ОПИСАНИЕ ИЗОБРЕТЕНИЯ К ПАТЕНТУ

(12)

РЕСПУБЛИКА БЕЛАРУСЬ

(19) **BY** (11) **4997**

(13) **C1**

(51)[7] **H 04L 9/00,**
G 06F 11/08

НАЦИОНАЛЬНЫЙ ЦЕНТР
ИНТЕЛЛЕКТУАЛЬНОЙ
СОБСТВЕННОСТИ

(54) **УСТРОЙСТВО КРИПТО-КОРРЕКТИРУЮЩЕГО ПРЕОБРАЗОВАНИЯ ИНФОРМАЦИИ**

(21) Номер заявки: a 19990661
(22) 1999.07.02
(46) 2003.03.30

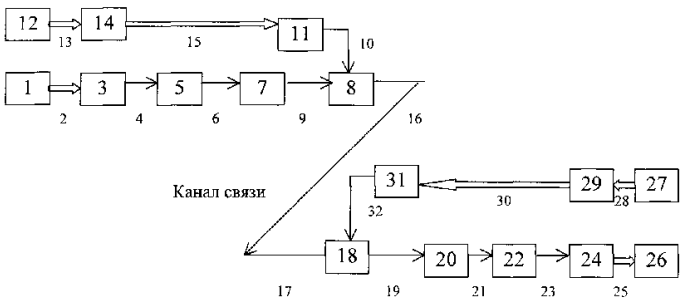
(71) Заявитель: Учреждение образования "Белорусский государственный технологический университет" (BY)

(72) Авторы: Урбанович Павел Павлович; Пацей Наталья Владимировна (BY)

(73) Патентообладатель: Учреждение образования "Белорусский государственный технологический университет" (BY)

(57)

Устройство крипто-корректирующего преобразования информации, содержащее на передающей стороне источник данных, выходами соединенный со входами первого регистра данных, первый источник ключа, выходами связанный со входами первого регистра ключа, блок помехоустойчивого кодирования, выход которого соединен с первым входом первого сумматора по модулю два, вторым входом подключенного к выходу первого генератора псевдослучайной последовательности, а выходом - к каналу передачи данных, соединенному на приемной стороне с первым входом второго сумматора по модулю два, вторым входом подключенного к выходу второго генератора псевдослучайной последовательности, а выходом соединенного со входом блока помехоустойчивого декодирования, второй источник ключа, выходами подключенный ко входам второго регистра ключа, **отличающееся** тем, что оно содержит блок сжатия данных, входом соединенный с выходом первого регистра данных, а выходом - со входом блока помехоустойчивого кодирования, блок развертывания, входом соединенный с выходом блока помехоустойчивого декодирования, а выходом - со вторым регистром данных, коммутирующим по выходам приемник данных, вход первого генератора псевдослучайной последовательности соединен с выходом первого регистра ключа, а вход второго генератора псевдослучайной последовательности - с выходом второго регистра ключа.



Фиг. 1

BY 4997 C1

(56)
US 4208739 A, 1980.
US 5574785 A, 1996.
EP 0676876 A1, 1995.
EP 0278170 A2, 1988.
SU 2096918 C1, 1997.
SU 2032990 C1, 1995.
SU 2097931 C1, 1997.
SU 2099890 C1, 1997.

Изобретение относится к криптографическим преобразованиям, сжатию данных и корректирующему кодированию и может быть использовано при хранении данных и в технике связи.

Известны способы и устройства шифрования информации в системах связи и обработки информации, которые построены на основе криптографических алгоритмов и корректирующих кодов. Некоторые из этих систем построены на основе добавления к криптографическим преобразованиям схем помехоустойчивого кодирования после [1, 2, 3] либо до них [4] (в [3] используется схема обнаружения ошибок с запросом повторной передачи).

Недостатком этих способов, и соответственно устройств, является то, что увеличивается размер закодированных данных и, как результат - замедление работы системы, снижение пропускной способности.

