УДК 681.32

Семеренко В.П.

ИНТЕГРИРОВАННАЯ ЗАЩИТА ИНФОРМАЦИИ: КРИПТОГРАФИЯ ПЛЮС ПОМЕХОУСТОЙЧИВОЕ КОДИРОВАНИЕ

В работе рассматривается способ совмещения во времени процессов поточного шифрования и помехоустойчивого кодирования на основе использовании единого математического аппарата – теории линейных последовательностных схем (ЛПС). Предлагаемая система шифрования состоит из трех уровней защиты: несистематического кодирования циклических кодов, линейного преобразования с помощью ЛПС и нелинейного преобразования с помощью бент-функций.

Ключевые слова: поточное шифрование, помехоустойчивое кодирование, циклические коды, линейная последовательностная схема, бент-функция

Введение. При передаче данных по современным каналам связи часто необходимо решать две задачи: защищать данные от атмосферных помех и возможных неисправностей аппаратуры, а также обеспечивать секретность передаваемой информации. Для решения первой задачи служит теория помехоустойчивого кодирования, а для решения второй задачи имеются различные методы шифрования данных. Математические основы помехоустойчивого кодирования и криптографии заложены в работах К. Шеннона [1]. Известный американский ученый впервые доказал, что, с одной стороны, теоретически можно достичь передачи информации почти без ошибок, и, с другой стороны, возможен совершенный шифр для обеспечения секретности передаваемых сообщений. Полученные К. Шенноном результаты стали отправной точкой для дальнейшего бурного развития теории кодирования и криптографии. Несмотря на много общих черт, эти отрасли науки имеют также и много различий (табл. 1), что является причиной их независимого развития и малого влияния друг на друга.

Сравнительная характеристика помехоустойчивого кодирования и криптографии Таблица 1

Параметры	**Помехоустойчивое кодирование**	**Криптография**
Источник искажений	Помехи в канале связи, неисправности аппаратуры	Действия злоумышленника
Соотношение длин входного и выходного сообщений	Выходное сообщение длиннее входного сообщения	Входное и выходное сообщения имеют одинаковую длину
Требования к сложности и времени восстановления входного сообщения	Минимальные во всех случаях	Минимальные для получателя и максимальные для злоумышленника
Виды математических преобразований	Линейные преобразования	Линейные и нелинейные преобразования

В последние десятилетия предпринимаются различные подходы к объединению криптографии и помехоустойчивого кодирования.

В 1979 году МакЭлис предложил двухключевую криптосистему, основанную на применении алгебраической теории кодирования [2]. В этой системе порождающая матрица G кода преобразуется секретным ключом в матрицу G', которая объявляется открытой и служит для кодирования заданного информационного вектора I и получения зашифрованного вектора Z_{krp}. Кроме того, вводится также секретный вектор ошибок веса не более τ. Уполномоченный пользователь, зная необходимую секретную информацию, вначале расшифровывает вектор Z_{krp}, а затем его декодирует для получения исходного

вектора I. Таким образом, эта система никак не защищена от ошибок в реальных каналах передачи данных и будет работать только при наличии идеального канала связи.

Аналогичный подход используется в криптосистеме Нидеррайтера [3] и в системе [4], в которой вводится "искусственный дефект", т.е. преднамеренные ошибки.

В работе [5] рассматривается система шифрование на основе двоичных кодов Рида-Маллера, а в работе [6] – на основе алгеброгеометрических кодов.

Указанные методы рассматривают помехоустойчивые коды лишь как теоретическую базу для обоснования защиты данных от несанкционированного доступа и никак не используют основное предназначение этих кодов – защиту от естественных искажений передаваемых данных.

Известны также подходы, которые обеспечивают одновременную защиту, как от ошибок канала связи, так и защиту от несанкционированного доступа.

Стохастическое кодирование, предложенном С.А. Осмоловским [7], включает две операции, выполняемые последовательно: собственно кодирование с помощью любого известного помехоустойчивого кода; стохастическое преобразование с помощью таблиц со случайным заполнением.

Попытка объединить операции кодирования и шифрования предпринята также и в работе [8], но при этом достигается слабая криптозащита (только на основе линейных преобразований) и на этапе расшифрования возможно влияние необнаруживаемой ошибки канала.

