УДК. 681.3

И. В. Коряков

# Защищенная передача сигналов на основе модулярного преобразования

Рассматривается оригинальный класс устройств защиты речевых и речеподобных сигналов, на основе *модулярного преобразования* сигнала. Такое преобразование совмещает процесс модуляции и шифрования. Модуляционное созвездие формируется путем выполнения операций по модулю над цифровыми отсчетами сигнала и отсчетами гаммы.

## Метод

Идея модулярного преобразования достаточно проста: если отсчеты исходного сигнала *s* представлены числами, то эти числа могут быть подвергнуты шифрованию и преобразованы в отсчеты зашифрованного сигнала *v*; восстановление подразумевает взятие отсчетов, расшифрование и преобразование в исходные отсчеты $s\hat{} = s + ds$ с некоторой ошибкой *ds*. Степень защиты при этом соответствует уровню алгоритмов шифрования данных.

Трудность прямого решения данной задачи заключается в том, что необходимо при шифровании отсчетов сохранять полосу исходного сигнала без “просачивания” исходной статистики в результат преобразования и, главное, восстанавливать сигнал при наличии шума и/или необратимых искажений в закрытом сигнале так, чтобы мощность шума существенно не увеличивалась при восстанов-

лении сигнала. Другими словами, преобразование должно обладать свойством непрерывности в следующем смысле: при некотором уменьшающемся приращении $\delta v$ значения $v$ отсчета закрытого сигнала, восстановленный отсчет $s\hat{}$ также должен иметь уменьшающееся приращение $\delta s$.

Этим требованиям удовлетворяет преобразование, в котором каждый комплексный отсчет сигнала **s** суммируется по модулю $D$ с отсчетом псевдослучайной последовательности **g** (гаммы) с равномерным на квадрате $D \times D$ распределением. Статистика результирующего сигнала **v** соответствует статистике гаммы и не содержит статистики исходного сигнала [1].

Формирование комплексного отсчета **v** из сигнала **s** и гаммы **g**, когда каждый из отсчетов представлен двумя целыми $d$-разрядными числами, осуществляется в соответствии с выражениями:

$$\begin{aligned} v_x &= (s_x + g_x) \bmod 2^d \\ v_y &= (s_y + g_y) \bmod 2^d \end{aligned} \qquad (1)$$

Удобно выбирать $d$, равное длине машинного слова, например, в конкретной реализации $d$=32. Тогда сложение по модулю определяется как сложение целых без учета переполнения. Причем, будут числа представлены как целые без знака или целые со знаком в дополнительном коде – не имеет значения, поскольку коды, получаемые в результате операций, идентичны. Восстановление сигнала **s**^ производится сложением **v** с дополнением **g** до $2^d$ по модулю $2^d$:

$$\begin{aligned} s_x^{\wedge} &= (v_x + (2^d - g_x)) \bmod 2^d \\ s_y^{\wedge} &= (v_y + (2^d - g_y)) \bmod 2^d \end{aligned} \qquad (2)$$

Свойства последовательности бит $b_i$, из которой формируются отсчеты $g_k$ гаммы как

$$g_k = \sum_{j=0}^{d-1} b_{kd+j} 2^{d-j-1}$$

должны соответствовать свойствам случайной равновероятной последовательности нулей и единиц. Тогда статистика последовательности **v** будет неотличима от статистики **g**, а проникновение статистики **s** в **v** полностью исключено. Отсчеты **g** и **v** имеют рав-

номерное распределение плотности вероятности на квадрате {[0, $2^d$-1], [0, $2^d$-1]} или для целых со знаком на квадрате {[-$2^{d-1}$, $2^{d-1}$-1], [-$2^{d-1}$, $2^{d-1}$-1]}.

Сигнал модулярного преобразователя в комплексном виде представляет собой квадратное созвездие с большим числом равноотстоящих точек ($2^{2d}$) с равномерной плотностью распределения вероятности, обеспечиваемой генератором гаммы. Для генерации $g_k$ возможно применение любой *работоспособной* криптографической функции [3].