Наиболее близким техническим решением к предлагаемому является устройство интегрированного криптографического и кодового преобразования и передачи информации [5], содержащее на передающий стороне источник данных (m), выходами соединенный со входами блока, реализующего функцию расширения (F); выходы его соединены со входами кодера (G_e), выходы которого соответственно коммутируются с выходами генератора искусственного шума (n), вследствие чего формируется канальное сообщение (x) на передающей стороне, на приемной стороне устройство содержит канальный декодер, входами соединенный с каналом передачи, а выходами - со входами потребителя данных. В этом устройстве функция расширения F может быть любой линейной временной зависимой или временной независимой функцией с памятью или без памяти, блоковым кодом или сверточным кодом. Процесс шифрования данных выглядит следующим образом:

$x = F(m)G_e + n$, где m - открытый текст, x - сообщение, подаваемое на вход канала.

В результате конкатенции (последовательного прибавления справа) F и G_e получаем на приемной стороне интегрированный сверточный декодер G_d, и дешифрование выглядит следующим образом:

$\hat{m} = G_d(y)$, где $\hat{m}$ - получаемое дешифрованное сообщение, а

$y = x + z = (F(m)G_e + n) + z = F(m)G_e + e$,

где $e = n + z$, y - сообщение на выходе канала передачи, z - аддитивная последовательность шума канала.

Так как данная система осуществляет криптографическое преобразование данных, то необходимым условием ее функционирования является существование секретных элементов. В данном случае ключом, который должен держаться в секрете, является функция расширения F или, другими словами, сам алгоритм шифрования. Пример реализации функции F, предложенный в [5], легко позволяет производить криптоанализ алгоритма за приемлемое время без знания функции F, а при компрометации функции система вовсе не требует анализа и становится тривиальной системой коррекции ошибок, возникающих в канале. Вместе с тем использование корректирующего кода приводит к увеличению длины исходного сообщения, зависящей в общем случае от типа применяемого помехоустой-

чивого кода. Перечисленные особенности известного решения снижают эффективность его использования в системах передачи данных с криптопреобразованиями и помехоустойчивым кодированием.

Задачей изобретения является снижение информационной избыточности сообщения и повышение эффективности устройства передачи потока данных с использованием криптографических преобразований и помехоустойчивого кодирования данных.

Поставленная задача достигается тем, что в устройство крипто-корректирующего преобразования информации, содержащее на передающей стороне источник данных, выходами соединенный со входами первого регистра данных, первый источник ключа, выходами связанный со входами первого регистра ключа, блок помехоустойчивого кодирования, выход которого соединен с первым входом первого сумматора по модулю два, вторым входом подключенного к выходу первого генератора псевдослучайной последовательности (ПСП), а выходом - к каналу передачи данных, соединенному на приемной стороне с первым входом второго сумматора по модулю два, вторым входом подключенного к выходу второго генератора псевдослучайной последовательности, а выходом соединенного со входом блока помехоустойчивого декодирования, соединенному с регистром данных, устройство содержит также второй источник ключа, выходами подключенный ко входам второго регистра ключа, блок сжатия данных, входом соединенный с выходом первого регистра данных, а выходом - со входом блока помехоустойчивого кодирования, блок развертывания, входом соединенный с блоком помехоустойчивого декодирования, а выходом - со вторым регистром данных, входы первого генератора псевдослучайной последовательности соединены с выходами первого регистра ключа, а выходы второго генератора псевдослучайной последовательности - с выходами второго регистра ключа.

Сущность изобретения заключается в том, что вместо блока преобразования данных (F), осуществляющего линейные преобразования, используется блок сжатия данных, построенный на основе нелинейных операций, и тем самым позволяющим снизить информационную избыточность сообщения.

Изобретение поясняется чертежами:

фиг. 1 - структурная схема устройства крипто-корректирующего преобразования двоичной информации;

фиг. 2 - структурная схема блока сжатия данных;

фиг. 3 - структурная схема блока помехоустойчивого кодирования;

фиг. 4 - структурная схема генератора ПСП;

фиг. 5 - структурная схема блока помехоустойчивого декодирования;

фиг. 6 - структурная схема блока развертывания;

фиг. 7 - пример построения дерева кодирования;

фиг. 8 - диаграмма состояний декодера Витерби.