Цель роботы. Целью работы является поиск новых подходов к сближению теории кодирования и криптографии на основе единого математического аппарата – теории линейных последовательностных схем (ЛПС), максимальное совмещение во времени процессов помехоустойчивого кодирования и поточного шифрования для ускорения передачи данных, повышение криптостойкости поточного шифрования.

Кодирование циклических кодов с позиций теории ЛПС. В качестве помехоустойчивых кодов будем рассматривать циклические коды, имеющие широкую сферу применения. Известны два способа кодирования циклического (n,k)-кода: систематическое и несистематическое [9]. На практике чаще применяется систематическое кодирование, в результате которого n-разрядный кодовый вектор Z состоит из двух частей: заданного k-разрядного информационного вектора I и вычисленного $(n-k)$-разрядного контрольного вектора R.

Для криптографической защиты информации более пригодным является несистематическое кодирование. В этом случае информационный вектор I преобразуется таким образом, что в полученном в кодовом векторе Z невозможно разделить информационные и контрольные разряды. По сути выполняется шифрование данных на основе стохастического преобразования вектора I [10].

Для представления циклического кода Ω будем использовать математический аппарат линейных последовательностных схем (ЛПС). Согласно [11], ЛПС Λ с одним входом, одним выходом и r элементами памяти в дискретные моменты времени t над полем Галуа $GF(2)$ задается функцией состояний (переходов)

$$S(t+1) = A \times S(t) + B \times U(t), \quad GF(2), \tag{1}$$

и функцией выходов

$$Y(t) = C \times S(t) + D \times U(t), \quad GF(2), \tag{2}$$

где $A = \|a_{ij}\|_{r\times r}$, $B = \|b_{ij}\|_{r\times 1}$, $C = \|c_{ij}\|_{1\times r}$, $D = \|d_{ij}\|_{1\times 1}$ – характеристические матрицы ЛПС,

$S = \|s_i\|_r$, $U = \|u_i\|_1$, $Y = \|y_i\|_1$ – векторы: состояний, входной и выходной.

Размерности матриц ЛПС Λ и параметры циклического кода Ω связаны через коэффициент r, который для кода равен числу контрольных разрядов кодового вектора Z ($r = n - k$).

При реализации несистематического кодирования ЛПС представляет собой кодер, на вход которого поступает информационный вектор I, а на выходе формируется кодовый вектор Z, т.е. в системе обозначений ЛПС: $U = I$, $Y = Z$. В этом случае ЛПС должна работать в режиме умножителя, поэтому характеристические матрицы ЛПС должны быть следующими:

$$A = \begin{Vmatrix} 0 & 1 & 0 & \dots & 0 \\ 0 & 0 & 1 & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & \dots & 1 \\ 0 & 0 & 0 & \dots & 0 \end{Vmatrix}, \quad B = \begin{Vmatrix} 0 \\ 0 \\ \dots \\ 0 \\ 1 \end{Vmatrix}, \quad C = \begin{Vmatrix} g_0 & g_1 & g_2 & \dots & g_{r-1} \end{Vmatrix}, \quad D = \begin{Vmatrix} 1 \end{Vmatrix} \tag{3}$$

Элементы матрицы C представляют собой коэффициенты порождающего многочлена кода Ω:

$$g(x) = g_0 + g_1 x + g_2 x^2 + \dots + g_{r-1} x^{x-1} + g_r x^r \tag{4}$$

Аппаратной реализацией этой ЛПС, которую назовем кодирующей, является r-разрядный регистр сдвига без обратных связей.

Поточное шифрование с позиций теории ЛПС. Шифрование информации только в процессе несистематического кодирования является криптографически слабым. Поэтому введем дополнительный этап защиты с помощью новой ЛПС, которую назовем шифрующей.