**Структура**

На рисунке 1 представлена упрощенная структура передающей и приемной части модулярного преобразователя. Отсчеты *s(n)* исходного сигнала *s(t)* при помощи преобразователя Гильберта H переводятся в комплексные отсчеты и переносятся к нулю частот (обозначим $\mathbf{s}_0(n)$) умножением на сигнал условной несущей частоты $f_{cs}$ такой, чтобы полоса сигнала была симметричной относительно нуля частоты и, естественно, меньше половины частоты дискретизации $f_s$.

Отсчет $\mathbf{s}_0(n)$ выражается в виде пары целых чисел длиной *d* двоичных разрядов. Числа шифруются сложением в соответствие с (1) с элементами гаммы $\mathbf{g}(n)$ также длиной *d* двоичных разрядов, выражаются в виде отсчетов, пропущенных через формирующий фильтр Найквиста F, и переносятся на несущую частоту $f_v$ (не обязательно $f_{cs} = f_v$) для получения действительных отсчетов *v(n)* и, соответственно, сигнала *v(t)*. На приемной стороне обеспечивается строгая синфазность дискретизации сигнала *v(t)* по отношению к передатчику, перенос на нулевую несущую от частоты $f_v$, компенсация линейных искажений в канале при помощи фазового корректора. Комплексные отсчеты выхода корректора представляются *d*-разрядными числами, суммируются в соответствии с (2) с элементами гаммы приемника $\mathbf{g}(n)$, интерполируются фильтром F и переносятся в действительную область на частоту $f_{cs}$ для получения отсчетов *s^(n)* и восстановления сигнала *s^(t)*. На рисунке 2 приведен вид сигналов в частотной области на этапах прямого модулярного преобразования.