На фиг. 1 представлена структурная схема устройства крипто-корректирующего преобразования двоичной информации.

Устройство (фиг. 1) содержит источник данных 1, выходами 2 подключенный к первому регистру данных 3, выходом 4 подключенный к входу блока 5 сжатия информации, выход которого 6 подключен к входу блока 7 помехоустойчивого кодирования. Устройство также содержит первый сумматор 8 по модулю два, первый вход которого соединен с выходом 9 блока кодирования 7, а второй вход сумматора 8 - с выходом 10 генератора ПСП 11, первый источник ключа 12, выходами 13 соединенный с первым регистром ключа 14, инициализирующим через выходы 15 первый генератор ПСП 11 по заданному алгоритму. Закодированные на передающей стороне данные 16 поступают в каналы связи и, поврежденные (чаще всего) шумом, поступают на первый вход 17 второго сумматора по модулю два 18 на приемной стороне, выходом 19 соединенный с блоком помехоустойчивого декодирования 20, сигнал с выхода 21 которого поступает на вход блока развертыва-

ния 22, выходом 23 соединенного со вторым регистром данных 24, коммутирующим по выходам 25 приемник данных 26. Приемная сторона содержит также второй источник ключа 27, выходами 28 соединенный со вторым регистром ключа 29, инициализирующим по входам 30 второй генератор 31 ПСП, выходом 32 связанный со вторым сумматором по модулю два 18.

Блок сжатия данных 5 может функционировать по любому из фундаментальных алгоритмов сжатия данных (арифметические или префиксные коды, коды Хаффмана, Шеннона-Фано, словарные алгоритмы, PCM и т.д.). В предлагаемой реализации блок сжатия данных 5 построен по схеме на основе кода Хаффмана переменной длины с множественными статичными таблицами (фиг. 2). Ключевая идея кодирования кодами переменной длины Хаффмана состоит в использовании более коротких кодовых слов для наиболее часто встречающихся символов, что позволяет сжимать текст в общем на 30 %-70 % [6]. В частности, он содержит i накапливающих сумматоров символов 33, подсчитывающих частоту встречаемости каждого символа в тексте. Данные с сумматоров 34 поступают в компаратор 35 для определения (формируется на выходе 36) наиболее подходящей кодовой таблицы Хаффмана, заранее построенной и хранимой в j блоках 37 кодовых таблиц Хаффмана. Сигнал 36 с компаратора 35, поступающий в блок кодирования 38, активизирует по шине 39 одну из таблиц кодирования 37, которая, в свою очередь, используется блоком кодирования 38 вместе с исходными данными 4. Номер используемой таблицы, необходимый для развертывания (декомпрессии, распознавания), по выходу 40 подается на выход 6 до начала поступления бинарного кода[6].

Блок помехоустойчивого кодирования 7 может быть реализован на основе сверточных кодов. На фиг. 3 для примера приведена схема блока 7 на основе сверточного кода (9,6), исправляющего одиночные ошибки с порождающей матрицей, представленной в виде многочленов[7]:

$G(x) = [x\ x^5 + 1\ x^4 + x^2 + x]$.

Блок 7 содержит последовательно-параллельный регистр 41 размером 2 бита с выходами 42 и 43, первый 44 и второй 45 регистры сдвига размера 2 бита, три сумматора по модулю два 46, 47, 48 и параллельно-последовательный регистр 49 на 3 бита с входами 50, 51 и 52. Принцип функционирования блока 7 известен [7].