Если на вход p-разрядной шифрующей ЛПС подать n-разрядный вектор Z, тогда на ее выходе через n тактов времени будет получен p-разрядный зашифрованный вектор Z_{crp} ($p \geq n$). В этом случае ЛПС должна работать в режиме делителя, и ее характеристические матрицы должны быть следующими:

$$A = \begin{bmatrix} 0 & 0 & 0 & \cdots & 0 & h_0 \\ 1 & 0 & 0 & \cdots & 0 & h_1 \\ 0 & 1 & 0 & \cdots & 0 & h_2 \\ \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & \cdots & 0 & h_{p-2} \\ 0 & 0 & 0 & \cdots & 1 & h_{p-1} \end{bmatrix}, \quad B = \begin{bmatrix} 1 \\ 0 \\ 0 \\ \dots \\ 0 \\ 0 \end{bmatrix}, \quad C = \begin{bmatrix} 0 & 0 & \dots & 0 & 1 \end{bmatrix}, \quad D = \begin{bmatrix} 0 \end{bmatrix}. \tag{5}$$

или

$$A = \begin{bmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & \cdots & 0 \\ 0 & 0 & 0 & \cdots & 1 \\ h_0 & h_1 & h_2 & \cdots & h_{p-1} \end{bmatrix}, \quad B = \begin{bmatrix} 0 \\ 0 \\ 0 \\ \dots \\ 0 \\ 1 \end{bmatrix}, \quad C = \begin{bmatrix} 1 & 0 & \dots & 0 & 0 \end{bmatrix}, \quad D = \begin{bmatrix} 0 \end{bmatrix}. \tag{6}$$

Элементы последнего столбца матрицы A вида (5) и элементы последней строки матрицы A вида (6) являются коэффициентами порождающего многочлена:

$$h(x) = h_0 + h_1 x + h_2 x^2 + \cdots + h_{p-2} x^{p-2} + h_{p-1} x^{p-1} + h_p x^p, \quad GF(2) \qquad (7)$$

Аппаратной реализацией шифрующей ЛПС, является p-разрядный регистр сдвига с линейными обратными связями (РСЛОС). ЛПС в режиме деления представляет собой генератор псевдослучайных чисел (ПСЧ), который обычно используется для формирования внешней псевдослучайной гаммы при поточном шифровании. В предлагаемом способе вектор Z проходит через шифрующую ЛПС, что равнозначно наложению на этот вектор псевдослучайной гаммы, как и при традиционном поточном шифровании. Для получения псевдослучайной последовательности максимальной длины 2^p (М-последовательности) порождающий многочлен (7) должен быть неприводимым и примитивным [11].

Кодирующая и шифрующая ЛПС могут работать одновременно, что дает возможность совместить во времени операции кодирования и шифрования. Как только на вход кодирующей ЛПС поступит первый разряд информационного вектора I, в следующем такте на ее выходе будет готов первый разряд кодового вектора Z. Полученные данные с выхода кодирующей ЛПС можно сразу же подавать на вход шифрующей ЛПС. Таким образом, шифрование будет осуществляться практически одновременно с помехоустойчивым кодированием, с задержкой лишь на один временной такт.

Основным способом криптографической защиты генераторов ПСЧ на основе РСЛОС является сохранение в секрете начального заполнения РСЛОС, т.е. начального состояния $S(0)$ в терминологии ЛПС. Однако, при наличии $2p$ разрядов открытого и зашифрованного текста, даже при отсутствии сведений о состоянии $S(0)$, легко вскрыть структуру внутренних связей РСЛОС (вид характеристических матриц ЛПС) и тем самым раскрыть весь шифр [12]. Если же начальное состояние ЛПС изменять каждые p тактов, тогда можно устранить такую возможность взлома. Поскольку просто хранить массив векторов начальных состояний $M = \{S_i(0)\}$ для шифрующей ЛПС слишком нерационально, поэтому мы приходим к необходимости генератора таких векторов ($i = 1,2,3,...$). В качестве указанного генератора может служить еще одна ЛПС (назовем ее вспомогательной), которая может иметь ту же структуру характеристических матриц, что и шифрующая ЛПС. Для i-го кодового вектора Z_i вспомогательная ЛПС будет генерировать вектор состояния $S_{aux}(i)$, который будет служить начальным состоянием $S_i(0)$ шифрующей ЛПС:

$$S_i(0) = S_{aux}(i).$$

Таким образом, для получения всего массива $M = \{S_i(0)\}$ необходимо задать лишь начальное состояние $S_{aux}(0)$ вспомогательной ЛПС, которое должно быть секретным.

В общепринятой криптографической терминологии начальное состояние $S_{aux}(0)$ вспомогательной ЛПС можно назвать базовым ключом K_b, а начальное состояние $S_i(0)$ шифрующей ЛПС – сеансовым ключом K_s.

Методы повышения криптостойкости шифросистем. Существуют различные критерии анализа стойкости криптосистем: теоретико-информационный, теоретико-сложностной, теоретико-системный.

