



УКРАЇНА

(19) UA (11) 23491 (13) A

(51)6 H 03 M 13/00

ДЕРЖАВНЕ
ПАТЕНТНЕ
ВІДОМСТВООПИС ДО ПАТЕНТУ
НА ВІНАХІДбез проведення експертизи по суті
на підставі Постанови Верховної Ради України
№ 3769-XII від 23 XII 1993 рПублікується
в редакції заявника

(54) СПОСІБ КОДУВАННЯ І ПЕРЕДАВАННЯ ІНФОРМАЦІЇ З ЗАХИСТОМ ТА ПРИСТРІЙ ДЛЯ ЙОГО ЗДІЙСНЕННЯ

1

(21) 96124764

(22) 20.12.96

(24) 02.06.98

(46) 31.08.98. Бюл. № 4

(47) 02.06.98

(72) Кулик Анатолій Ярославович, Кривогуб-
ченко Сергій Григорович, Компанець Мико-
ла Миколайович, Шават Роман
Володимирович(73) Вінницький державний технічний
університет

(57) 1. Способ кодирования и передачи информации, включающий в себя модуляцию последовательности элементарных бинарных сигналов и передачу по каналу связи, отличающийся тем, что на передающей стороне дискретную информацию считывают в размере стандартного блока, численными методами рассчитывают коэффициенты ряда Фурье, полученные гармоники поочередно отбрасывают, начиная с конца до тех пор, пока погрешность восстановления будет в пределах 0,5, добиваясь минимального состава ряда Фурье, полученные коэффициенты разбивают на байты по правилам компьютерной адресации, преобразуют в последовательный код и передают в канал связи; на принимающей стороне элементарные бинарные сигналы считывают из канала связи, демодулируют, преобразуют в параллельный код побайтно, вводят в персо-

2

нальный компьютер, где по правилам компьютерной адресации из них формируют коэффициенты ряда Фурье длиной в стандартное машинное слово, рассчитывают значения функции для аргумента, равного $1,2,\dots,n$, где n – длина стандартного блока информации, полученные значения округляют до ближайшего целого числа.

2. Устройство для передачи и приема дискретной информации с защитой, содержащее канал передачи информации и модем, отличающееся тем, что в него введены программируемый контроллер прерываний, последовательный порт и персональный компьютер, включающий в себя центральный процессор, оперативное запоминающее устройство, арифметический сопроцессор, постоянное запоминающее устройство, монитор, клавиатуру, печатающее устройство, системный канал и носитель информации, причем модем, связанный с каналом передачи информации, по двуправленной шине связан с информационным каналом последовательного порта, выходы запросов прерывания которого подключены ко входам программируемого контроллера прерываний, а посредством системного канала центральный процессор связан с арифметическим сопроцессором, постоянным и оперативным запоминающим устройствами, монитором, клавиатурой, печатающим устройством и носителем информации.

(19) UA (11) 23491 (13) A

Изобретение относится к технике передачи информации и может применяться в сетях и системах обмена информацией.

Известен способ перекодирования m -разрядных кодовых слов и устройство для его осуществления [Авт.св. СССР № 1605935, кл. Н 03 М 7/00]. Способ заключается во вводе m -разрядного кода, продвижении его по m -разрядному регистру с изменением уровней элементарных сигналов по несовпадающим битам входного и выходного слова и выводе m -разрядных бинарных сигналов.

Известен также способ передачи и приема двоичных сигналов и устройство для его осуществления [Авт.св. СССР № 1164892, кл. Н 03 М 13/00]. Способ заключается в том, что при передаче перед каждым импульсом преобразованной последовательности формируют дополнительный импульс, полярность которого устанавливают в соответствии с корреляционным преобразованием полярности импульсов исходной двоичной последовательности, а на приеме перед сравнением каждого сигнала, полученного после стробирования с заданным порогом, определяют его полярность и формируют сигнал, соответствующий полярности данного сигнала, полученного после стробирования и сигнал предсказания полярности последующего сигнала, полученного после стробирования в последующий отсчетный момент времени в соответствии с корреляционным преобразованием, осуществляемым на передаче, который сравнивают с сигналом, соответствующим полярности последующего сигнала, полученного после стробирования, и при их несоответствии увеличивают заданный порог.