Параллельно с процессом помехоустойчивого кодирования формируется псевдослучайная последовательность бит генератором 11. Пример построения генератора ПСП 11 показан на фиг. 4. Он строится на основе комбинации двух известных техник формирования ПСП: А- схеме Геффе, при которой используются линейные сдвиговые регистры с обратной связью с разными периодами характеристических полиномов и В - алгоритма сотовой системы связи А5 [8]. Генератор А состоит из трех линейных регистров сдвига 53, 54, 55, трех сумматоров 56, 57 и 58 по модулю 2 соответственно в цепи обратной связи и мультиплексора 59. Выход 60 регистра 55 используется для выбора одного из выходов 61 или 62 двух других регистров 54 и 53. Сдвиговые регистры функционируют на основе характеристических полиномов последовательностей максимальной длины, имеющих вид для 53, 54, 55 соответственно:

$1 + x^{27} + x^{98}$,

$1 + x + x^7 + x^8 + x^{27}$,

$1 + x^2 + x^{19} + x^{21} + x^{40}$.

Генератор В - также построен на трех линейных регистрах сдвига 63, 64, 65, трех сумматорах 66, 67 и 68 по модулю 2 соответственно в цепи обратной связи, трех элементах НЕ 69, 70, 71 и трех элементах И 72, 73 и 74. Сдвиговые регистры функционируют на основе характеристических полиномов, имеющих вид для 63,64, 65 соответственно:

$x^2 + x^{12} + x^{16} + x^{21}$,

$x^2 + x^6 + x^8 + x^{16}$,

$x^2 + x^5 + x^{11} + x^{22}$.

Сдвиговые регистры 53, 54, 55, 63, 64 и 65 инициализируются последовательно ключом из первого регистра ключа 14 (фиг. 1). Выходные сигналы генераторов А -75 и В -76 суммируются в блоке 77 суммирования по модулю, в результате чего формируется результирующий сигнал 10, подаваемый на вход блока 8.

На приемной стороне второй генератор 31 ПСП выполнен аналогично генератору 11 на передающей стороне и инициализируется тем же ключом, который поступает из второго источника ключа 27 через второй регистр ключа 29.

Блок помехоустойчивого декодирования может быть реализован на основе последовательного или синдромного декодирования, либо по схеме Витерби. Так как в выбранном коде (9,6) длина кодового ограничителя $\nu = 4$, то можно применить полный алгоритм декодирования Витерби с фиксированным временем декодирования[7]. Блок 20 помехоустойчивого декодирования (фиг. 5) состоит из последовательно-параллельного регистра 78 размера 3 бита, вычислителя метрики ветвей 79, блока 80 изменения состояния, блока принятия решения 81 и параллельно-последовательного регистра 82 размера 2 бита[7] (принцип функционирования блока рассмотрен ниже на конкретном примере).

Декодированные данные 21 с исправленными ошибками подаются на вход блока развертывания 22. Блок развертывания 22 (фиг. 6) хранит j статичных таблиц кодирования Хаффмана 83 идентичных таблицам 37 (фиг. 2). Блок 22 состоит также из блока выбора таблицы 84, на который подается сигнал 85 с приемника о номере использованной при кодировании таблицы и непосредственно декодера 86 с поступающим на него бинарным кодом 21 и выходом 23.

Отметим, что во всех описанных схемах (фиг. 1-6) сигналы синхронизации не показаны.

Если ввести следующие обозначения: m - исходные данные, К - ключ, G_e- порождающая матрица помехоустойчивого кода, F - функция сжатия данных, H - функция формирования псевдослучайной последовательности, а x - закодированная последовательность данных, то процесс прямого крипто-корректирующего преобразования можно записать так:

$x = G_e d \oplus H(K)$,

где

$d = E(m)$.

Тогда процесс обратного преобразования может быть представлен следующим образом:

$m = H(K) \oplus DF(G_d(y))$,

где $y = x + z$, а z - канальный шум, G_d- функция помехоустойчивого декодирования, DF - функция развертывания.

Рассмотрим на примере процесс функционирования предлагаемого устройства. Пусть задан ключ размером 256 бит:

QegpwuPfDtMETvweQXEwENOJKWAZUSNO,

или в ASCII: 71 65 67 70 77 75 50 66 44 74 4D 45 54 76 77 65 51 58 45 77 45 4E 4F 4A 4B 57 41 5A 53 4E 4F 71 74.