Согласно К. Шеннону стойкий шифр должен обладать свойствами рассеивания и полноты [1].

Свойство рассеивания (diffusion) заключается в перераспределении избыточности исходного сообщения, которая имеется в различных местах этого сообщения посредством распространения ее на весь текст сообщения. Шифр будет обладать этим свойством, если изменение хотя бы одного бита открытого текста вызовет значительное (не менее половины

всех бит) изменение шифротекста. Несистематическое кодирование циклических кодов, как следует из формулы (1), обладает этим свойством.

Свойство полноты формулируется правилом: каждый выходной бит является нетривиальной функцией всех входных битов. В результате происходит перемешивание (confusion) битов исходного сообщения и зависимость между ключом преобразования и шифротекстом становится максимально сложной. Как следует из (2), выходной вектор $Y(t)$ шифрующей ЛПС, линейно зависит от всего входного вектора $U(t)$, который является кодовым вектором Z и исходным сообщением для этой ЛПС. Следовательно, прохождение кодового вектора Z через шифрующую ЛПС обеспечивает необходимое перемешивание разрядов этого вектора.

Однако, линейная зависимость значений результата от значений аргумента позволяет криптоаналитику легко взломать шифр с помощью статистического оценивания, используя, например, метод нахождения линейной регрессии [13]. Для устранения такой возможности необходимо выбирать для шифрования необратимые преобразования, причем для самого шифра должно сохраниться обратимое преобразование. Именно такую возможность – построить обратимый шифр из необратимых преобразований – позволяет сеть Фейстеля, которая является дальнейшим развитием шенноновской модели криптозащиты. В качестве необратимого преобразования для сети Фейстеля выбирают некоторую нелинейную функцию $\varphi()$, т.е. которую нельзя представить в виде линейного полинома от входных аргументов.

Подвергать нелинейным преобразованиям полученный с выхода шифрующей ЛПС вектор Z_{crp} нерационально, поскольку при ошибках в канале связи мы потеряем возможность его декодирования на стороне приемника. Напомним, что главным преимуществом циклических кодов является простые процедуры кодирования и декодирования благодаря именно их линейным свойствам. Сохранить линейные свойства кода и одновременно повысить уровень защиты от несанкционированного доступа можно, если в качестве нелинейной функции $\varphi()$ выбрать функцию, которая связывает соседние начальные состояния $S_i(0)$ и $S_{i+1}(0)$ шифрующей ЛПС:

$$S_{i+1}(0) = \varphi(S_i(0)). \qquad (8)$$

Поскольку мы приняли начальное состояние этой ЛПС в качестве сеансового ключа, поэтому преобразование (8) означает по сути формирование нелинейного сеансового ключа K_s^{non} из линейного сеансового ключа K_s:

$$K_s^{non} = \varphi(K_s). \qquad (9)$$

В качестве функций $\varphi()$ предлагается использовать бент-функции [14], которые обладают максимальной нелинейностью и легко аппаратно реализуются в течение одного временного такта [15]. В результате в канал передается квазислучайная последовательность, не зависящая от передаваемой информации.

Таким образом, предлагаемая система шифрования является композиционной, состоящей из трех последовательно применяемых шифров (уровней защиты): $F : F_1 \times F_2 \times F_3$, где F_1 – шифрование исходного информационного вектора на основе несистематического кодирования циклических кодов; F_2 – шифрование кодового вектора с помощью шифрующей ЛПС; F_3 – нелинейное преобразование сеансового ключа (9).

Если каждый по отдельности шифр не является достаточно стойким, однако их композиция уже отвечает как и классическим требованиям криптостойкости по Шеннону так и современным требованиям к построению шифров.

На рис. 1 показан процесс кодирования и шифрования на стороне передатчика.

Дешифрирование и декодирование с позиций теории ЛПС. Полученный из канала связи кодовый вектор необходимо дешифрировать и декодировать, желательно за

минимальное время. Рассмотрим математическое обоснование процесса дешифрирования на стороне приемника.