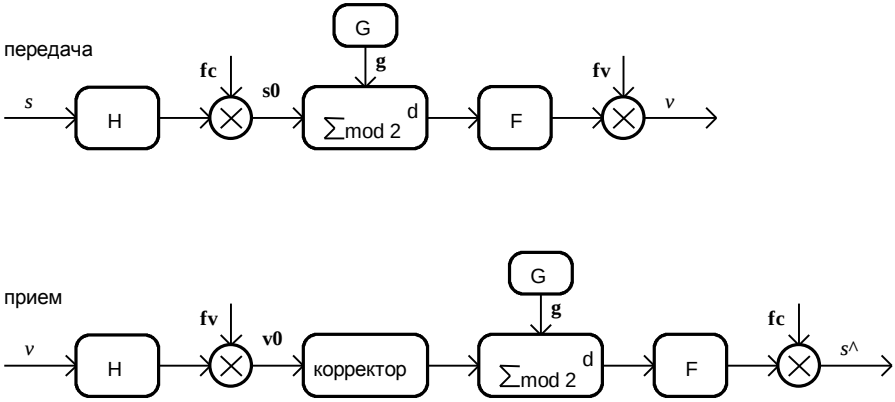


Рис. 1 – Структура модулярного преобразователя

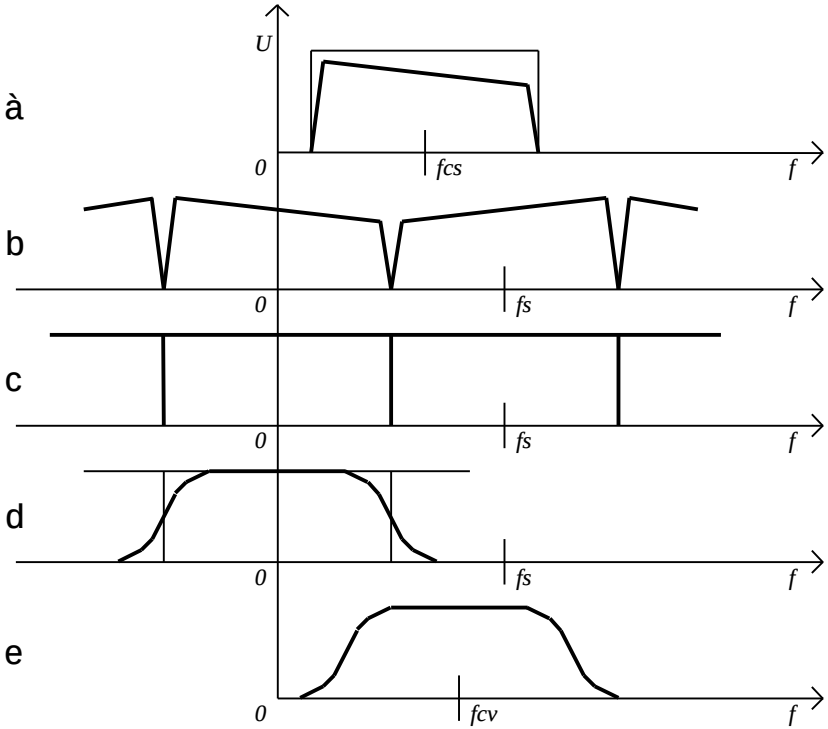


Рис. 2 – Формирование закрытого сигнала

На рисунке 2 этапы формирования сигналов обозначены буквами:

a. Спектр исходного действительного сигнала *s*, ограниченный фильтром с частотной характеристикой, близкой к прямоугольной и шириной полосы, равной частоте дискретизации $f_s$ комплексного сигнала. Условная несущая $f_{cs}$ соответствует середине спектра сигнала *s*.

b. Спектр комплексного сигнала **s**, децимированного к частоте дискретизации $f_s$ на нулевой несущей.

c. Спектр комплексной гаммы **g** (и результата суммирования по модулю).

d. Комплексный сигнал, полученный в результате интерполяции к частоте дискретизации $4f_s$ фильтром Найквиста.

e. Действительный сигнал *v* после переноса на несущую $f_{cv}$.

На рисунке 3 приведен вид сигналов в частотной области на этапах обратного модулярного преобразования:

a. Спектр принятого действительного сигнала *v*.

b. Спектр комплексного сигнала **v**, децимированного к частоте дискретизации $f_s$ после переноса от несущей $f_{cv}$ к нулю.

c. Спектр комплексной гаммы **g** (и результата суммирования по модулю).

d. Комплексный сигнал **s^**, полученный в результате интерполяции к частоте дискретизации $4f_s$ фильтром с частотной характеристикой, близкой к прямоугольной.

e. Восстановленный действительный сигнал *s^* после переноса на условную несущую $f_{cs}$.

**Особенности реализации**

В практической реализации устройства защиты на основе модулярного преобразования для передачи сигналов в стандартном телефонном канале структура рисунка 1 дополняется адаптивным подавителем сигналов эхо и системой синхронизации по несущей $f_{cv}$ и по тактовой частоте $f_s$.