Передается сообщение: EXAMPLTEXT (из источника сообщения 1).

В блоках 33 схемы сжатия 5 считается частота каждого символа текста (табл. 1) и в 35 выбирается оптимальная таблица кодирования. Допустим, что выбрана вторая таблица 37, построенная на основе дерева кодирования (фиг. 7), в котором узлы с наименьшей частотой объединяются в новый узел с частотой равной сумме исходных. Кодирование начинается с корня. Если обход идет по правой ветви, то ставится 1, если по левой, то 0. Согласно этому правилу кодирования, исходный текст кодируется 30-ю битами и принимает вид:

00010011001111001010011 0001011.

Таким образом, текст сжимается на 52,5 % по сравнению с представлением его в двоичном коде ASCII (80 бит - в ASCII и 8 + 30 бит в сжатом виде). На выход 6 блока 5 будет

передаваться сначала номер используемой таблицы кодирования 40, а затем текст сообщения (в данном случае это 30 бит). Закодированный тест поступает на блок помехоустойчивого кодирования 7. Согласно алгоритму его работы (фиг. 3), получаем закодированный текст с избыточными разрядами (табл. 2), всего 45 бит (для упрощения номер выбранной таблицы не указывается):

000101000101011100110010001011100011001011111.

Формирование псевдослучайной последовательности происходит согласно схеме, представленной на фиг. 4. Значения сигналов на выходах 75, 76, 10, 9 и 16 представлены в табл. 3.

Предположим, что в процессе передачи данных возникли 3 одиночные ошибки: в 6-ом, 15-ом и 36-ом разрядах (ошибочные символы подчеркнуты, а в табл. 3 обозначены - x):

11100**0**00011010**1**0100010001011101101000**0**01110101.

Тогда в приемнике после суммирования входных данных 17 по модулю два с псевдослучайной последовательностью получаем данные 19 (см. табл. 3), которые поступают на блок помехоустойчивого декодирования 20.

Декодирование строится по алгоритму Витерби. Решетка декодирования или диаграмма состояний декодера (фиг. 8) построена и функционирует на основе таблицы состояний (табл. 4) и таблицы выходов (табл. 5) помехоустойчивого кодера 7. Декодирование начинается с нулевого состояния (t = 0), по 3-ем битам принятой последовательности 19 - 000 определяется наиболее правдоподобный путь к каждому из возможных узлов (состояний). Переход из 0-ого состояния в 4-ое возможен при входном кадре 101, из 0-ого в 0-ое при 000, из 0-ого в 8-ое при 010 и из 0-ого в 12-ое при 111 (на фиг. 8 обозначены линиями со стрелками). Определяется расстояние между каждым из возможных путей и принятым кадром, которое в дальнейшем будем называть мерой расходимости [7]. В первом такте (t = 0) наименьшая мера расходимости, равная нулю, будет при переходе из 0-ого в 0-ое состояние. По табл. 5 определяются выходные биты: 00. Во втором такте (t = 1) аналогично выбирается наиболее правдоподобный путь. Это переходы из 0-ого в 8-ое и из 0-ого в 11-ое состояния, что соответствует входным 010 и 111 и выходным 01 и 11 кадрам. Мера расходимости в обоих случаях равна единице. Для разрешения неопределенности необходимо продолжить оба этих пути. На третьем такте (t = 2) при входном кадре 001 наиболее правдоподобными являются переходы из 8-ого во 2-ое состояние (мера расходимости равна нулю), и из 12-ого во 2-ое (мера расходимости также равна нулю). Для устранения неопределенности выбирается путь из 8-ого состояния во 2-ое. Аналогично идет процесс декодирования в оставшихся кадрах. Для разрешения неопределенности в пятом такте (t = 4) все пути с наименьшей мерой расходимости продолжаются до восьмого такта (t = 7), где продолжение двух менее правдоподобных путей не имеет смысла. На фиг. 8 жирной линией обозначен кратчайший путь к следующему узлу решетки декодера (или путь декодирования); двойной пунктирной - пути к узлам решетки, относительно которых существует неопределенность, и тонкой со стрелкой - все возможные пути из текущего узла.