Указанные способы обладают тем недостатком, что при перекодировании преобразование осуществляется по битам или словам, то есть избыточность сообщения, присутствующая с самого начала не уменьшается. Кроме того, они не позволяют защищать информацию.

Наиболее близким по технической сущности является способ кодирования и передачи информации [Авт.св. СССР № 1432788, кл. Н 03 М 13/12]. Способ включает в себя кодирование информационной последовательности элементарных бинарных сигналов с помощью частотной манипуляции с непрерывной фазой и последующую передачу модулированного сигнала по каналу связи. Благодаря чередованию каждых n ($n \geq 1$) кодированных сверточным кодом элементарных бинарных сигналов информационной последовательности с некодированным

элементарным бинарным сигналом этой последовательности, после чего осуществляют частотную модуляцию с непрерывной фазой, обеспечивается повышение скорости передачи. При этом кодовое расстояние остается неизменным.

Каждый ансамбль из возможных комбинаций бит разделяется на две группы, которые кодируются как независимые группы сигналов. В каждую группу помещаются сигналы, для которых первые элементарные сигналы совпадают. Для кодирования сигналов в каждой группе нет необходимости кодировать общий элементарный сигнал. Кодирование осуществляется сверточным кодом со скоростью $1/2$ и, так как кодируется только часть информационных сигналов, скорость передачи повышается.

Вместе с тем общее время передачи информации складывается из двух составляющих:

$$T_o = T_k + T_n, \quad (1)$$

где T_o – общее время передачи информации;
 T_k – время кодирования информации;
 T_n – время прохождения информации по каналу связи.

Учитывая достаточно высокое быстродействие электронной аппаратуры, можно сделать вывод, что время, затрачиваемое на кодирование информации будет значительно меньше, чем прохождение информации по каналу связи. Так, сообщение длиной 1024 байта при скорости передачи 1200 бит/с составит:

$$T_n = 1024 \cdot 8 / 1200 = 6,82 \text{ (с)}.$$

Перекодирование даже всех бит в программном режиме на персональном компьютере IBM-PC с тактовой частотой 20 МГц составляет (время перекодирования 1 бита – 20 тактов):

$$T_k = 1024 \cdot 8 \cdot 20 \cdot 5 \cdot 10^{-8} = 8,192 \cdot 10^{-3} \text{ (с)}.$$

Программная реализация кодирования занимает больше времени, чем аппаратная, поэтому для устройства, выбранного в качестве прототипа, разница будет еще больше.

Недостатками прототипа являются высокая сложность аппаратуры и низкое быстродействие, а также высокая информационная избыточность. Кроме этого способ не обеспечивает защиты передаваемой информации от несанкционированного прочтения, в случае, если она является конфиденциальной.

Таким образом существенный эффект может дать сокращение времени передачи, которое возможно только при условии сокращения времени передачи количества передаваемых байт без потери информации, а также видоизменение передаваемой информации.

В основу изобретения поставлена задача создания способа кодирования и передачи информации, в котором за счет введения новых операций обеспечивается минимизация передаваемой информации, снижается время, затрачиваемое на передачу информации, и повышается эффективность использования канала.

Указанная цель достигается тем, что на передающей стороне дискретная информация считывается с носителя в виде стандартного блока, длина которого устанавливается в диалоговом режиме, численными методами рассчитываются параметры ряда Фурье, аппроксимирующего данную последовательность дискретных значений (байт) таким образом, чтобы погрешность восстановления чисел была не больше 0,5. После этого полученные коэффициенты разбивают на байты по методу компьютерной адресации, преобразуют в последовательный код, модулируют и передают в линию связи побайтно. На принимающей стороне элементарные бинарные сигналы считывают из канала связи, демодулируют, преобразуют в параллельный код побайтно, вводят в персональный компьютер, где по правилам компьютерной адресации из них формируют коэффициенты ряда Фурье длиной в стандартное машинное слово, рассчитывают значения аппроксимирующей функции для аргумента, равного $1, 2, \dots, n$, где n – размер стандартного блока информации, и полученные значения округляют до ближайшего целого числа.

