Министерство образования Республики Беларусь
Учреждение образования
«Белорусский государственный университет
информатики и радиоэлектроники»

Кафедра сетей и устройств телекоммуникаций

ВРЕМЕННЫЕ ПЕРЕСТАНОВКИ ДЛЯ ЗАЩИТЫ РЕЧЕВЫХ СООБЩЕНИЙ

Пособие к лабораторной работе по курсу
«Цифровая обработка речи и изображений»
для студентов специальности 1-45 01 03 «Сети телекоммуникаций»
дневной формы обучения

Минск 2006

УДК 621.391.25 (075.8)
ББК 32.811.4 я 73
В 81

Авторы-составители:
А.А. Борискевич, А.Ю. Лагойко

Временные перестановки для защиты речевых сообщений: Пособие
В 81 к лаб. работе по курсу «Цифровая обработка речи и изображений» для студ. спец. 1-45 01 03 «Сети телекоммуникаций» дневн. формы обуч. / Сост. А.А. Борискевич, А.Ю. Лагойко – Мн.: БГУИР, 2006. – 32 с.: ил.
ISBN 985-488-004-4

В пособии рассмотрены основные методы защиты речевых сообщений, передаваемых по каналам связи, на основе скремблирования во временной области и критерии оценки эффективности алгоритмов скремблирования. Сведения, представленные в настоящем издании, могут быть использованы для решения задач обработки и защиты речевых сообщений, передаваемых по каналам связи.

УДК 621.391.25 (075.8)
ББК 32.811.4 я 73

ISBN 985-488-004-4

ЦЕЛЬ РАБОТЫ

Изучение особенностей защиты речевых сигналов в телефонных каналах связи на основе алгоритмов блочного скремблирования речевых сообщений во временной области.

1. ТЕОРЕТИЧЕСКАЯ ЧАСТЬ

1.1. Введение

Способов защиты речевой информации и технических средств, реализующих эти способы, существует достаточно много, и они постоянно совершенствуются. В настоящее время активно развиваются два направления защиты речевых сообщений, передаваемых по телефонным каналам. Одно из них связано с физической защитой телефонных линий, другое направление защиты телефонной голосовой связи основано на преобразовании речевых сигналов.

Наиболее эффективным направлением защиты речевой информации, передаваемой по телефонным каналам связи, является направление, основанное на преобразовании речевых сигналов. При этом преобразование должно быть таким, что восстановление исходного сообщения санкционированным абонентом осуществлялось бы очень просто, а восстановление сообщения злоумышленником требовало бы существенных временных и материальных затрат, что делало бы сам процесс восстановления неэффективным. В системах связи известны два основных метода преобразования речевых сигналов, разделяющихся по способу передачи по каналам связи: аналоговое скремблирование и криптографическое шифрование речевого сигнала.

Под скремблированием понимается процесс изменения характеристик речевого сигнала, в результате которого преобразованный сигнал, обладая свойствами неразборчивости и неузнаваемости, занимает такую же полосу частот спектра, как и исходный открытый сигнал. Это позволяет передавать скремблированный сигнал по стандартным телефонным каналам связи. На приемном конце с помощью секретного ключа производится обратное преобразование. При аналоговом скремблировании реализуются, как правило, два основных способа преобразования: временные и частотные перестановки образуют группу одномерных скремблеров, а комбинация этих двух способов образует группу двумерных скремблеров.

Аналоговые одномерные скремблеры, основанные на перестановках во временной области, подразделяются на два вида:

- скремблеры, основанные на перестановках отсчетов речевого сигнала;
- скремблеры, основанные на перестановках сегментов речевого сигнала.

В свою очередь, в зависимости от способа реализации алгоритмов скремблирования данные виды скремблеров подразделяются на:

- блочные скремблеры;
- последовательные скремблеры.

1.2. Алгоритмы скремблирования речевых сигналов во временной области

1.2.1. Алгоритм скремблирования на основе перестановок сегментов речевого сигнала

Целью скремблирования на основе перестановок сегментов является уменьшение или полное устранение разборчивости речевого сигнала посредством изменения исходного порядка следования сегментов речи во времени. Чем больше расстояние в скремблированной последовательности между смежными сегментами, тем ниже ожидаемая разборчивость.

На рис.1 представлен блочный подход к сегментному скремблированию речевых сигналов. Речевой сигнал $x(t)$ разбивается на равные по длительности временные блоки $x_p(t):\{x_p(t)\}_{p=\overline{1,M}}$, где M – число блоков. Каждый временной блок дополнительно делится на N временных сегментов $s_q(t)$ длительностью $T: x_p(t)=\{s_q(t)\}_{q=\overline{1,N}}$. В запоминающем устройстве скремблера, включающем первый исходный блок из N непрерывных сегментов, сегменты “перемешиваются” между собой в соответствие с правилом, определяемым случайным секретным ключом k, и из него поблочно поступают в канал связи. Последующий 2-й блок (рис.1.) поступает в память скремблера после того, как все N сегментов предыдущего 1-го блока (рис.1) будут переставлены и переданы в канал связи. На приемной стороне канала связи осуществляется обратное преобразование скремблированного блока речевых сегментов в исходную последовательность сегментов.

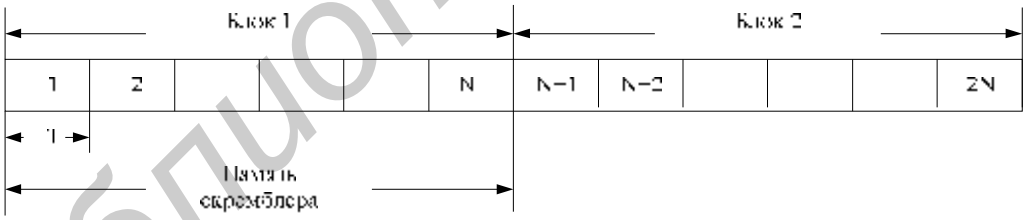

Рис.1. Временные блочные перестановки сегментов

На рис.2 представлен последовательный подход к сегментному скремблированию речевых сигналов. В этом случае на каждой итерации обрабатывается только один сегмент, а не целый блок как в блочном способе. Процесс перестановки ограничивается двумя параметрами: памятью скремблера (или длиной обрабатываемого блока N) и максимальным временем T, в течение которого сегмент может находиться в памяти скремблера. Когда первый q-й сегмент (рис.2), выбранный псевдослучайным образом для передачи, будет переставлен, содержимое памяти скремблера справа от q-го сегмента будет перемещено влево на одну позицию, и последняя позиция будет немедленно занята $(N+1)$-м сегментом, который не входил в состав

предыдущего блока. Процесс обработки происходит по принципу “сегмент за сегментом” с ограничением на максимальное время нахождения каждого сегмента в памяти скремблера. Следовательно, если q-й сегмент находится в памяти скремблера в течение времени, равного суммарной длительности $(N-1)$ сегментов, то он направляется для передачи в течение времени, равного длительности N-го сегмента, что может противоречить алгоритму случайной выборки сегмента и является недостатком данного способа. Исходя из этого, важной характеристикой последовательного скремблера является то, что каждый сегмент имеет равную вероятность нахождения в памяти скремблера в течение максимально возможного времени.

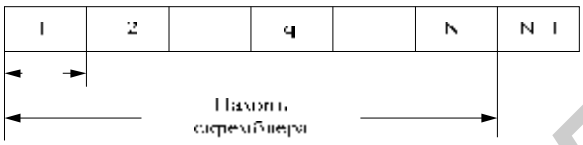

Рис.2. Временные последовательные перестановки сегментов

На рис.3 представлены скремблированные последовательности для блочного (рис.3, б) и последовательного скремблирования (рис.3, в) сегментов речевого сигнала.

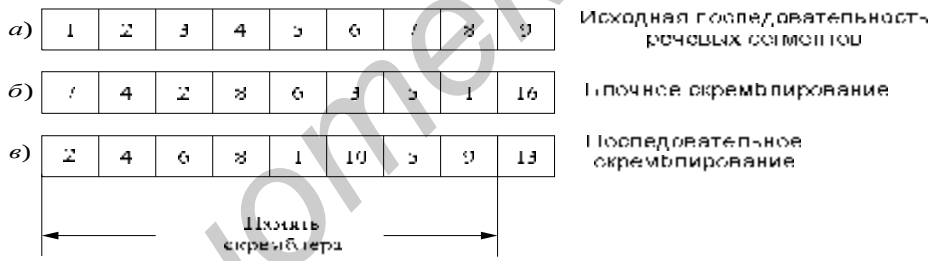

Рис.3. Скремблированные последовательности

Таблица 1 иллюстрирует рассмотренные алгоритмы скремблирования во временной области, где N – содержимое памяти скремблера, $s_q(t)$ – переданный сегмент.

Таблица 1

Результаты блочной и последовательной перестановок

Блочная перестановка									Последовательная перестановка								
N								$s_q(t)$	N								$s_q(t)$
1	2	3	4	5	6	7	8	7	1	2	3	4	5	6	7	8	2
1	2	3	4	5	6	8		4	1	3	4	5	6	7	8	9	8
1	2	3	5	6	8			2	1	3	4	5	6	7	9	10	4
1	3	5	6	8				8	1	3	5	6	7	9	10	11	9
1	3	5	6					6	1	3	5	6	7	10	11	12	5

Продолжение табл. 1

1	3	5						3	1	3	6	7	10	11	12	13	10
1	5							5	1	3	6	7	11	12	13	14	6
1								1	1	3	7	11	12	13	14	15	1
9	10	11	12	13	14	15	16	16	3	7	11	12	13	14	15	16	13
9	10	11	12	13	14	15		12	3	7	11	12	14	15	16	17	3
9	10	11	13	14	15			10	7	11	12	14	15	16	17	18	18
9	11	13	14	15				9	7	11	12	14	15	16	17	19	14
……								…	……								…

К преимуществам рассмотренных способов скремблирования относится их сравнительная простота и возможность передачи зашифрованного телефонного сообщения по стандартным телефонным каналам. Однако данные методы скремблирования позволяют обеспечить лишь невысокую степень защиты речевой информации.