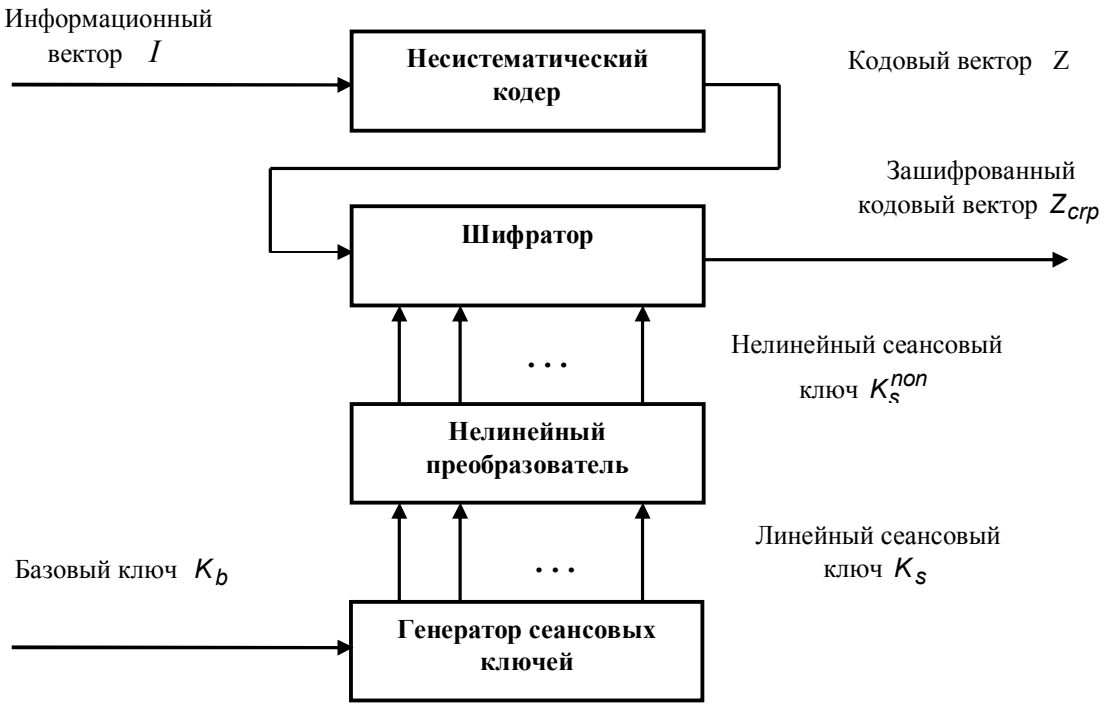

Рис. 1 Процесс кодирования и шифрования на стороне передатчика

Введем понятие сеансового пароля P_s как результат умножения нелинейного сеансового ключа K_s^{non} на n-ю степень характеристической матрицы A шифрующей ЛПС:

$$P_s = K_s^{non} \times A^n, \quad GF(2). \tag{10}$$

ТЕОРЕМА. Исходный кодовый вектор Z может быть получен в результате поразрядного сложения по модулю 2 зашифрованного кодового вектора Z_{crp} и сеансового пароля P_s:

$$Z = Z_{crp} + P_s, \quad GF(2). \tag{11}$$

Доказательство. Из теории ЛПС [11] известно, что в n-управляемой n-разрядной ЛПС для любых двух известных состояний $S_i(t)$ и $S_j(t)$ существует n-разрядный входной вектор $U(t)$, такой что

$$S_j(t) + A^n \times S_i(t) = L_n \times U(t), \quad GF(2) \tag{12}$$

где $L_n = \left| A^{n-1}B, A^{n-2}B, \ldots, AB, B \right|$, A^i - i-я степень характеристической матрицы A.

Для характеристических матриц A и B вида (5) и (6) матрица L_n представляет собой единичную $(n \times n)$-разрядную матрицу. Поэтому равенство (12) можно переписать как

$$S_j(t) + A^n \times S_i(t) = U^{\text{т}}(t), \quad GF(2) \tag{13}$$

где $U^{\text{т}}(t) = U^T(t)$ для матриц A и B вида (5), $U^{\text{т}}(t) = U(t)$ для матриц A и B вида (6).

Вектор $U^T(t)$ отличается от вектора $U(t)$ инверсным расположением элементов (на первом месте – последний и т.д.). Если вектор состояния $S_i(t)$ интерпретировать как нелинейный сеансовый ключ K_s^{non}, вектор состояния $S_j(t)$ – как переданный

зашифрованный кодовый вектор Z_{crp}, а входной вектор $U^{1}(t)$ – как исходный кодовый вектор, тогда из равенств (10) и (13) следует равенство (11). Теорема доказана.