Файл передаваемой информации можно рассматривать как таблично заданную функцию, в которой X_i – номер байта в файле ($i = 1, 2, \dots, n$), Y_i – значение байта (00h – FFh). Поскольку можно считать, что на участке $1 - n$ функция разрывов не имеет, то ее можно разложить в ряд Фурье, то есть получить ряд гармонических составляющих:

$$y(i) = \frac{a_0}{2} + \sum_{k=1}^{\infty} (a_k \cos 2\pi k f i + b_k \sin 2\pi k f i), \quad (2)$$

где f – частота первой гармоники;

k – номер гармоники.

Коэффициенты a_k и b_k для периодической функции $y(i)$, заданной на отрезке $[1, n]$

дискретными отсчетами сводится к нахождению коэффициентов:

$$a_k = \int_0^n y(t) \cos(2\pi k f t) dt, \quad (3)$$

$$b_k = \int_0^n y(t) \sin(2\pi k f t) dt. \quad (4)$$

Исходя из формул численного интегрирования для метода прямоугольников, можно получить:

$$a_k = \frac{2}{N} \sum_{i=0}^{N-1} y_i \cos(2\pi k f i), \quad (5)$$

$$b_k = \frac{2}{N} \sum_{i=0}^{N-1} y_i \sin(2\pi k f i). \quad (6)$$

Поскольку передаваемая информация представлена в дискретном виде (значение байта может принимать значения $0, 1, 2, \dots, 255$), то фактически погрешность восстановления сводится к погрешности округления и составляет 0,5. Таким образом, расчет коэффициентов ряда продолжается до тех пор, пока разность между каждым из действительных и рассчитанных по аппроксимирующему ряду значений не будет меньше 0,5.

Поскольку в линию связи передается не сама информация, а коэффициенты аппроксимирующей функции, без знания вида и всех параметров которой восстановить информацию нельзя, то выполняется и функция защиты конфиденциальной информации.

Описанный способ включает следующие действия:

на передающей стороне:

- чтение массива дискретной информации в размере стандартного блока;

- расчет коэффициентов ряда Фурье численными методами с погрешностью восстановления по каждому значению не более 0,5;

- разбиение полученных коэффициентов на байты по правилам компьютерной адресации;

- передача по каналу связи размера блока и коэффициентов ряда Фурье;

на приемной стороне:

- прием из линии связи размера блока;

- прием байтов из линии связи и формирование из них коэффициентов ряда Фурье по правилам компьютерной адресации;

- расчет значений функции (2) для значений $x = 1, 2, 3, \dots, n$, где n – размер блока передаваемой информации;

– округление рассчитанных значений $y_1, y_2, y_3, \dots, y_n$ до ближайшего целого числа.

Известно устройство для осуществления способа перекодирования m -разрядных кодовых слов, состоящее из m -разрядного регистра сдвига, двоичных элементов связи и датчиков сигнала управления [Авт.св. СССР № 1605935, кл. Н 03 М 7/00].

Известно также устройство для приема дискретных сигналов с корреляционным кодированием по уровню [Авт.св. СССР № 1164892, кл. Н 03 М 13/00], включающее в себя кодирующий блок и формирователь сигнала на передающей стороне, а также формирователь входного сигнала, решающий блок, регистр сдвига, блок предсказания знака, блок сравнения, элемент совпадения и инвертор.

Указанные устройства обладают тем недостатком, что при перекодировании преобразование осуществляется по битам или словам, то есть избыточность сообщения, присутствующая с самого начала, не уменьшается. Кроме того передаваемая информация не является защищенной.

Наиболее близким по технической сущности является устройство, реализующее способ кодирования и передачи информации [Авт.св. СССР № 1432788, кл. Н 03 М 13/12], включающее в себя коммутаторы, блок сверточного кодирования, блок модуляции и канал связи, причем первый вход первого коммутатора подключен к первому входу второго коммутатора, второй вход первого коммутатора подключен ко входу блока сверточного кодирования, выходы которого являются соответственно вторым и третьим входами второго коммутатора, вход блока модуляции, именуемого в дальнейшем "модем", соединен с выходом второго коммутатора, а выход – с каналом связи.