Возможным средством повышения криптостойкости рассмотренных способов скремблирования являются использование смены знаков сегментов совместно с перестановками. Однако в этом случае происходит расширение спектра преобразованного сигнала, что затрудняет передачу зашифрованного телефонного сообщения по стандартным телефонным каналам.

1.2.2. Алгоритм перестановок речевых отсчетов

Общее количество перестановок, возможных на временном кадре из N отсчетов, равно $N!$. Если также учитывать возможность смены знака выборок, то общее количество возможных перестановок составит $2^N \times N!$. На практике используется гораздо меньшее количество перестановок, что связано с избыточностью речевого сигнала. Временные перестановки характеризуются оператором перестановок P, который представляет собой матрицу размерностью $N \times N$, элементами которой являются нули и единицы.

Процесс перестановок временных отсчетов внутри кадра осуществляется путем перемножения вектор-столбца исходных значений отсчетов $\mathbf{r}_x=(x_0,\ldots x_n,\ldots x_{N-1})^T$ и матрицы перестановок P. Если конечную переставленную последовательность отсчетов представить как вектор-столбец $\mathbf{r}_y=(y_0,\ldots y_n,\ldots y_{N-1})^T$, то процесс перестановок отсчетов внутри кадра в матричном виде можно записать в виде:

$$\mathbf{r}_y = P \times \mathbf{r}_x . \qquad (1)$$

Для того чтобы из преобразованной последовательности получить исходную последовательность, необходимо воспользоваться обратной матрицей перестановок. Матрица P^{-1} называется обратной для матрицы P, если выполняются следующие равенства:

$$P^{-1} \times P = P \times P^{-1} = E, \tag{2}$$

где E – единичная матрица вида $\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & 1 \end{bmatrix}$.

Всегда будет существовать только одна обратная матрица. Процесс обратных перестановок временных отсчетов внутри кадра осуществляется путем перемножения вектор-столбца с переставленными отсчетами $\vec{y}=(y_0,...,y_n,...,y_{N-1})^T$ и матрицы обратных перестановок P^{-1}. Тогда процесс обратных перестановок отсчетов в матричном виде можно записать в виде:

$$\vec{x} = P^{-1} \times \vec{y}. \tag{3}$$

Перестановка отсчетов внутри кадра во временной области приводит к изменению частотного спектра сигнала.

Обозначим через $\vec{x} = (x_0,...,x_n,...,x_{N-1})^T$ входной кадр с N отсчетами, в котором должны быть осуществлены перестановки, а $\vec{X} = (X_0,..., X_k,..., X_{N-1})^T$ – вектор-столбец спектральных компонент вектора $\vec{x}$. В этом случае они связаны следующим соотношением:

$$\vec{X} = F \times \vec{x}, \tag{4}$$

где F – матрица дискретного преобразования Фурье:

$$F = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 \\ 1 & W & W^2 & W^3 & W^{N-1} \\ 1 & W^2 & W^4 & W^6 & W^{2(N-1)} \\ \dots & \dots & \dots & \dots & \dots \\ 1 & W^{N-1} & W^{2(N-1)} & \dots & W^{(N-1)^2} \end{bmatrix}. \tag{5}$$

Элементами матрицы ДПФ являются весовые функции W:

$$W = e^{(-j \cdot 2 \cdot p / N)} = \cos(\frac{2 \cdot p}{N}) - j \cdot \sin(\frac{2 \cdot p}{N}). \tag{6}$$

Пусть $\vec{x}_P$ является переставленной последовательностью отсчетов, $\vec{X}_P$ – искретным преобразованием Фурье переставленной последовательности, T – матрицей перестановок выборок дискретного преобразования Фурье, P – матрицей перестановок отсчетов во временной области. Тогда можно записать следующие соотношения:

$$\vec{X}_P = T \times \vec{X} = T \times F \times \vec{x}, \quad (7)$$

$$\vec{X}_P = F \times \vec{x}_P = F \times P \times \vec{x}. \quad (8)$$

Приравнивая (7) и (8) и производя соответствующие преобразования, получаем:

$$T = F \times P \times F^{-1}, \quad (9)$$

$$P = F^{-1} \times T \times F. \quad (10)$$

Обратная матрица дискретного преобразования Фурье F^{-1} имеет следующий вид:

$$F^{-1} = N^{-1} \times \begin{bmatrix} 1 & 1 & 1 & 1 & 1 \\ 1 & W^{-1} & W^{-2} & W^{-3} & W^{1-N} \\ 1 & W^{-2} & W^{-4} & W^{-6} & W^{2(1-N)} \\ \dots & \dots & \dots & \dots & \dots \\ 1 & W^{1-N} & W^{2(1-N)} & \dots & W^{-(N-1)^2} \end{bmatrix}. \quad (11)$$

Выражения (9) и (10) показывают взаимосвязь между матрицами перестановок во временной и частотной области. Следовательно, возможен поиск матрицы среди частотных перестановок, связанной с соответствующей матрицей временных перестановок. Из выражений (9) и (10) следует, что перестановки могут осуществляться в частотной области. В этом случае возможен поиск матрицы среди временных перестановок, связанной с соответствующей матрицей частотных перестановок.

1.2.3. Алгоритм скремблирования на основе псевдослучайных перестановок речевых отсчетов

В технологии шифрования для генерации псевдослучайной ключевой последовательности используются регистры линейного сдвига. Генератор псевдослучайной последовательности (ПСП) может быть реализован на регистре сдвига с использованием контура обратной связи, предназначенного

для вычисления нового элемента (бита) на основе N предыдущих элементах ключевой последовательности.

Псевдослучайное скремблирование временных отсчетов речевого сигнала в пределах блока длины N отсчетов достигается назначением каждому отсчету нового адреса A (A=1, или 2, или 3,…, или N), определяемого состоянием регистра сдвига максимальной длины.

Если период повторения последовательности, генерируемой D каскадным линейным регистром сдвига, равен $p = 2^D - 1$, то это последовательность называется последовательностью максимальной длины. Если период последовательности меньше $(2^D - 1)$, то последовательность не является последовательностью максимальной длины.

Алгоритм преобразования речевого сообщения, основанный на псевдослучайных перестановках и представленный на рис.4, включает два этапа: скремблирование и дескремблирование речевого сигнала.

Этап скремблирования включает следующие операции:

- на передающей стороне речевой сигнал $x(t)$ фильтруется в полосе 0,3–3,4 кГц;

- отфильтрованный сигнал оцифровывается в аналого-цифровом преобразователе (частота дискретизации 8000 Гц, длина кодового слова 8 бит) и разбивается на временные кадры длиной N отсчетов;

- каждый кадр $\mathbf{x} = (x_0,...,x_n,...,x_{N-1})^T$ последовательно подается на блок скремблирования, на который также подается матрица перестановок или криптографическая матрица M размерности $N \times N$ с выхода генератора ПСП;

- в блоке скремблирования осуществляется перестановка временных отсчетов внутри кадра в соответствии с матрицей M;

- преобразованный кадр речевого сигнала посредствам цифро-аналогового преобразователя переводится в аналоговую форму и передается на приемную сторону.

На этапе дескремблирования все операции аналогичны этапу скремблирования речевого сигнала, отличие состоит лишь в направление считывания таблицы перестановок, формируемой с помощью генератора ПСП, и, соответственно, используется матрица обратных перестановок M^{-1}.

Алгоритм генерации ПСП и формирования криптографической матрицы состоит из следующих операций:

- выбирается регистр сдвига разрядностью $D = \log_2(N)$, (предполагается, что длина кадра временных отсчетов N является степенью 2, а элементами регистра являются логические единицы или нули);

- из специальных таблиц выбирается примитивный полином $Q(y)$ степени D, и производится подключение $(D-d)$ ячейки регистра $d = \overline{0, D-1}$ к блоку исключающее ИЛИ (сумматор по *mod2*), если коэффициент при y^d в $Q(y)$

является отличным от нуля. Сумматор по *mod2* расположен в цепи обратной связи;

- выбирается секретный ключ, который будет являться исходным состоянием регистра сдвига, и заносится в регистр сдвига;

- сдвигая поразрядно вправо секретный ключ и учитывая результат суммирования по *mod2* в цепи обратной связи, генерируется таблица перестановок и формируется матрица перестановок.