Таким образом, для дешифрования кодового вектора Z_{crp} с целью восстановления кодового вектора Z на стороне приемника необходимо последовательно выполнить две задачи: вначале сформировать нелинейный сеансовый ключ K_S, а затем – сеансовый пароль P_S. Выполнение первой задачи осуществляется точно так же, как и на стороне передатчика, следовательно, понадобится точно такая же шифрующая ЛПС и средства реализации бент-функции.

Возможны два варианта выполнения второй задачи: последовательный и параллельный. Как следует из (10) сеансовый пароль P_S можно найти за n тактов, поочередным умножением сеансового ключа K_S на матрицу A шифрующей ЛПС: $P_S = K_S \times (A \times A \times \ldots \times A)$, $GF(2)$. Если передача по каналу связи зашифрованного вектора Z_{crp} осуществляется последовательно, тогда к окончанию его передачи будет закончено вычисление и сеансового пароля P_S. Если же вектор Z_{crp} поступает по каналу связи сразу, тогда за один такт можно сформировать и сеансовый пароль P_S, поскольку n-ю степень матрицы A можно вычислить заранее. В этом случае процесс дешифрования, согласно (11), может быть выполнен одновременно (параллельно) по всем n разрядам векторов, т.е. за один временной такт.

Для получения исходного информационного вектора I выполняется декодирование кодового вектора Z в течение n тактов с помощью ЛПС (назовем ее декодирующей) в режиме делителя с порождающим многочленом (4). Начальное состояние кодера и декодера принимается нулевым. Если конечное состояние этой ЛПС после декодирования снова станет нулевым, это будет свидетельствовать об отсутствии ошибок при передачи данных. В противном случае после декодирования необходимо исправить появившиеся ошибки, если их количество не превышает корректирующую способность циклического кода. На рис. 2 показан процесс дешифрирования и декодирования на стороне приемника.

Заключение. Помехоустойчивое кодирование и криптография – это две разновидности преобразования информации, которые дополняют друг друга, а их совместное использование позволяет эффективно использовать каналы связи для надежной защиты передаваемой информации.

Использование единого математического аппарата – теории ЛПС – обеспечивает максимальное совмещение во времени операций кодирования и криптозащиты, что позволяет утверждать о действительном объединении этих способов защиты данных. Достоинством такого способа объединения является то, что наложение на кодовый вектор псевдослучайной гаммы с помощью шифрующей ЛПС никак не ухудшает корректирующие свойства циклического кода.

Предлагаемая трехуровневая система шифрования отвечает и требованиям криптостойкости по Шеннону, и современным требованиям к построению шифров. Каждый разряд исходных данных кодируется и шифруется в течение одного такта работы ЛПС (т.е. сдвига регистра), что значительно быстрее поиска нужных данных в громоздких стохастических таблицах [7].