Недостатком данного устройства является большая информационная избыточность и, как следствие этого, малая скорость передачи информации. Поскольку скорости коммутаторов находятся в соотношении 2/3 и кодовая последовательность на выходе коммутатора 3 содержит как кодированные, так и некодированные символы, то общее количество символов, поступающих в линию связи, значительно повышается (при этом количество информации, содержащееся в сообщении, остается неизменным. Кроме этого за счет кодирования информации, скорость передачи снижается на 1/3. Кроме того, если передаваемая информация является конфиденциальной, то она незащищена от считывания в процессе передачи.

В основу изобретения поставлена задача усовершенствования устройства кодиро-

вания и передачи информации, в котором за счет введения новых блоков и связей уменьшается избыточность передаваемой информации и повышается скорость передачи. Это происходит за счет разделения во времени процессов кодирования и передачи информации, а также изменения принципа кодирования информации. С этой целью в состав устройства вводятся персональный компьютер и последовательный интерфейс с соответствующими связями. За счет объединения модулятора и демодулятора в единый блок (модем) и использования одних и тех же технических средств как для приема так и для передачи информации (то есть реализация двунаправленного режима передачи – полной дуплексной связи), осуществляется расширение функциональных возможностей. Кроме того, информация видоизменяется, то есть отличается от первоначального вида и, в случае ее конфиденциальности и несанкционированного считывания с линии связи не может быть восстановлена без знания алгоритма получения истинных значений.

Поставленная задача достигается тем, что в устройство, содержащее канал связи, модулятор и демодулятор, объединенные под названием "модем", дополнительно введены программируемый контроллер прерываний, последовательный порт и персональный компьютер, включающий в себя центральный процессор, арифметический сопроцессор, оперативное и постоянное запоминающие устройства, монитор, системный канал, клавиатуру, печатающее устройство и носитель информации, причем модем, подключенный к каналу передачи информации по двунаправленной шине, стыкуется с информационным каналом последовательного порта, первый (Зпр0) и второй (Зпр1) выходы формирования запросов прерывания которого соединены соответственно с первым (Вх0) и вторым (Вх1) входами программируемого контроллера прерываний, посредством системного канала центральный процессор связан с блоками, входящими в состав персонального компьютера, программируемым контроллером прерываний и последовательным портом.

На фиг.1 представлена схема, реализующая способ кодирования и передачи информации; на фиг.2 – схема программного обеспечения для режима передачи информации; на фиг.3 – схема программного обеспечения для режима приема информации.

Устройство для кодирования и приема-передачи дискретной информации с защитой содержит канал передачи информации

1, связанный с модемом 2, программируемый контроллер прерываний 3, первый ($Vx0$) и второй ($Vx1$) входы которого соединены соответственно с первым ($3пр0$) и вторым ($3пр1$) выходами формирования запросов прерываний последовательного порта 4, двунаправленный информационный канал которого соединен с двунаправленным каналом модема 2, персональный компьютер 5, в состав которого входят клавиатура 6, печатающее устройство 8, носитель информации 8, системный канал 9, арифметический сопроцессор 10, постоянное запоминающее устройство 11, монитор 12, центральный процессор 13 и оперативное запоминающее устройство 14, причем посредством системного канала центральный процессор 13 связан с блоками, входящими в состав персонального компьютера 5, а также с программируемым контроллером прерываний 3 и последовательным портом 4.

Способ заключается в следующем.

На передающей стороне дискретную информацию считывают в размере стандартного блока, численными методами рассчитывают коэффициенты ряда Фурье, полученные гармоники поочередно отбрасывают, начиная с конца до тех пор, пока погрешность восстановления будет в пределах 0,5, добиваясь минимального состава ряда Фурье, полученные коэффициенты разбивают на байты по правилам компьютерной адресации, преобразуют в последовательный код и передают в канал связи; на принимающей стороне элементарные бинарные сигналы считывают из канала связи, демодулируют, преобразуют в параллельный код побайтно, вводят в персональный компьютер, где по правилам компьютерной адресации из них формируют коэффициенты ряда Фурье длиной в стандартное машинное слово, рассчитывают значения функции для аргумента, равного $1, 2, \dots, n$, где n — длина стандартного блока информации, полученные значения округляют до ближайшего целого числа.