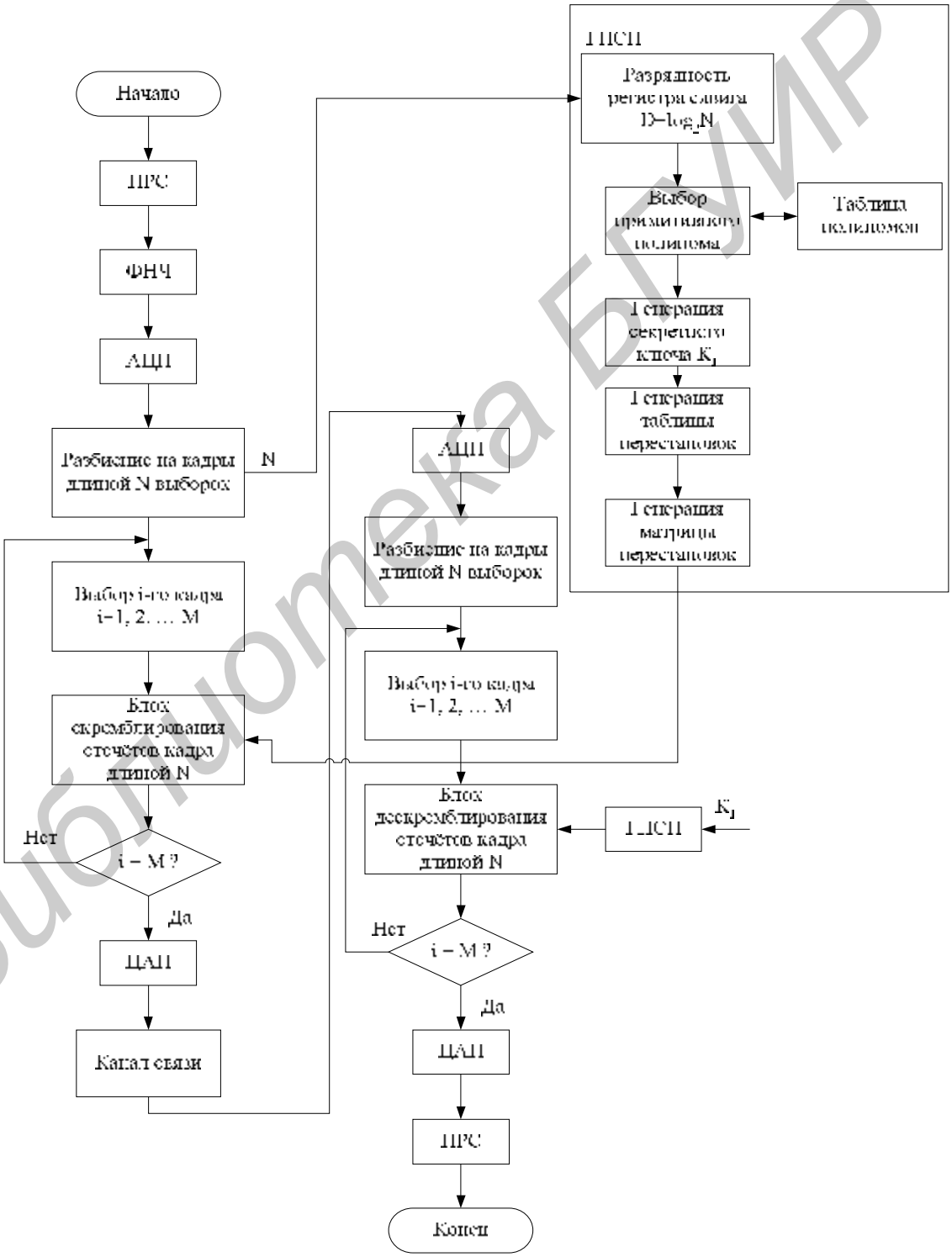

Рис. 4. Блок-схема алгоритма скремблирования и дескремблирования

Неприводимый полином $Q(y)$ порядка m является примитивным, если наименьшим положительным целым числом n, для которого $y^n + 1$ делится на $Q(y)$, будет $n = 2^m - 1$.

Неприводимый полином – это полином, который нельзя представить в виде произведения полиномов меньшего порядка.

Полученная схема регистра сдвига в последовательные интервалы времени генерирует последовательность с $2^D - 1 = 2^{\log_2 N} - 1 = N - 1$ отличными от нуля состояниями, после чего цикл повторяется, начинаясь еще раз с исходного состояния регистра сдвига, которое является секретным ключом и может отличаться от предыдущего исходного состояния. Следовательно, $(N-1)$ состояний регистра сдвига могут использоваться как псевдослучайные номера отсчетов кадра, состоящего из $(N-1)$ входных отсчетов. Если входной блок имеет N, а не $(N-1)$ отсчетов (из-за требования, чтобы N было степенью 2), то псевдослучайный номер N-го отсчета обычно оставляют неизменным.

Рассмотрим процесс формирования таблицы прямых и обратных перестановок на примере. Если количество отсчетов в кадре $N = 32$, а $D = 5$, то один из возможных примитивных полиномов имеет вид $Q_5(y) = y^5 + y^2 + y^0 = y^5 + y^2 + 1$.

Согласно алгоритму схема генератора ПСП может быть представлена в виде (рис. 5):

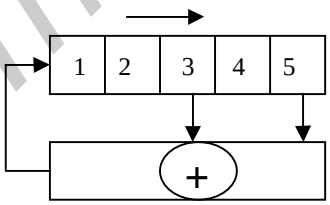

Рис.5. Схема генератора ПСП на 5 разрядном регистре сдвига

Секретный ключ заносится справа налево, так что младший бит секретного ключа будет располагаться в пятой ячейке. Так как разрядность регистра сдвига $D = 5$, то $d = \overline{0, D-1} = \{0,1,2,3,4\}$. В выбранном полиноме присутствуют члены $y^d = \{y^0, y^2\}$, при которых значения коэффициентов отличны от нуля. В этом случае согласно правилу $D - d$ содержимое ячеек регистра сдвига с номерами $D - d = \{3,5\}$ направляется на сумматор по mod2. Первая ячейка всегда используется для организации обратной связи.

Пусть значение секретного ключа равно 00001. Согласно схеме генератора (рис.5) таблица перестановок будет соответствовать таблице 2. Из таблицы перестановок видно, что входным выборкам (1, 2, 3, 4, 5, 6, 7,…31)

присваиваются новые позиции соответственно (1, 16, 8, 4, 18, 9, 20,…31), позиция 32-ой выборки остается неизменной.

Следует отметить, что таблица определяет только новые положения исходных номеров отсчетов, но не определяет порядок следования отсчетов. Для формирования скремблированной последовательности используется криптографическая матрица перестановок, полученная на основе таблицы перестановок.

На рис.5 представлена матрица перестановок, которую еще называют криптографической матрицей. Номера строк в данной матрице соответствуют номерам отсчетов в исходном кадре, а номера столбцов соответствуют номерам новых позиций, которые займут исходные отсчеты. Исходя из представленной матрицы, можно записать, что конечной переставленной последовательностью будет (1, 31, 18, 4, 30,…32).

Таблица 2

Формирование новых номеров отсчетов

Номер отсчета в кадре	Состояние регистра сдвига	Номер отсчета в скремблированном кадре
1	00001	1
2	10000	16
3	01000	8
4	00100	4
5	10010	18
6	01001	9
7	10100	20
…	…	…
31	00010	2

Использование другого секретного ключа (отличного от 00001) приведет к новой последовательности скремблированных отсчетов. Для каждого полинома $Q_5(y)$ будет существовать соответственно $(N-1)$ отличных от нуля секретных ключей. Так как число примитивных полиномов $Q_5(y)$ равно 6, то это приводит к увеличению общего количества возможных перестановок. В таблице 3 приведены примеры примитивных полиномов степени D и их количество.

Рассмотрим процесс дескремблирования на приемной стороне. Генератор ПСП, который используется на приемной стороне, аналогичен генератору ПСП на передающей стороне. Для генерации таблицы обратных перестановок на приемной стороне используется тот же секретный ключ, что и на передающей стороне. Таблица обратных перестановок будет совпадать с таблицей 2.

Правило дескремблирования заключается в том, что при приеме скремблированного кадра считается, что отсчеты в кадре идут по порядку, как и в исходном кадре (1, 2, 3, 4,…), так как порядок перестановки не известен. Тогда прочитав таблицу перестановок не слева направо, как при

скремблировании, а справа налево можно получить однозначное отображение номеров отсчетов в исходном кадре. В этом случае таблицу обратных перестановок можно записать в виде таблицы 4.

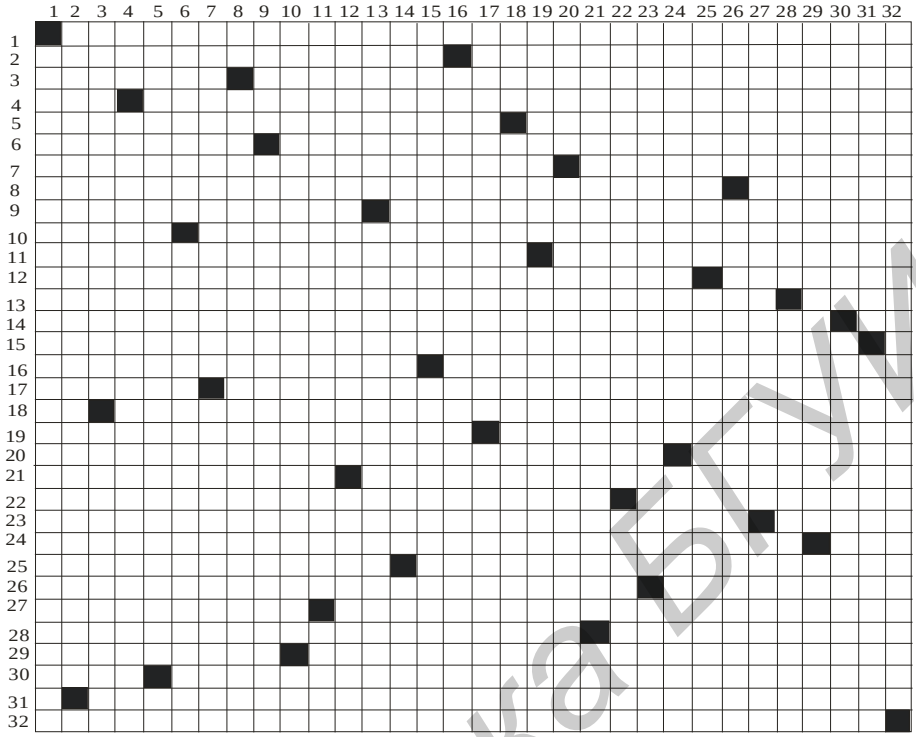

Рис.6. Криптографическая матрица псевдослучайных перестановок *M*

Таблица 3

Список примитивных полиномов для $D = 1\ldots12$

Степень *D*	Примитивные полиномы	Число примитивных полином *L(D)* степени *D*
1	$y+1$	1
2	y^2+y+1	1
3	y^3+y+1	2
4	y^4+y+1	2
5	y^5+y^2+1	6
6	y^6+y+1	6
7	y^7+y+1	18
8	$y^8+y^4+y^3+y^2+1$	16
9	y^9+y^4+1	48
10	$y^{10}+y^3+1$	60
11	$y^{11}+y^2+1$	176
12	$y^{12}+y^6+y^4+y+1$	144