После исправления ошибок (фиг. 8) получаем последовательность:

00 010 0110 0111 100 101 00 11 00 010 11,

которая поступает на блок развертывания 22. Декодирование начинается с вершины (см. фиг. 7): первый бит равен 0, следовательно обход идет по левой ветви и в стек блока 86 заносится второй бит - 0, снова выбирается левая ветвь и достигается лист дерева E. Аналогично двигаясь по пути 010, достигается символ X и т.д., пока весь текст не будет восстановлен. После развертывания получаем текст: EXAMPLTEXT, что соответствует передаваемой последовательности.

Таблица 1

Символ	Частота
E	3
X	2
A	1
M	1
P	1
L	1
T	2

Таблица 2

Выходы блока 41		Входы блока 49		
42	43	50	51	52
0	0	0	0	0
0	1	0	1	0
0	0	0	0	1
1	1	1	1	0
0	0	0	0	1
1	1	1	0	0
1	1	1	1	0
0	0	0	1	0
1	0	1	1	0
1	0	1	0	1
0	1	0	0	0
1	0	1	1	0
0	0	0	0	1
1	0	1	1	1
1	1	1	1	1

Таблица 3

Входы / Выходы						
75	76	10	9	16	17	19
0	1	1	0	1	1	0
1	0	1	0	1	1	0
1	0	1	0	1	1	0
1	1	0	0	0	0	0
0	1	1	1	0	0	1
0	1	1	0	1	**×0**	**1**
1	1	0	0	0	0	0
1	1	0	0	0	0	0
0	1	1	1	0	0	1
1	1	0	1	1	1	1
1	1	0	1	1	1	1
0	0	0	0	0	0	0
0	1	1	0	1	1	0
1	1	0	0	0	0	0

Продолжение табл. 3

Входы / Выходы						
75	76	10	9	16	17	19
0	1	1	1	0	**×1**	**0**
1	0	1	1	0	0	1
0	1	1	0	1	1	0
1	1	0	0	0	0	0
0	1	1	1	0	0	1
1	0	1	1	0	0	1
0	1	1	0	1	1	0
1	1	0	0	0	0	0
0	1	1	1	0	0	1
1	1	0	0	0	0	0
0	0	0	1	1	1	1
1	0	1	1	0	0	1
0	1	1	0	1	1	0
1	1	0	1	1	1	1
0	1	1	0	1	1	0
0	1	1	1	0	0	1
0	1	1	0	1	1	0
0	1	1	0	1	1	0
1	1	0	0	0	0	0
1	1	0	1	1	1	1
1	0	1	1	0	0	1
1	1	0	0	0	0	0
0	1	1	0	1	**×0**	**1**
1	1	0	0	0	0	0
1	1	0	1	1	1	1
1	1	0	1	1	1	1
1	1	0	1	1	1	1
1	0	1	1	0	0	1
1	1	0	1	1	1	1
1	0	1	1	0	0	1
1	1	0	1	1	1	1

Таблица 4

Входные кадры	00	01	10	11
Текущ. сост.	Следующее состояние			
0000	0000	0100	1000	1100
0001	0000	0100	1000	1100
0010	0000	0100	1000	1100
0011	0000	0100	1000	1100
0100	0001	0101	1001	1101
0101	0001	0101	1001	1101
0110	0001	0101	1001	1101
0111	0001	0101	1001	1101
1000	0010	0110	1010	1110
1001	0010	0110	1010	1110
1010	0010	0110	1010	1110
1011	0010	0110	1010	1110
1100	0011	0111	1011	1111
1101	0011	0111	1011	1111
1110	0011	0111	1011	1111
1111	0011	0111	1011	1111