Устройство работает следующим образом.

При включении питания центральный процессор 13 выводит на монитор 12 сообщение о первоначальном размере стандартного блока информации и ожидает подтверждения, введенного с клавиатуры 6 персонального компьютера 5. После этого центральный процессор 13 осуществляет чтение данных с носителя информации 8 в размере стандартного блока данных в оперативное запоминающее устройство 14. После этого совместно с арифметическим

сoproцессором 10 центральный процессор определяет максимальную длину ряда Фурье в соответствии с формулой:

$$k = n/2L - 2, \quad (7)$$

где L — длина одного коэффициента (Байт).

После этого центральный процессор 13 вместе с арифметическим сопроцессором 10 осуществляет расчет коэффициентов a_k и b_k по формулам (5) и (6), где k принимает значения от нуля до максимального, вычисленного по формуле (7).

Исходя из формулы (2), рассчитываются значения y_{pi} , которые сравниваются с соответствующими значениями y_i , подлежащими передаче. Если по каждому из значений абсолютная погрешность не превышает 0,5, то последняя гармоническая составляющая (коэффициенты a_k и b_k) отбрасывается, после чего снова рассчитываются значения y_{pi} и сравниваются со значениями y_i . Процесс продолжается до тех пор, пока при $(y - j - 1)$ значении погрешности хотя бы по одному значению не превысит 0,5. После этого восстанавливаются коэффициенты a_{k-j} и b_{k-j} (последняя отброшенная гармоника). Это позволит сформировать минимальный ряд Фурье, позволяющий восстанавливать значения функции без искажений.

Если с самого начала погрешность превышает 0,5, то размер блока уменьшается и процесс повторяется снова.

Рассчитанные значения коэффициентов ряда представляют собой переменные типа "float" и занимают 4 байта в памяти компьютера [Удиит М. и др. Язык Си. — М.: Мир, 1988. — С. 40–67]. Таким образом, данный тип переменной представляет собой естественно дискретизованную величину и легко разделяется на байты.

Следующим этапом является инициализация последовательного порта 4 и программируемого контроллера прерываний 3.

Передача размера блока и коэффициентов ряда осуществляется побайтно в режиме прерываний. Центральный процессор 13 пересылает байт информации в последовательный порт 4, который преобразует его в последовательный код и по битам передает в модем 2. Окончание этой операции характеризуется установлением флага (сигнала) на выходе $3пр0$, последовательного порта. Поступая на вход $Vx0$ программируемого контроллера прерываний 3, этот сигнал вызывает запрос прерывания по вектору 0. Следуя этому сигналу, центральный процессор 13 приостанавливает выполнение основной программы и приступает к выполнению подпрограммы обработки пре-