Таблица 4

Таблица обратных перестановок номеров отсчетов

Номер отсчета в скремблированном кадре	Состояние регистра сдвига	Номер отсчета в исходном кадре
1	00001	1
16	10000	2
8	01000	3
4	00100	4
8	10010	5
9	01001	6
20	10100	7
…	…	…
2	00010	31

Из таблицы перестановок видно, что входным скремблированным выборкам (1, 16, 8, 4, 18, 9, 20,…2, 32) присваиваются соответственно исходные позиции (1, 2, 3, 4, 5, 6, 7,…31, 32). Тогда матрица обратных перестановок, в соответствии с которой будет получена исходная последовательность, примет вид, как показано на рис.7.

Номера строк в данной матрице соответствуют номерам отсчетов в скремблированном кадре, а номера столбцов соответствуют номерам исходных позиций отсчетов.

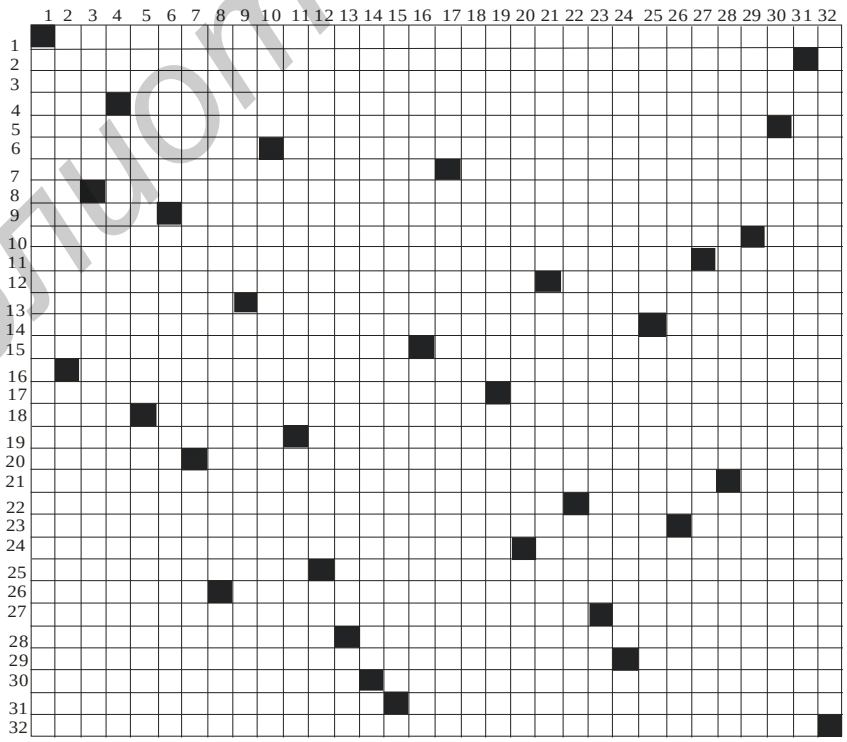

Рис.7. Обратная матрица псевдослучайных перестановок $\boldsymbol{M}^{-1}$

Анализируя матрицы прямых (рис.6) и обратных (рис.7) перестановок, можно заметить, что обратная матрица перестановок M^{-1} является транспонированным вариантом матрицы прямых перестановок M : $M^{-1} = M^T$.

1.2.4. Алгоритм скремблирования на основе однородных перестановок речевых выборок

Однородное скремблирование временных отсчетов речевого сигнала в пределах блока длины N достигается присваиванием каждому отсчету нового адреса A (A = 1, или 2, или 3,…, или N). В основе данного алгоритма лежит использование методов модулярной арифметики.

Процесс скремблирования описывается следующим выражением:

$$s = (k_1 \times r) \bmod N, \tag{12}$$

где k_1 – секретный ключ, который является взаимно простым с N; N – число отсчетов во временном кадре, который скремблируется; r – номер отсчета внутри исходного кадра; s – номер отсчета внутри скремблированного кадра.

Процесс дескремблирования осуществляется согласно соотношению:

$$r = (k_2 \times s) \bmod N, \tag{13}$$

где k_2 – секретный ключ, является обратной величиной k_1.

$$k_2 = k_1^{-1} \bmod N. \tag{14}$$

Алгоритм закрытия речевого сообщения, основанный на однородных перестановках (рис.8), включает два этапа: скремблирование и дескремблирование речевого сигнала.

Этап скремблирования включает следующие операции:

- на передающей стороне речевой сигнал $x(t)$ фильтруется в полосе 0,3–3,4 кГц;
- отфильтрованный сигнал оцифровывается в аналого-цифровом преобразователе (частота дискретизации 8000 Гц, длина кодового слова 8 бит) и разбивается на временные кадры длиной N отсчетов;
- каждый кадр $\mathbf{r}_x = (x_0,...,x_n,...,x_{N-1})^T$ последовательно подается на блок скремблирования, на который также подается матрица перестановок или криптографическая матрица M размерности $N \times N$ с выхода генератора ПСП;
- в блоке скремблирования осуществляется перестановка временных отсчетов внутри кадра в соответствии с матрицей M;
- преобразованный кадр речевого сигнала посредствам цифро-аналогового преобразователя переводится в аналоговую форму и передается на приемную сторону.

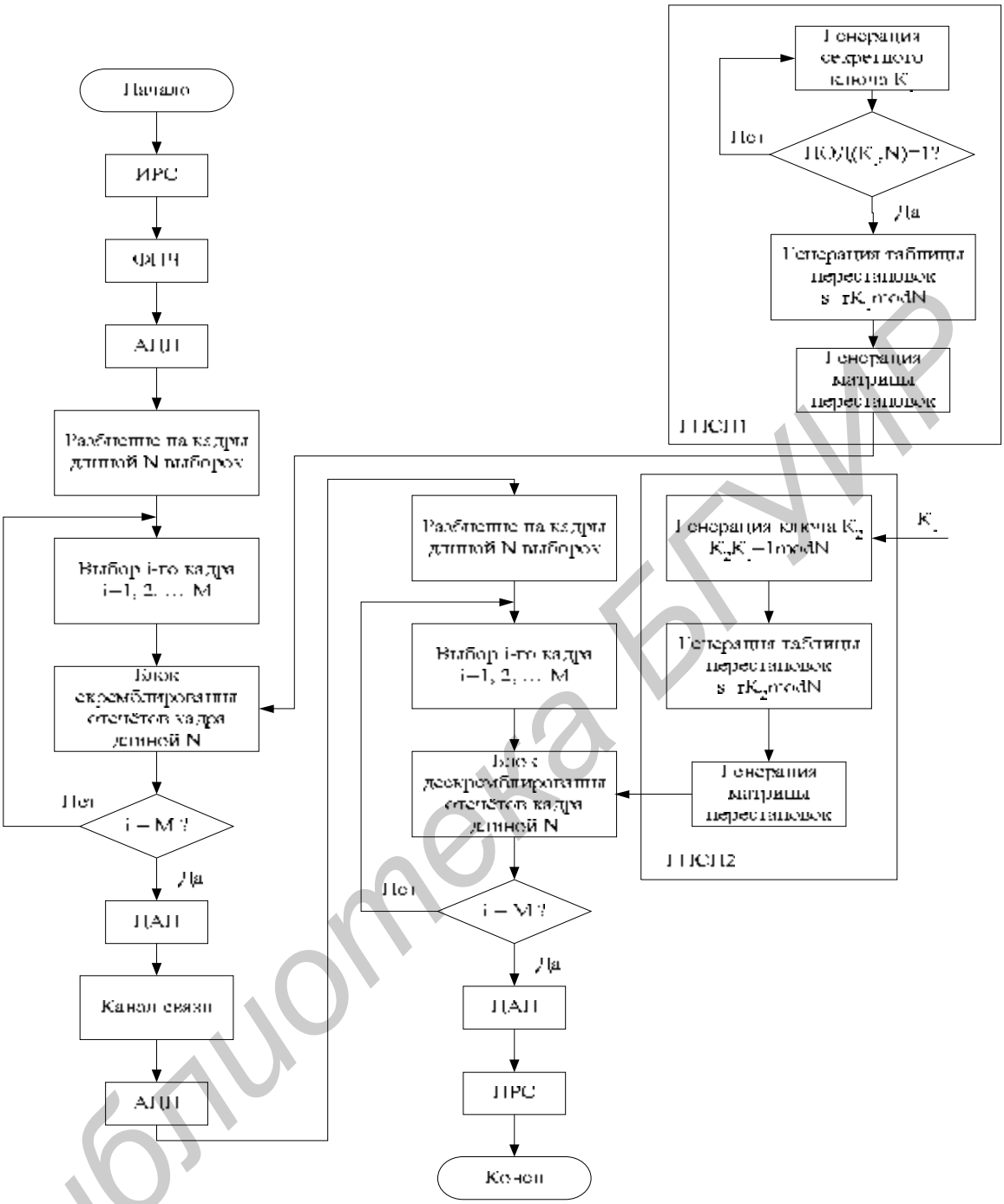

Рис. 8. Блок-схема алгоритма скремблирования и дескремблирования

Алгоритм генерации ПСП и формирования криптографической матрицы на передающей стороне состоит из следующих операций:

- задается случайное число k_1 – секретный ключ;

- проверяется выполнение условия того, что k_1 и N являются взаимно простыми числами. Числа k_1 и N называются взаимно простыми, если наибольший общий делитель этих чисел равен 1: $НОД(k_1, N) = 1$. Для нахождения *НОД* двух чисел используется алгоритм Евклида (рис.9);

- если секретный ключ удовлетворяет необходимому условию, то вычисляется таблица перестановок номеров отсчетов по правилу: $s = (k_1 \times r) \bmod N$, $r = \overline{1, N}$;

- на выходе генератора ПСП в соответствии с таблицей перестановок формируется криптографическая матрица перестановок.