Таблица 5

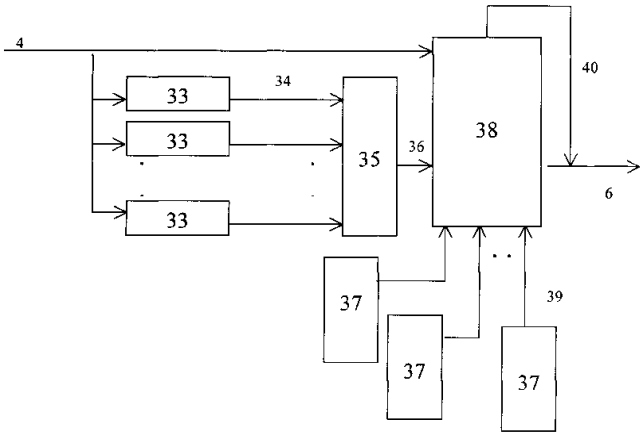
Входные кадры	00	01	10	11
Текущ. сост.	Выходные кадры			
0000	000	101	010	111
0001	010	111	000	101
0010	001	100	011	110
0011	011	110	001	100
0100	000	101	010	111
0101	010	111	000	101
0110	001	100	011	110
0111	011	110	001	100
1000	001	100	011	110
1001	011	110	001	100
1010	000	101	010	111
1011	010	111	000	101
1100	001	100	011	110
1101	011	110	001	100
1110	000	101	010	111
1111	010	111	000	101

Таким образом, предлагаемое устройство потокового крипто-корректирующего преобразования информации выполняет те же функции, что и известное. Однако преимущество предлагаемого устройства состоит в увеличении фактической пропускной способности устройства преобразования и в более эффективном использовании каналов связи (или устройств хранения информации). Действительно сжатие исходных данных на 20 %-100 % и более (в приведенном примере исходная последовательность в 80 бит сжимается на 52,5 %) позволяет использовать в данном устройстве помехоустойчивые коды с раз-

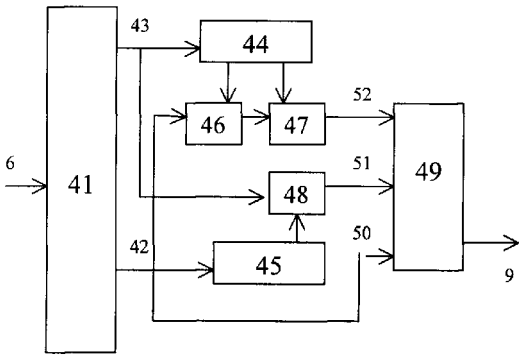
личной корректирующей способностью и соответственно увеличивать избыточность сжатых данных для исправления возникающих ошибок практически без увеличения размера исходной последовательности, что невозможно в известном устройстве [5] без увеличения размера передаваемого сообщения.

Источники информации:

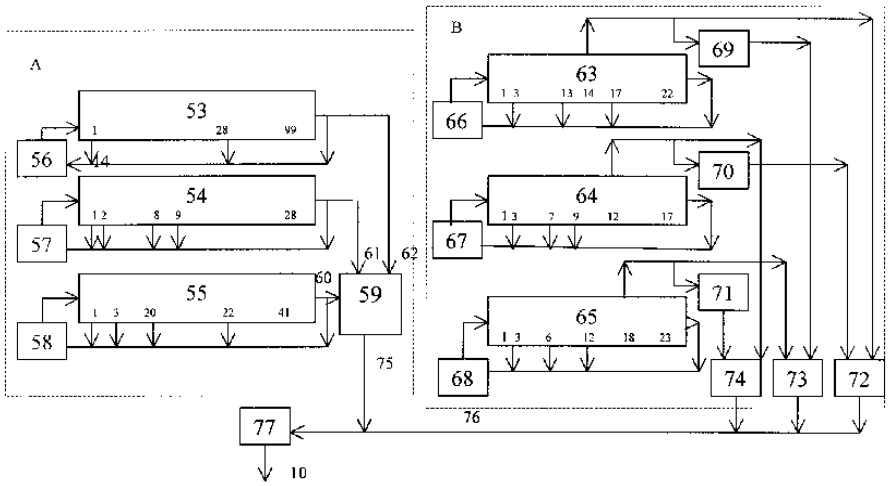
1. Патент США 5574785, МПК H 04L 9/00, 1996.
2. Патент США 4639548, МПК H 04L 9/00, 1987.
3. Патент США 5073932, МПК H 04K 1/00, H 04M 1/00, 1990.
4. Патент США 5504818, МПК H 04L 9/00, 1996.
5. Патент США 4208739, МПК H 04L 9/00, 1980.
6. Патент США 5528628, МПК H 04B 1/66, H 04B 14/04, H 04N 11/02, 1996.
7. Блейхут Р. Теория и практика кодов, контролирующих ошибки. - М.: Мир, 1986. - С. 480.
8. Savard J., Shift-Register stream cipher, 1998, URL: http://fn2 freenet. edmonton.ab.ca/~jsavard/co041101.html.