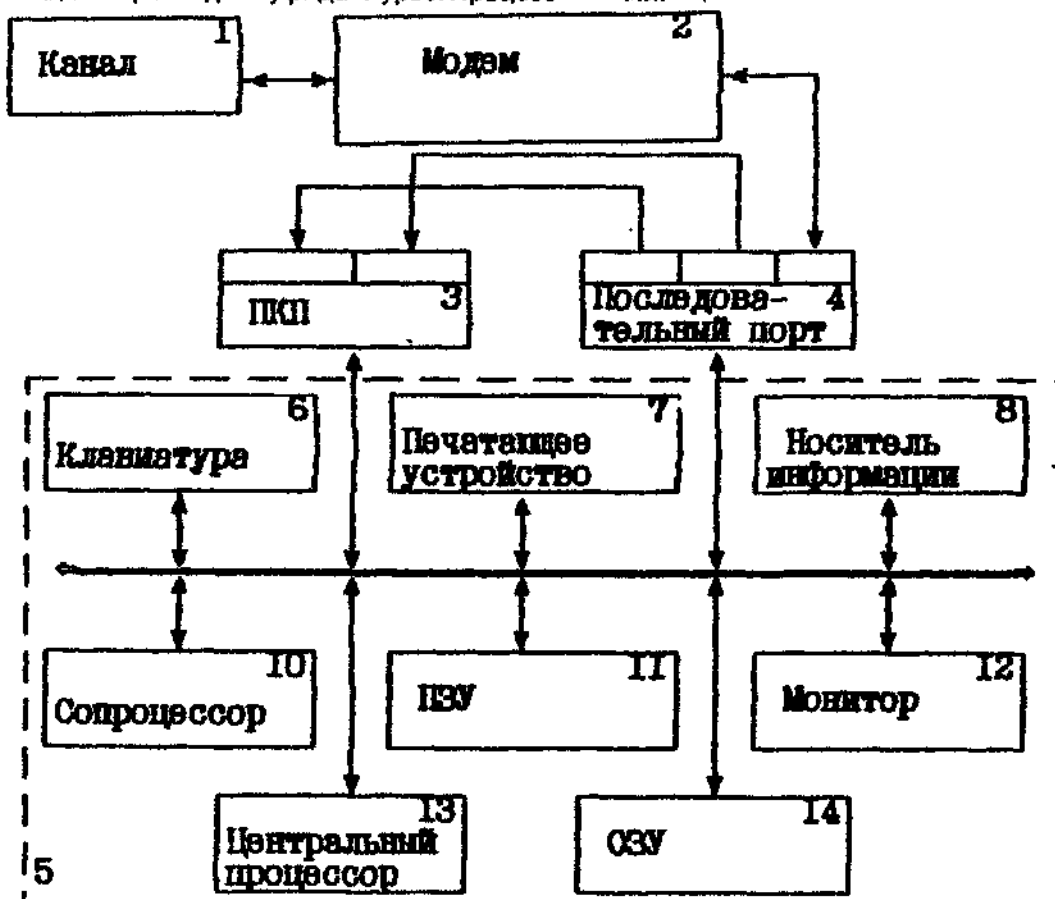
ывания. Она заключается в проверке количества переданных байт и блоков. Если переданы все байты очередного коэффициента, то указатель устанавливается на следующий коэффициент. Если все коэффициенты переданы, то процессор возвращается к выполнению основной программы и приступает к обработке следующего блока информации по описанному алгоритму. Процесс продолжается до тех пор, пока вся информация, содержащаяся на носителе 8, не будет обработана и переслана в линию связи.

В режиме приема информации последовательный код, поступивший из канала 1 через модем 2 в последовательный порт 4, преобразуется в параллельный код. Одновременно с этим на выходе 3пр1 последовательного интерфейса 4 устанавливается флаг (сигнал), поступающий на вход Вх1 программируемого контроллера прерываний 3 и вызывающий прерывание работы центрального процессора 13 по вектору 1. Следуя этому сигналу, центральный процессор 13 считывает байт информации из порта 4 и размещает его в соответствующем месте оперативного запоминающего устройства 14. Место определяется согласно порядкового номера байта в передаваемом коэффициенте, с учетом того, что первый принятый байт характеризует длину передаваемого блока, а второй – длину ряда Фурье. Процесс