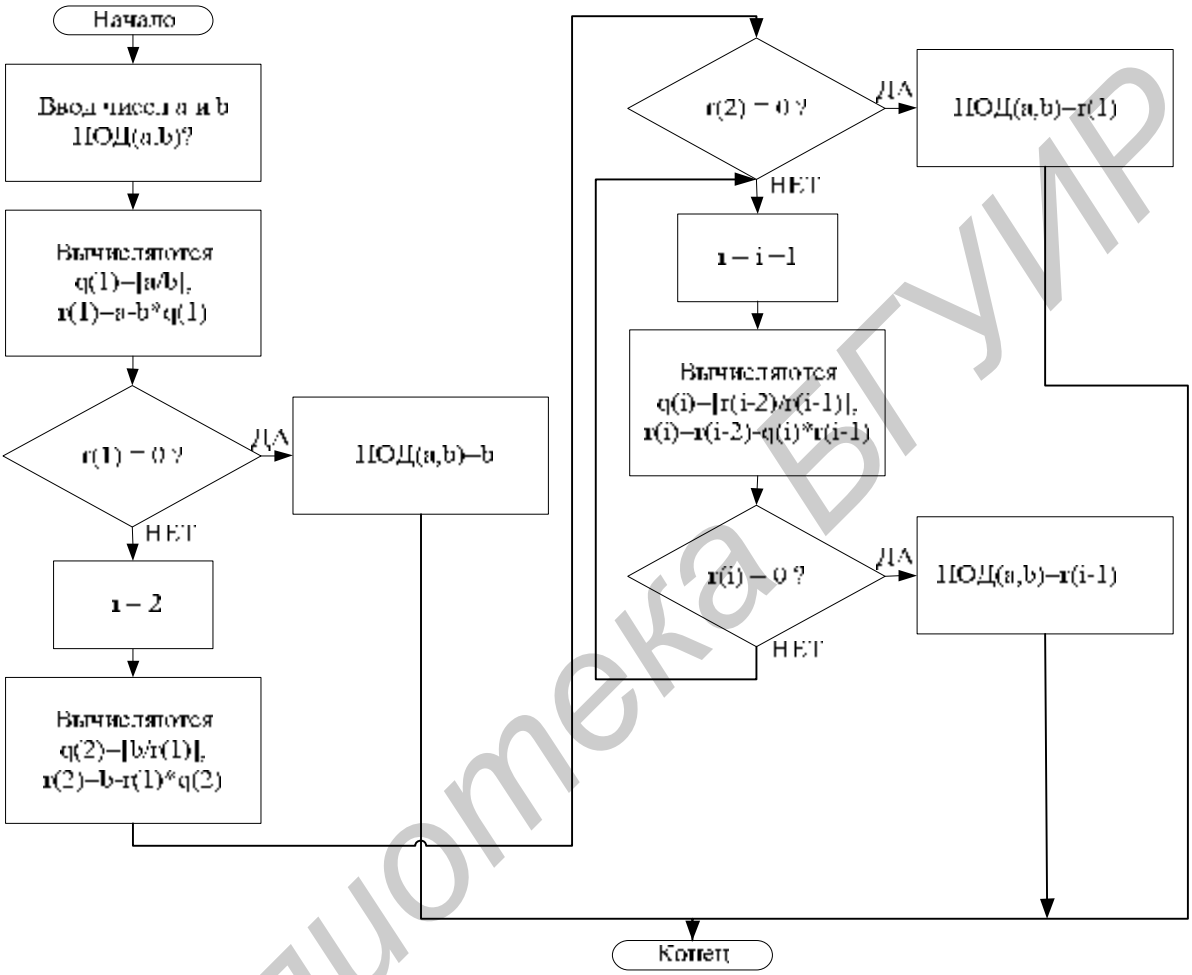

Рис.9. Алгоритм Евклида для нахождения НОД

Этап дескремблирования включает следующие операции:

- скремблированный сигнал оцифровывается в аналого-цифровом преобразователе (частота дискретизации 8000 Гц, длина кодового слова 8 бит) и разбивается на временные кадры длиной N отсчетов;

- каждый кадр последовательно подается на блок дескремблирования, на который также подается матрица обратных перестановок M^{-1} размерности $N \times N$;

- в блоке дескремблирования осуществляется перестановка временных отсчетов внутри кадра в соответствии с матрицей M^{-1};

- преобразованный кадр речевого сигнала посредствам цифро-аналогового преобразователя переводится в аналоговую форму и передается на оконечное устройство абонента.

Алгоритм генерации ПСП и формирования матрицы обратных перестановок на стороне приемника состоит из следующих операций:

- задается секретный ключ k_1, который использовался на передающей стороне;

- вычисляется обратная величина секретного ключа k_1: $k_2 = k_1^{-1} \bmod N$. Величина k_2 называется обратной величиной k_1 по $\bmod N$, если их произведение сравнимо с $1 \bmod N$, т.е. $k_1 \times k_2 = 1 \bmod N$. Не все числа имеют обратные величины. Обратная величина существует, если $НОД(k_1, N) = 1$. Для нахождения обратной величины используется расширенный алгоритм Евклида (рис.10), на каждом шаге которого рассматриваются два вектора;

- генерируется таблица обратных перестановок номеров отсчетов по правилу: $r = (k_2 \times s) \bmod N$, $s = \overline{1, N}$, и формируется матрица обратных перестановок.

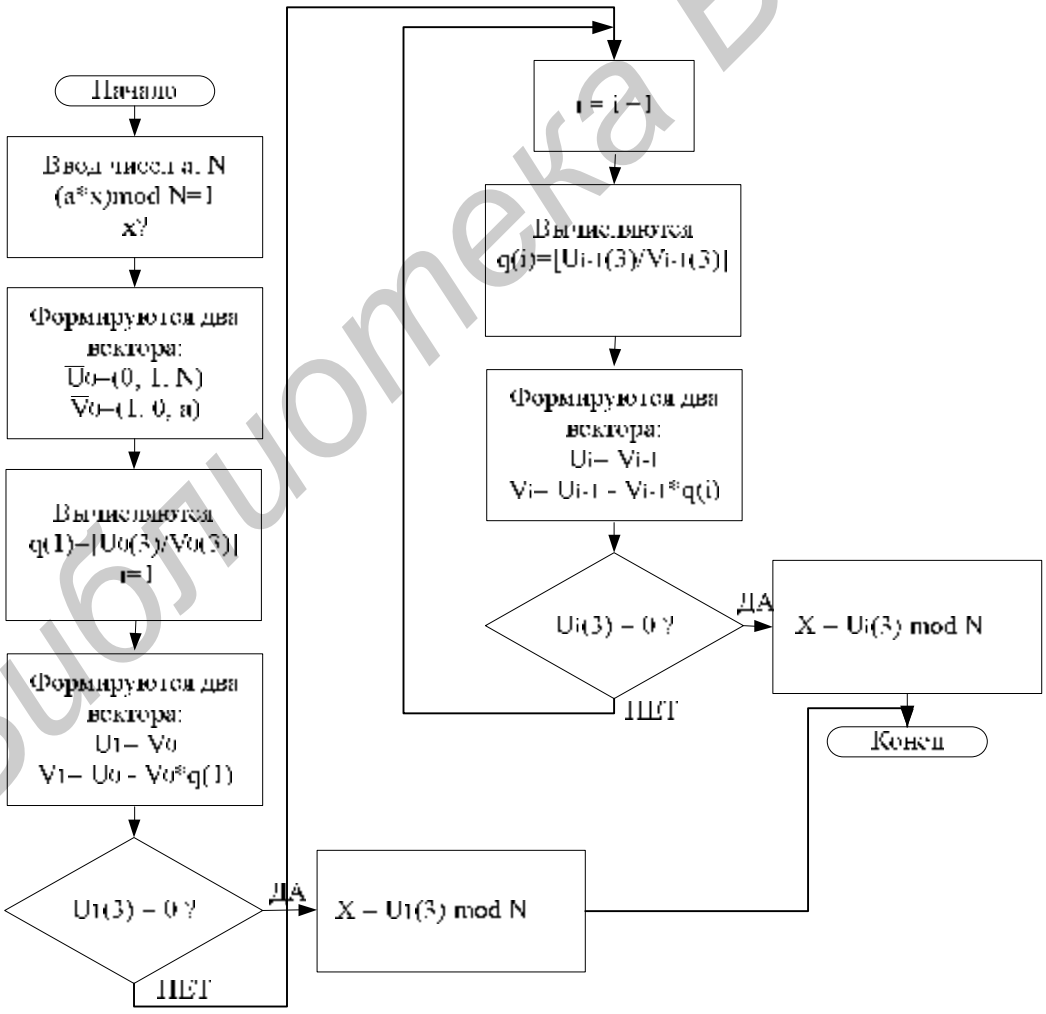

Рис.10. Расширенный алгоритм Евклида

Рассмотрим процесс формирования таблицы прямых и обратных перестановок на примере: значение количества отсчетов в кадре $N = 32$, значения секретного ключа $k_1 = 7$. Данный секретный ключ удовлетворяет всем необходимым требованиям, в чем легко убедиться, вычислив $НОД(32,7) = 1$. Согласно алгоритму построения генератора ПСП и используя выражение (12), получим таблицу прямых перестановок (табл.5).