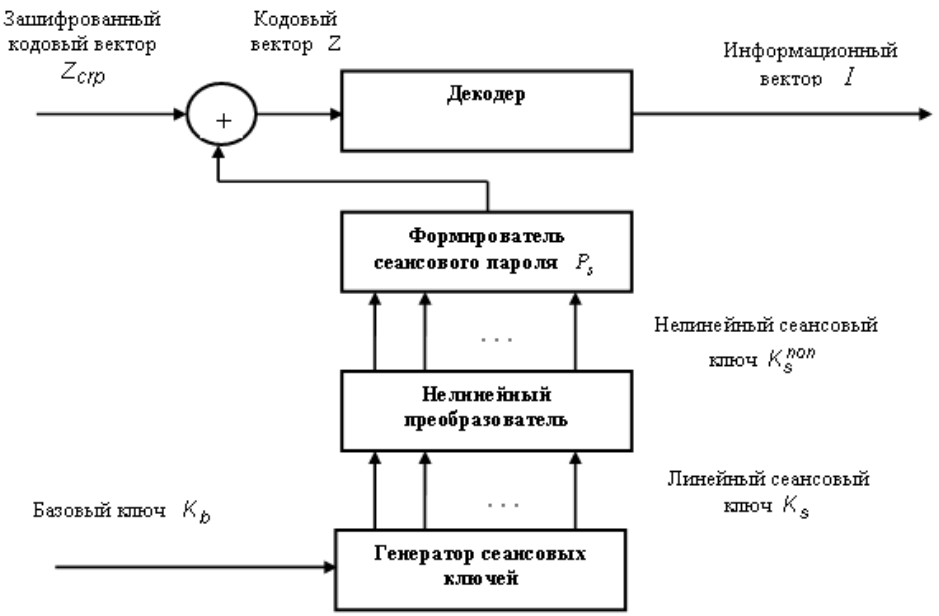

Рис. 2. Процесс дешифрирования и декодирования на стороне приемника

В предлагаемой системе рассматривается только традиционная модель ошибок в канале связи (инверсные ошибки), поэтому дальнейшие исследования должны быть направлены на учет более широкого класса канальных ошибок и повышения степени криптозащиты.

ЛИТЕРАТУРА

1. Шеннон К. Работы по теории информации и кибернетике / К. Шеннон – М.: Изд-во иностр. лит., 1963. – 829 с.

2. R.J. McEliece. A Public-Key Criptosystem Based on Algebraic Theory. // DGN Progres Report 42-44, Jet Propulsi on Lab. Pasadena, CA. January – February, 1978. – pp. 114-116.

3. H. Niederreiter. Knapsack-Type Cryptosystems and Algebraic Coding Theory. // Probl. Control and Inform. Theory. – 1986. – V.15. – pp. 19-34.

4. Конопелько В.К. Защита информации кодовыми криптосистемами на основе теории норм синдромов и свойств циклотомической перестановки чисел / В.К. Конопелько, О.Г. Смолякова – Технические средства защиты информации. Материалы докл. 6-й Белорусско-российской научно-техн. конф. (Минск 19-23 мая 2008 г.), Минск, с. 65.

5. Сидельников В.М. Открытое шифрование на основе двоичных кодов Рида-Маллера / В.М. Сидельников // Дискретная математика, М. – 1994. – том 6, выпуск 3. – С.3-20.

6. Стасев Ю.В. Несимметричные теоретико-кодовые схемы с использованием алгеброгеометрических кодов / Ю.В. Стасев, А.А. Кузнецов // Кибернетика и системный анализ. – 2005. – №3. – С. 47-57.

7. Осмоловский С.А. Стохастические методы защиты информации / Осмоловский С.А. – М.: Радио и связь, 2003. – 320 с.

8. Кириллов С.Н. Модифицированный помехозащищенный кодер на основе БИХ-фильтра / С.Н. Кириллов, Д.С. Семин // Вестник РГРТУ. Рязань – 2009. – № 2 (вып. 28). – С. 27-30.

9. Морелос-Сарагоса Р. Искусство помехоустойчивого кодирования / Морелос-Сарагоса Р. Методы, алгоритмы, применение: Пер. с англ. – М.: Техносфера, 2006. – 320 с.

10. Патент України на корисну модель 50203, МПК H03M 13/00. Спосіб завадостійкого кодування дискретної інформації із захистом / Семеренко В. П., Дубров О.Ф.; заявл. 21.12.09 ; опубл. 25.05.10, Бюл. №10, 2010.

11. 11. Гилл А. Линейные последовательностные машины / А. Гилл: пер. с англ. А.С. Бернштейна. – М.: Наука, 1974. – 288 с.

12. Семеренко В. П. Потокове шифрування на основі теорії лінійної послідовнісної машини / В.П. Семеренко, Ю.В. Степанишин, М.Л. Гаєвський // Інформаційні технології та комп'ютерна інженерія. – 2007. – № 3 – С. 86-93.

13. Аграновский А.В. Практическая криптография: алгоритмы и их программирование / А.В. Аграновский, Р.А. Хади – М.: СОЛОН-Пресс, 2002. – 256 с.

14. Логачев О.А. Булевы функции в теории кодирования и криптологии / Логачев О.А., Сальников А.А., Ященко В.В. – М.: МЦНМО, 2004. – 470 с.

15. Семеренко В. П. Параллельная реализация поточного шифрования. – Тези міжвідомчої науково-практичної конференції “Сучасні проблеми захисту інформації з обмеженим доступом”. (Київ, 20-21 листопада 2008 р.) – Київ, НАУ, 2008. – с.50-51.

Надійшла: 17.09.2011

Рецензент: д.т.н., проф. Юдін О.К.