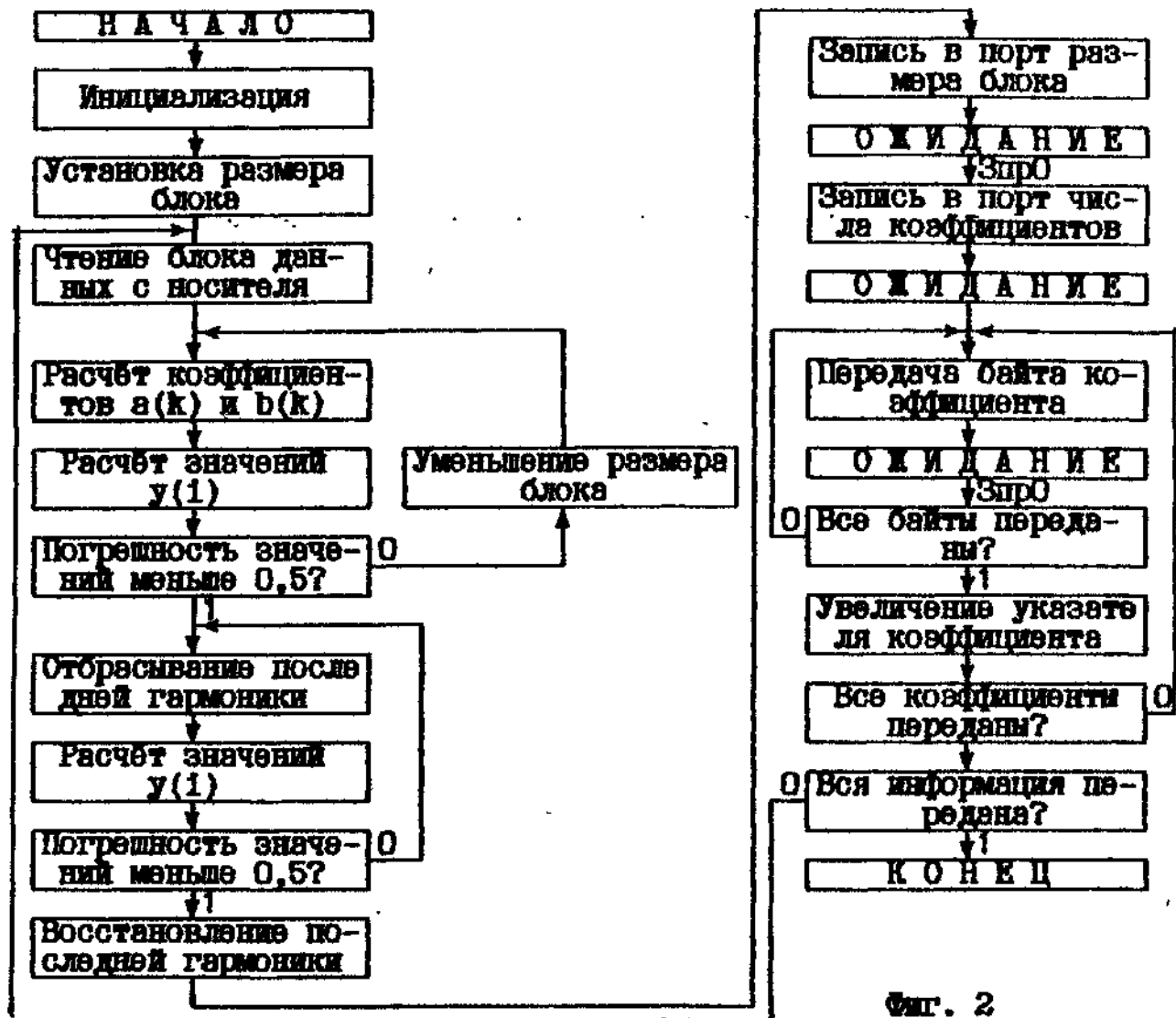
продолжается до тех пор, пока все коэффициенты ряда в побайтном режиме не будут приняты и размещены в соответствующих местах оперативного запоминающего устройства 14. После этого центральный процессор 13 совместно с арифметическим сопроцессором 10 осуществляет расчет значений функции $y(i)$ согласно формулы (2) в соответствии с полученными коэффициентами $a_0, a_1, \dots, a_{k-1}, b_0, b_1, \dots, b_{k-1}$, подставляя последовательно значения $i=1, i=2, \dots, i=n$, где n – длина передаваемого блока. Рассчитанные значения округляются до ближайшего целого числа и записываются на носитель информации 8. Одновременно с этим они могут быть выведены на монитор 12 или печатающее устройство 7.

Поскольку в линию связи передается не сама информация, а коэффициенты аппроксимирующей функции, без знания вида и всех параметров которой восстановить информацию нельзя, то выполняется и функция защиты конфиденциальной информации.