Из таблицы перестановок видно, что входным выборкам (1, 2, 3, 4, 5, 6, 7, …32) присваиваются новые позиции соответственно (7, 14, 21, 28, 3, 10, 17, …32). Согласно табл. 5 для получения конечной последовательности отсчетов необходимо сформировать матрицу прямых перестановок. Полная матрица прямых перестановок показана на рис.11. Из рис. 11 видно, что единицы расположены в матрице 32×32 однородно.

Таблица 5

Формирование новых номеров отсчетов

Номер отсчета в кадре, r	Номер отсчета в скремблированном кадре, s
1	7
2	14
3	21
4	28
5	3
6	10
7	17
…	…
32	32

Номера строк в данной матрице соответствуют номерам отсчетов в исходном кадре, а номера столбцов соответствуют номерам новых позиций, которые займут исходные отсчеты. В перестановках участвуют $(N-1)$ отсчетов, причем адрес N-го отсчета остается неизменным.

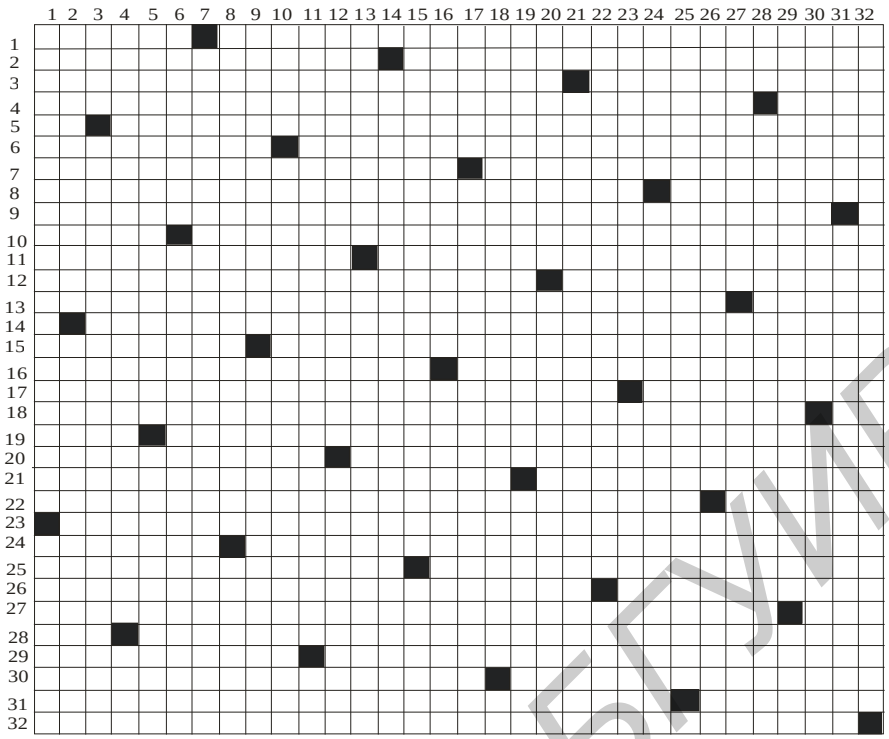

Рис.11. Матрица однородных перестановок

Используя матрицу однородных перестановок (рис.11), переставленную последовательность можно записать в виде (23, 14, 5, 28, 19,…32).

Рассмотрим процесс дескремблирования на приемной стороне. Генератор ПСП на приемной стороне для генерации таблицы обратных перестановок использует секретный ключ k_2, который является обратной величиной секретного ключа k_1. В данном примере значение ключа $k_1 = 7$, тогда согласно выражению (14) значение ключа $k_2 = 23$, $k_1 \times k_2 \bmod N = 1$.

Процесс дескремблирования на приемной стороне будет осуществляться согласно выражению (13), и таблица обратных перестановок для рассматриваемого примера будет соответствовать таблице 6.

Таблица 6

Формирование обратных номеров отсчетов

Номер отсчета в скремблированном кадре, s	Номер отсчета в исходном кадре, r
1	23
2	14
3	5
4	28
5	19
6	10
7	1
…	…
32	32

Матрица обратных перестановок, в соответствии с которой будет получена исходная последовательность, примет вид, показанный на рис.12.

Номера строк в данной матрице соответствуют номерам отсчетов в скремблированном кадре, а номера столбцов соответствуют номерам исходных позиций отсчетов.

Анализируя обе матрицы для данного алгоритма, можно заметить, что единицы в матрице прямых перестановок и матрице обратных перестановок отстоят друг от друга на расстоянии k_1 и k_2 соответственно. Следовательно, процесс формирования прямой и обратной криптографических матриц можно свести к заданию номеров скремблированного и дескремблированного отсчетов в первой строке и циклическому сдвигу на величину, равную значению секретного ключа k_1 и k_2 соответственно.

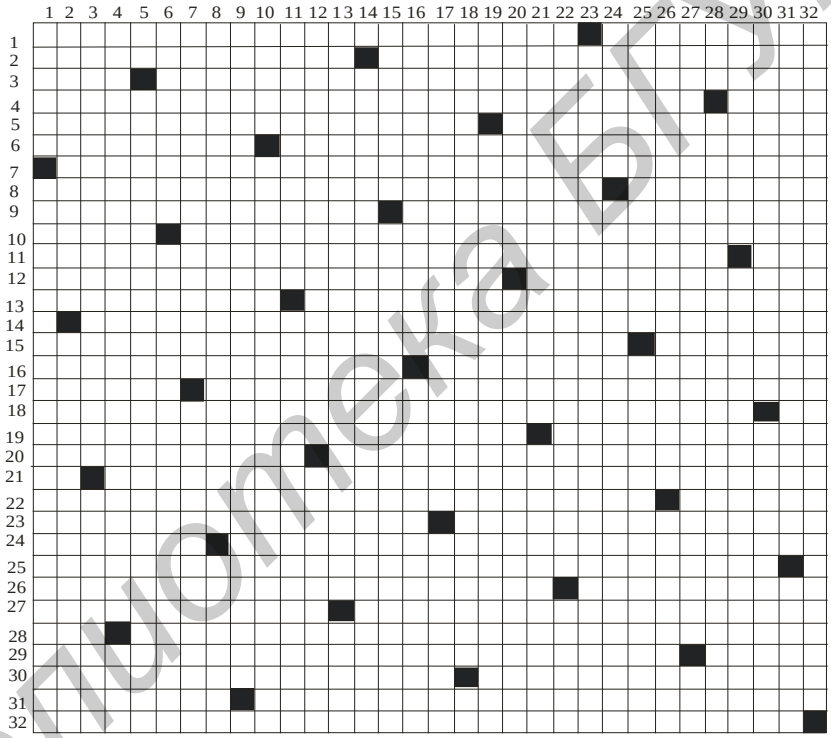

Рис.12. Обратная матрица однородных перестановок

1.3. Анализ и оценка основных параметров алгоритмов скремблирования

1.3.1. Оценка длины временного кадра

Выбор длины временного кадра или временного блока является первым шагом при разработке скремблеров, основанных на перестановках речевых отсчетов и перестановках сегментов речевого сигнала. От выбора данного параметра зависят основные характеристики скремблеров.

Длина временного кадра определяет число отсчетов речевого сигнала, к которым будет применяться операция перестановок, а длина временного блока определяет число сегментов, к которым будет применяться операция перестановок.

При выборе длины временного кадра следует учитывать ряд противоречивых требований. С одной стороны, от длительности кадра зависит остаточная разборчивость речевого сигнала, которая с увеличением длительности кадра уменьшается, так как увеличивается число эффективных перестановок. Под остаточной разборчивостью понимают степень возможности восстановления речевого сообщения при прослушивании его с помощью технических средств, не оснащенных данным типом устройств защиты информации. Увеличение количества отсчетов, участвующих в перестановках, ведет как к увеличению криптостойкости алгоритмов, так и к улучшению качества дескремблированного речевого сигнала. С другой стороны, с увеличением длины кадра, происходит увеличение временной задержки в процессе скремблирования, что играет немаловажную роль при выборе той или иной системы скремблирования, и, с этой точки зрения, необходимо выбирать минимальную длину кадра.

При решении задачи выбора длительности кадра необходимо учитывать следующий факт. Если кадр достаточно мал и не отражает квазипериодический характер сигнала, обусловленный частотой колебания голосовых связок речевого аппарата, то независимо от способа скремблирования конечным результатом будет лишь определенная потеря качества звука, но никакого эффекта по устранению разборчивости достигнуто не будет. Длительность окна должна быть больше, чем период основного тона. Если частота основного тона речи не менее 120 Гц, то длительность окна или временного кадра следует выбирать не менее (1000 мс/120) ≥ 8 мс.