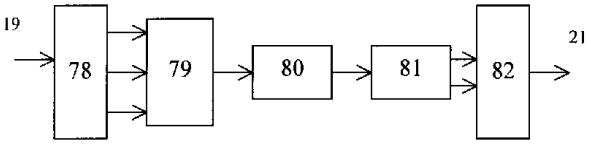
Фиг. 2



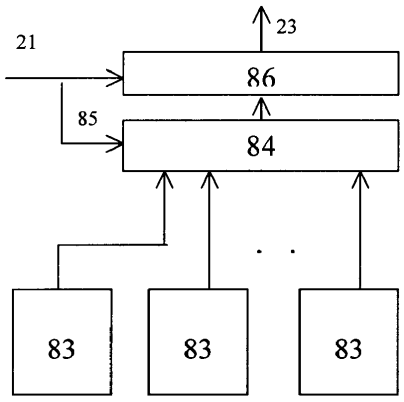
Фиг. 3



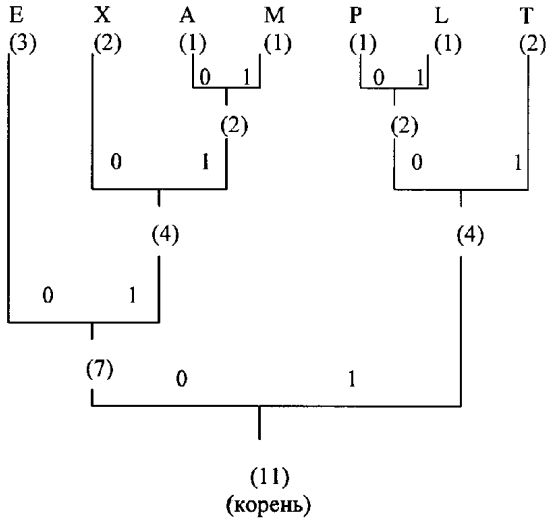
Фиг. 4



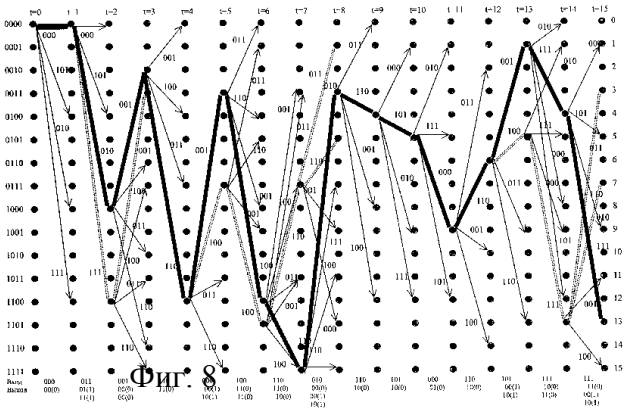
Фиг. 5



Фиг. 6



Фиг. 7



Фиг. 8