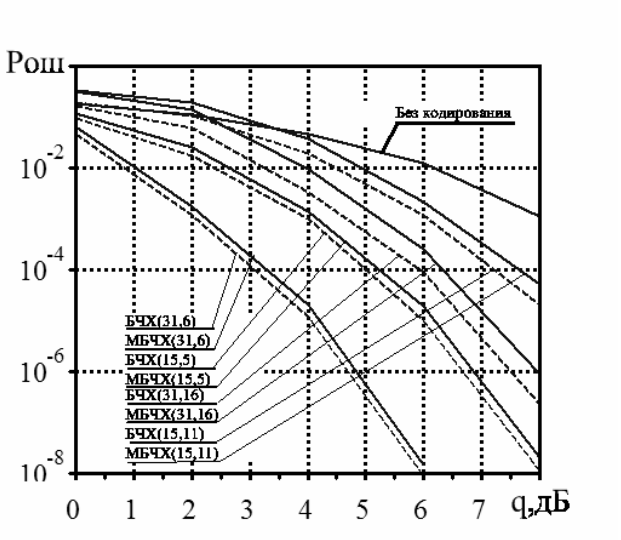

Рисунок 3 – Вероятности ошибки кода от отношения сигнал-шум в канале с АБГШ при ОФМн-сигналах

Недостатком подобной схемы помехозащищенного кодера является небольшое уменьшение помехоустойчивости по сравнению с базовым помехоустойчивым кодом.

Достоинством является простота схемной реализации кодирующего устройства на основе БИХ-фильтра по сравнению с другими аналогичными устройствами (Мак-Элис, стохастическое кодирование) при высокой скрытности информации и возможности адаптации под состояние канала связи.

Для увеличения помехоустойчивости можно в схему, предложенную на рисунке 2, ввести дополнительные нерекурсивные ветви (рисунок 4).

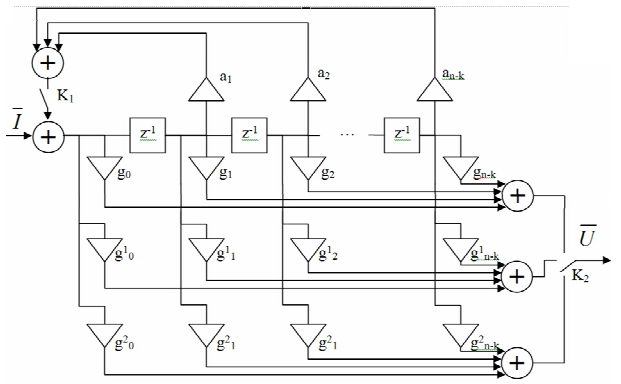

Рисунок 4 – Помехозащищенный кодер с возможностью кодирования различными типами кодов

При этом появляется возможность использования сверточных и более сложных составных кодов, в том числе турбокодов.

Заключение. Предложена модификация помехозащищенного кодирующего устройства на основе БИХ-фильтра, позволяющая увеличивать защищенность передаваемой информации. Про-

веденное имитационное моделирование показало, что при количестве ключей $3{,}7 \cdot 10^{38}$ в модифицированном алгоритме кодирования на основе БИХ-фильтра происходит небольшое уменьшение помехоустойчивости на 0.2–0.8 дБ по сравнению с базовым помехоустойчивым кодом.

Библиографический список

1. *Крысяев Д.Е., Фам С.Н.* Исследование помехоустойчивости системы кодирования Мак–Элис. Вестник РГРТА. – 2005. – № 16 – С. 112–116.

2. *Кириллов С.Н., Крысяев Д.Е., Дмитриев В.Т.* Методы повышения помехозащищенности алгоритма кодирования информации Мак–Элис. Труды научно–технического общества радиотехники, электроники и связи имени А.С. Попова Цифровая обработка сигналов и ее применение, 2007», Вып IX-I. – С. 396 – 398.

3. *Осмоловский С.А.* Стохастические коды, исправляющие ошибки с гарантированной точностью // Системы и средства связи, телевидения и радиовещания. М.: АО “ЭКОС”, 2001. – № 2, 3. [Электронный ресурс]. – Режим доступа:
http://www.stokos.ru/stat5.htm

4. *Селетков В.Л.* Варианты идентификации кодеров и декодеров систем помехоустойчивого кодирования // Радиоэлектроника. – 2007. – № 8. – С.11–22.

5. *Блейхут Р.* Теория и практика кодов контролирующих ошибки / пер. с английского Н.Н. Грушко, В.М. Блиновского.- М.:Мир, 1986. –576 с.

6. *Скляр Б.* Цифровая связь. Теоретические основы и практическое применение. Издание 2-е испр.: пер. с англ. – М: Издательский дом «Вильямс», 2003. – 1104 с.