Длительность кадра для алгоритмов скремблирования на основе псевдослучайных и однородных перестановок выбирается предпочтительно равной степенью двойки, поэтому минимальная длина временного кадра при скремблировании речевого сигнала, с точки зрения кратковременного анализа, ограничивается 16 мс, что, в свою очередь, соответствует 128 временным отсчетам. Выбор меньшей длины кадра приведет к неэффективности алгоритмов скремблирования, основанных на перестановках речевых отсчетов.

В случае алгоритма скремблирования на основе перестановок сегментов речевого сигнала длительность сегмента также ограничивается 16 мс. Однако, в отличие от перестановок речевых отсчетов, это значение равно максимальной длительности речевого сегмента в блоке. Это обусловлено тем, что при увеличении значения длительности речевого сегмента число, участвующих в перестановках внутри блока сегментов, уменьшается при условии сохранения длительности временного блока. Это приводит к уменьшению криптостойкости алгоритмов. Кроме того, увеличение длительности речевого сегмента является неэффективным с точки зрения остаточной разборчивости. Поскольку внутри

сегмента сигнал не разрушается, то сегменты желательно выбирать достаточно короткими, чтобы в них не содержались целые фрагменты сообщения, например отдельные слова. Это связано с тем, что при прослушивании в скремблированном сигнале пары $(i, i+2)$ соседних сегментов человеческий мозг в состоянии, как правило, восстановить пропущенный $(i+1)$-й сегмент, то есть восстановить соответствующую часть сообщения. Также необходимо учитывать фактор временной задержки. Число сегментов в блоке обычно выбирается равным 8 – 10 сегментам.

При выборе длительности речевых сегментов, равной длительности речевых отсчетов, алгоритм скремблирования на основе перестановок сегментов вырождается в алгоритм на основе перестановок отсчетов речевого сигнала. Следовательно, алгоритмы скремблирования речевых сигналов на основе перестановок речевых отсчетов являются частным случаем алгоритмов, основанных на перестановках сегментов речевого сигнала, при длительности сегмента, равной длительности отсчета.

1.3.2. Криптостойкость алгоритмов скремблирования

Общее количество перестановок, возможных на временном кадре (блоке) из N отсчетов (сегментов), равно $N!$. Если учитывать возможность смены знака отсчетов (сегментов) речевого сигнала, то общее количество возможных перестановок составит $2^N \times N!$. Однако это число не отображает реальной криптографической стойкости системы из-за избыточности информации, содержащейся в речевом сигнале, а также из-за остаточной разборчивости несовершенным образом переставленных отсчетов (сегментов) речевого сигнала. Поэтому криптоаналитику часто необходимо опробовать лишь $K << N!$ случайных перестановок для вскрытия речевого кода.

Свойство криптосистемы противостоять криптоатаке называется криптостойкостью. Криптостойкость алгоритма определяется в затратах злоумышленника, которые он несет вскрывая криптосистему (измеряется в машинном времени). Правило Киркхоффа гласит, что криптостойкость системы определяется не секретностью криптоалгоритма, а секретностью ключа, и, соответственно, размерностью пространства ключей.

Количество секретных ключей скремблера, использующего в качестве генератора ПСП регистр сдвига, определяется различными исходными состояниями регистра сдвига и выбором различных примитивных полиномов.

Число секретных ключей $K_{ПС}$ для псевдослучайных перестановок N ($N = 2^D$) временных отсчетов определяется соотношением:

$$K_{ПС} = (N-1) \times L(\log_2 N). \qquad (15)$$

Первый сомножитель, равный $(N-1)$, указывает на общее количество возможных исходных состояний для регистра сдвига, а второй член $L(D)$ определяет число примитивных полиномов степени $D = \log_2 N$.

Количество секретных ключей скремблера, использующего алгоритм однородного скремблирования, определяется различными значениями параметра N, равного количеству отсчетов внутри временного кадра.

Число секретных ключей K_U для однородных перестановок временных отсчетов:

$$K_U = G(N) \times N. \tag{16}$$

Первый сомножитель в данном выражении $G(N)$ используется для определения числа возможных значений секретного ключа k_1, которые являются взаимно простыми к длине N временного кадра.

Значения $G(N)$ зависит от того, является ли N простым или степенью 2:

$$\begin{cases} G(N) = N - 2, & \text{если } N - \text{простое} \\ G(N) = N - D - 1, & \text{если } N = 2^D. \end{cases} \tag{17}$$

Второй сомножитель в выражении (16) показывает количество возможных способов выбора первой строки в матрице размерностью $N \times N$.

Число секретных ключей K_S для перестановок временных сегментов речевого сигнала определяется соотношением:

$$K_S = N!, \tag{18}$$

где N – число речевых сегментов в блоке.

Таблица 6 иллюстрирует зависимость количества секретных ключей $K_{ПС}$ и K_U от числа отсчетов в кадре при однородных и псевдослучайных перестановках.

Число сегментов в блоке обычно выбирается равным 8 сегментам. Тогда, согласно выражению (18), число возможных секретных ключей будет равно $K_S = 40320$.

На основании данных таблицы 6 можно сделать вывод, что количество возможных секретных ключей для однородной перестановки K_U увеличивается значительно быстрее с ростом числа отсчетов в кадре N, чем для псевдослучайных перестановок. По этой причине однородные перестановки, с точки зрения криптостойкости, превосходят псевдослучайные и являются более эффективными для защиты речевых сигналов.

Таблица 7

Число секретных ключей для алгоритмов скремблирования

Число отсчетов в кадре, N	Число ключей при псевдослучайных перестановках, $K_{ПС}$	Число ключей при однородных перестановках, K_U
8	14	32
16	30	176
32	186	832
64	378	3648
128	2286	15360
256	4080	63232
512	24528	257024
1024	61380	1037312

1.3.3. Оценка временной задержки алгоритмов скремблирования

Временная задержка алгоритмов скремблирования системы передачи речи является параметром, связанным с требованием качества восстановленного сигнала. В системе передачи выделяют задержку, связанную с подсистемой скремблирования речи, и задержку, связанную с процессом передачи речи.

Задержка скремблирования состоит из следующих компонентов:

- задержка кадра (алгоритмическая задержка);
- задержки на обработку речи.

Алгоритмическая задержки обусловлена необходимостью сохранения в буфере памяти значения выборок речевого кадра. Задержка на обработку речи – время, необходимое для обработки сохраненных речевых выборок, складывается из времени обработки для преобразования речи на передающей и приемной стороне.

Суммарная задержка, состоящая из алгоритмической задержки и задержки на обработку, является задержкой системы одного направления. Максимально допустимая величина задержки системы в одном направлении составляет 400 мс при отсутствии эхо в канале. На практике предпочтительна задержка менее 200 мс.

Пусть выборка речевого сигнала занимает интервал времени, равный T с, а длина кадра составляет N выборок. Временная задержка при скремблировании будет являться суммой следующих двух слагаемых: 1) задержка в передатчике $(N-1)\times T$ – время необходимое для завершения обработки кадра (блока); 2) дополнительная задержка $(N-1)\times T$ в приемнике – максимальное время, в течение которого дескремблеру придется ждать, прежде чем он получит значение первого отсчета (сегмента) исходного кадра (блока) в переставленной последовательности. Таким образом, если не учитывать время передачи, задержка составляет $2\times(N-1)\times T$.

Минимальная длительность кадра для случая однородных и псевдослучайных перестановок речевых отсчетов составляет 16 мс, задержка скремблирования в этом случае равна 32 мс, что удовлетворяет требованию $t_з$<200 мс, поэтому можно увеличивать длительность кадра. При длине кадра, равной 256 отсчетам, что соответствует 32 мс, время задержки составляет 64 мс, что также удовлетворяет требованиям. При количестве отсчетов в кадре равном 512 задержка равна 128 мс. Дальнейшее увеличение длины кадра приводит к выходу за границы допустимой задержки, поэтому максимальное значение длительности кадра соответствует 64 мс или 512 отсчетам.

Максимальная длительность блока для алгоритмов скремблирования на основе перестановок речевых сегментов составляет 16 мс, среднее число сегментов в блоке равно 8, следовательно задержка равна 224 мс, что не удовлетворяет требованию $t_з$<200 мс, поэтому необходимо уменьшать длительность сегмента. При длине сегмента равной 14 мс время задержки составляет 196 мс, что удовлетворяет требованиям. Дальнейшее уменьшение длины сегмента приводит к уменьшению задержки и возможности увеличения числа сегментов в блоке.

Исходя из анализа и оценки результатов, можно рекомендовать следующие допустимые длительности временных кадров – [16, 32, 64] мс или соответственно [128, 256, 512] отсчетов для алгоритмов скремблирования на основе перестановок отсчетов речевого сигнала во временной области, а также выбор временного блока, равного 64 мс с длительностью речевых сегментов, равной 4 мс, что соответствует 16 сегментам в блоке.

1.3.4. Оценка качества блочных перестановок

В отличие от алгоритмов скремблирования на основе перестановок речевых отсчетов, для алгоритмов на основе перестановок речевых сегментов важным параметром является мера эффективности (или качества) перестановок. Существует несколько различных способов представления и оценки данной меры.