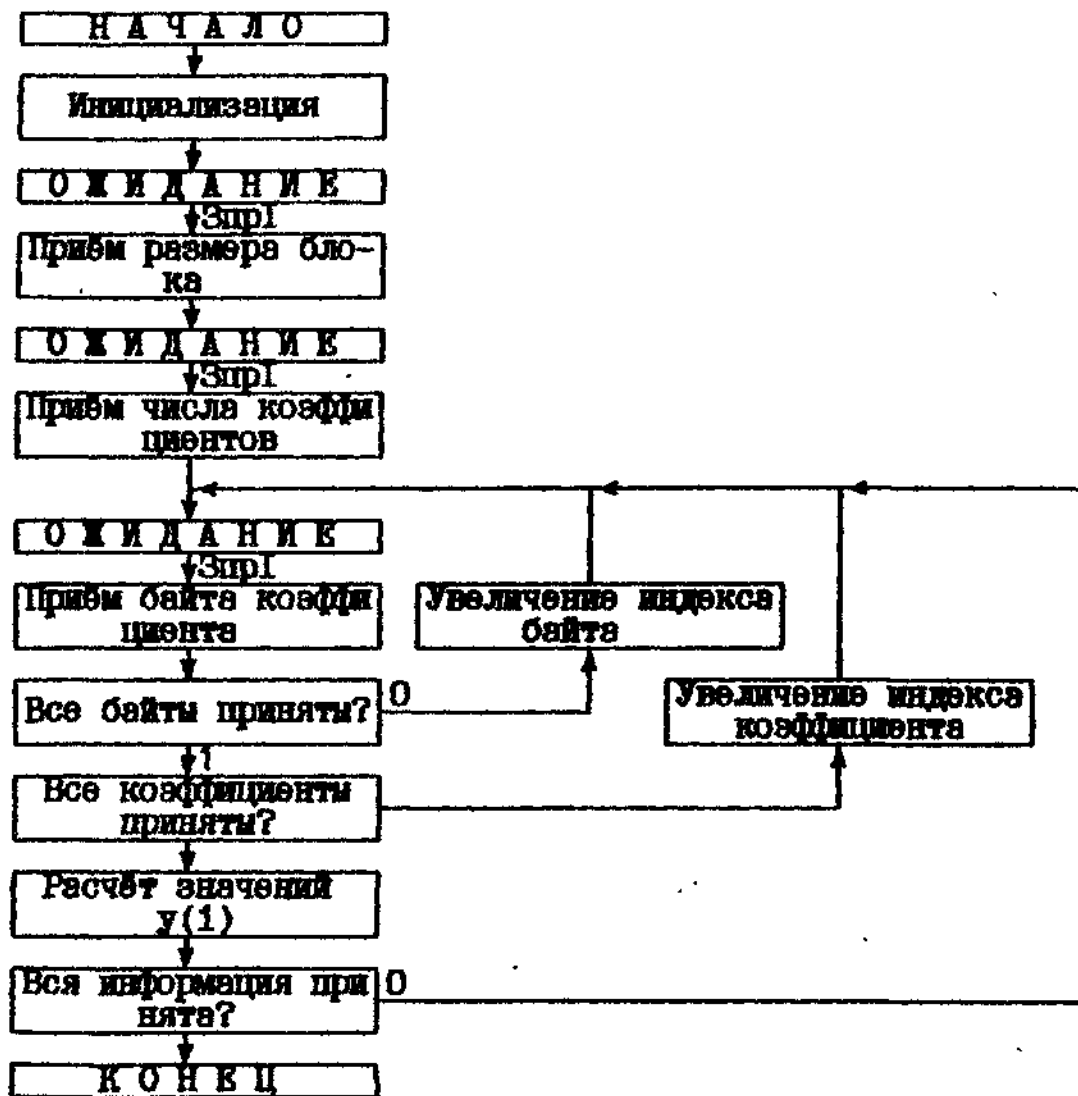
Предлагаемое способ и устройство для его осуществления целесообразно реализовать на базе персонального компьютера IBM-PC, модемы также выпускаются серийно, а программируемый контроллер прерываний и последовательный порт реализованы интегральными микросхемами.



CH. I



Фиг. 2



Фиг. 3

Упорядник

Техред М.Келемеш

Коректор О.Обручар

Замовлення 4543

Тираж

Підписне

Державне патентне відомство України,
254655, ГСП, Київ-53, Львівська пл., 8

Відкрите акціонерне товариство "Патент", м. Ужгород, вул.Гагаріна, 101