Объективной мерой эффективности перестановок речевых сегментов является временное расстояние d между парой сегментов в скремблированном блоке (рис.13). Временное расстояние d оценивается следующим соотношением:

$$\begin{cases} d = 1, & \textit{для смежных сегментов в исходном блоке} \\ d \geq 1, & \textit{для смежных сегментов в скремблированном блоке}. \end{cases} \qquad (19)$$

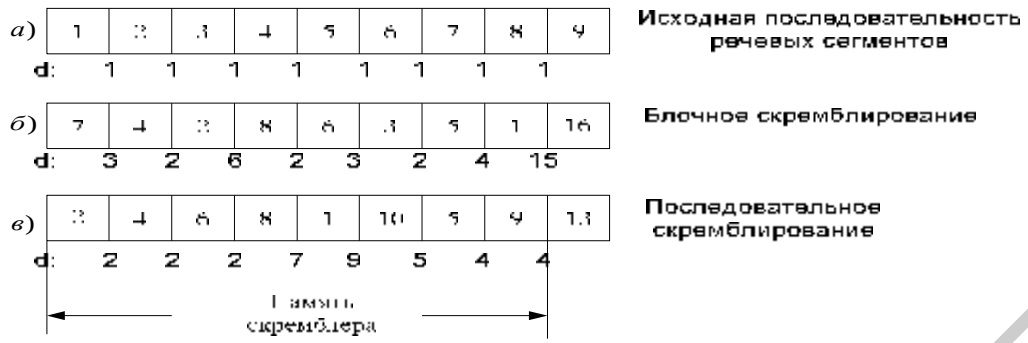

Рис.13. Временное расстояние d между речевыми сегментами блока

Максимальное значение d (рис.13, б) достигается в случае, когда случайная перестановка такова, что последний сегмент блока M (сегмент 16 рис.3, б) следует за первым сегментом блока $(M-1)$ (сегмент 1, рис.3, б), и в общем случае определяется следующим выражением:

$$\max(d) = 2M - 1 \ (\textit{в сегментах}). \tag{20}$$

Пусть для произвольной перестановки сегмента внутри блока $a(i)$ обозначает позицию, на которую a перемещает *i*-й сегмент. Тогда смещение *i*-го сегмента после перестановки равно $|i - a(i)|$, а среднее смещение после перестановки характеризуется величиной

$$g(a) = \frac{1}{N}\sum_{i=1}^{N}|i - a(i)|. \tag{21}$$

Величина $g(a)$ называется сдвиговым фактором и является мерой эффективности перестановок речевых сегментов. Для примера блочного скремблирования (рис.13, б) сдвиговый фактор $g(a) = 3.25$, а для примера последовательного скремблирования (рис.13, в) $g(a) = 2.375$. Следует отметить, что перестановки, приводящие к скремблированному речевому сигналу с низкой остаточной разборчивостью, имеют большой сдвиговый фактор, хотя обратное может быть неверным.

Очевидным способом получения меры эффективности перестановок в пределах блока является вычитание из скремблированной последовательности сегментов исходной последовательности. В результате вычитания формируется вектор $\vec{r}$, состоящий из положительных и отрицательных элементов. Элементы вектора положительны, если выборка была переставлена из своей позиции влево, и отрицательны, если выборка была задержана или переставлена вправо.

Таким образом, данный вектор (гамма-вектор) $\vec{r} = (r_1, r_2, ..., r_N)$ должен удовлетворять следующему условию:

$$\sum_{i=1}^{N} r_i = 0. \qquad (22)$$

Мера качества Γ перестановки сегментов речевого сигнала определяется гамма-вектором $\vec{r}$ и имеет следующий вид:

$$\Gamma = \sum_{i=1}^{N} | \ r_i \ |, \qquad (23)$$

где Γ – гамма-число.

Исходная последовательность речевых сегментов называется нулевой последовательностью, так как ее число гамма равно 0. Для примера блочного скремблирования (рис.13, б) гамма-вектор имеет вид $(6, 2, -1, 4, 1, -3, -2, -7)$ и $\Gamma = 26$, а для примера последовательного скремблирования (рис.13, в) гамма-вектор имеет вид $(1, 2, 3, 4, -4, 4, -2, 1)$ и $\Gamma = 21$.

Представленные способы оценки качества перестановок речевых сегментов позволяют обеспечить минимальную остаточную разборчивость путем выбора наиболее эффективных перестановок.

2. ЛАБОРАТОРНОЕ ЗАДАНИЕ

1. Изучите теоретическую часть.

2. Лабораторная работа выполняется в среде MATLAB с использованием графического интерфейса пользователя.

3. Порядок выполнения лабораторной работы следующий:

1) выберите режим работы скремблера.

2) создайте и загрузите в рабочую область среды MATLAB речевой сигнал с расширением .wav, частотой дискретизации 8000 Гц, разрядностью 8 бит.

3) выберите длительность речевого кадра.

4) выберите режим генерации секретных ключей.

5) получите результаты скремблирования речевого сигнала.

6) получите результаты дескремблирования речевого сигнала.

7) проведите оценку ширины спектра скремблированного и исходного речевых сигналов.

8) получите и сравните результаты скремблирования речевого сигнала для других режимов работы скремблера.

4. Оформите отчет и сделайте выводы.

3. СОДЕРЖАНИЕ ОТЧЕТА

1 Выполнение задания.

2. Результаты выполнения работы.

3. Анализ результатов и выводы.

4. КОНТРОЛЬНЫЕ ВОПРОСЫ

1. Что понимается под скремблированием и чем оно отличается от шифрования речевого сигнала? Назовите признаки классификации алгоритмов скремблирования?

2. В чем состоит сущность скремблирования речевого сигнала на основе перестановок сегментов? Достоинство и недостатки данного типа скремблирования? От чего зависит остаточная разборчивость речевого сигнала для алгоритмов данного типа?

3. Что определяет оператор перестановок отсчетов речевого сигнала? Поясните операцию прямых и обратных перестановок речевых отсчетов? Какова связь между перестановками во временной и частотной областях?

4. Поясните сущность основных этапов алгоритма скремблирования на основе псевдослучайных перестановок речевых отсчетов? К какому типу криптосистем можно отнести данный алгоритм? Поясните процедуру генерации криптографических матриц на этапе скремблирования и дескремблирования?

5.Поясните суть основных этапов алгоритма скремблирования на основе однородных перестановок речевых отсчетов? К какому типу криптосистем можно отнести данный алгоритм? Поясните процедуру генерации криптографических матриц на этапе скремблирования и дескремблирования?

6. Чем отличается алгоритм Евклида для нахождения *НОД* от расширенного алгоритм Евклида. Почему *НОД(k_1,N)* должен быть равен *1*?

7. Назовите основные критерии эффективности алгоритмов скремблирования? Чем определяется криптостойкость алгоритмов скремблирования?

8. Какими параметрами определяется степень остаточной разборчивости скремблированного речевого сигнала?

9. Какие алгоритмы скремблирования речевых сигналов можно использовать в телефонных каналах связи? Можно ли использовать данные алгоритмы для скремблирования речевых сигналов в частотной области?

10. Приведите таблицу сравнения алгоритмов блочного скремблирования, псевдослучайного и однородного скремблирования по основным параметрам?

ЛИТЕРАТУРА

1. Петраков А.В., Лагутин В.С. Утечка и защита информации в телефонных каналах. – М.: Солон-Пресс, 2003. – 363 с.

2. Дегтярев Н.П. Параметрическое и информационное описание речевых сигналов. – Мн.: Бестпринт, 2003. – 265 с.

3. Рылов А.С. Анализ речи в распознающих системах. – Мн.: Бестпринт, 2003. – 264 с.

4. Андрианов В.И., Бородин В.А. Шпионские штучки и устройства для защиты объектов и информации. – СПб.: Лань, 1997. – 262 с.

5. Галяшина Е.Н. Речь под микроскопом // Компьютерра. 1999. № 15. С.15 – 20.

6. Сергиенко А.Б. Цифровая обработка сигналов. - СПб.: Питер, 2003. – 608 с.

7. Jayant N.S., Cox R.V., McDermott B.J. Analog scramblers for speech based on sequential permutations in time and frequency // The Bell system technical journal. №1. 1983. С. 25 – 46.

8. Шелухин О.И., Лукъянцев Н.Ф. Цифровая обработка и передача речи. – М.: Радио и связь, 2000. – 415 с.

9. Phillips V.J., Lee M.N. Speech scrambling by the re-ordering of amplitude samples // The radio and electronic engineer. №3. 1971. С.99 – 104.

10. Kak S.C., Jayant N.S. On speech encryption using waveform scrambling // The Bell system technical journal. №5. 1977. С.781 – 809.

11. Рудаков П.И., Сафонов И.В. Обработка сигналов и изображений. – М.: Диалог Мифи, 2000. – 413 с.

12. Борискевич А.А., Лагойко А.Ю. Метод однородных перестановок для защиты речевых сообщений // Известия Белорусской Инженерной Академии, 2005, №2(20)/1.

13. Борискевич А.А., Лагойко А.Ю. Защита речевых сообщений на основе псевдослучайных и однородных перестановок // Доклады БГУИР 2005, № 5.

Св. план 2006, поз. 106

Учебное издание

ВРЕМЕННЫЕ ПЕРЕСТАНОВКИ ДЛЯ ЗАЩИТЫ РЕЧЕВЫХ СООБЩЕНИЙ

Пособие
к лабораторной работе по курсу
«Цифровая обработка речи и изображений»
для студентов специальности 1-45 01 03 «Сети телекоммуникаций»
дневной формы обучения

Авторы-составители:
Борискевич Анатолий Антонович,
Лагойко Алексей Юрьевич

Ответственный за выпуск А.А. Борискевич

Подписано в печать	Формат 60x84 1/16.	Бумага офсетная.
Гарнитура «Таймс».	Печать ризографическая.	Усл. печ. л.
Уч.-изд. л. 1,4.	Тираж 100 экз.	Заказ 81.

Издатель и полиграфическое исполнение: Учреждение образования
«Белорусский государственный университет информатики и радиоэлектроники»
ЛИ №02330/0056964 от 01.04.2004. ЛП №02330/0131518 от 30.04.2004.
220013, Минск, П. Бровки, 6