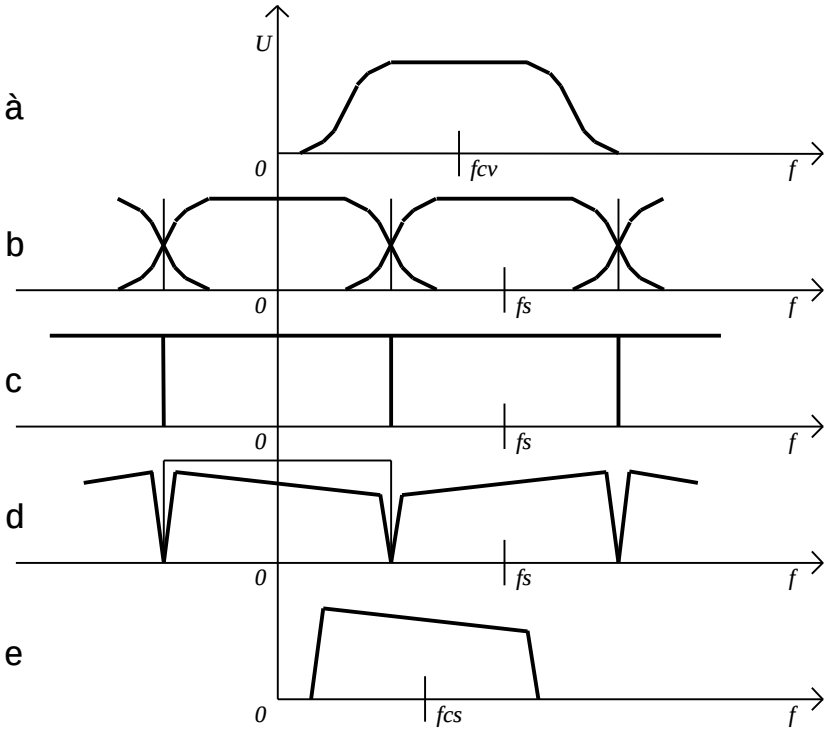


Рис. 3 – Восстановление исходного сигнала

Для реализации функций адаптации и синхронизации в структуру сигнала модулярного преобразователя включаются так называемые реперные точки, представляющие собой элементы созвездия (например CCITT-81380) в последовательности, известной обеим сторонам. В конкретной реализации одна реперная точка включается после каждых 18 отсчетов сигнала **v**. На приемной стороне реперные точки исключаются.

Фазовый корректор в составе модулярного приемника может быть построен так же, как и в обычных модемах передачи данных, за исключением одной уникальной особенности. Типовой корректор модема с решающей обратной связью [2] содержит инверсный фильтр ИФ, на вход которого поступает принимаемый сигнал, а из выходного сигнала вычитается реакция прямого фильтра ПФ, на

вход которого поступает решение (идеальные координаты точки созвездия, по которой было принято решение на предыдущем шаге).

На вход прямого фильтра корректора модулярного приемника поступают комплексные отсчеты гаммы и, если в модеме текущее и все будущие решения неизвестны, то в модулярном приемнике гамма известна в отрицательном и в положительном времени. Прямой фильтр модема, являясь каузальной системой, не может полностью компенсировать искажения, связанные с потерями в спектре принимаемого сигнала, в модулярном приемнике такие потери могут быть скомпенсированы полностью.

На рисунке 4 приведена упрощенная структура корректора модулярного приемника с предсказанием ошибки по гамме.

Модулярный приемник, помимо обычного дробно-интервального адаптивного корректора ИФ, содержит предсказатель ПФ, на вход которого поступают отсчеты гаммы **g**. Сигнал ошибки **e**, по которой производится адаптация, определяется как модулярная разность выхода корректора **y** и предсказателя **eg** в соответствие с (2).

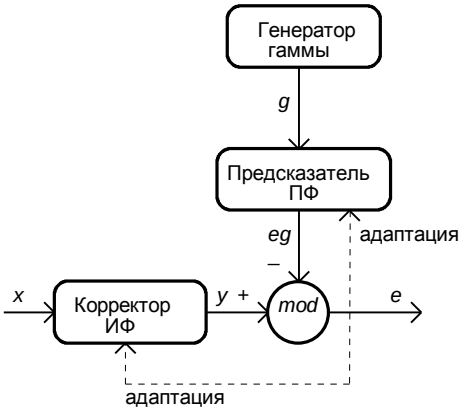


Рис. 4 – Упрощенная структура корректора с предсказанием по гамме

Корректор ИФ определяется фильтром:

$$y(n) = \sum_{i=0}^{N-1} w(i)x(n-i)\,,$$

коэффициенты $\mathbf{w}_i$ которого адаптируются на $m$-том шаге в соответствии с формулой:

$$w_i = w_i + u\_e^* x(m-i),$$

где $u_c$ - коэффициент адаптации корректора; **e*** означает комплексно сопряженный сигнал ошибки. Для конкретной реализации дробно-интервального корректора $m=2n$.

Предсказатель ПФ определяется фильтром:

$$eg(m) = \sum_{i=0}^{M-1} b(i)e(m-i),$$

коэффициенты $b_i$ которого адаптируются на $m$-том шаге в соответствии с формулой:

$$b_i = b_i + u_p e^*(m-i),$$

где $u_p$ – коэффициент адаптации предсказателя.

Реальные значения длины фильтров $N$ и $M$ определяются требованиями к допустимой величине ошибки и производительностью процессора DSP. Ориентировочно, для дробно-интервального корректора с кратностью 2 и частотой дискретизации 4800 Гц $N$ может составлять 64 комплексных отсчета, а $M$ – 16 комплексных отсчетов с частотой дискретизации 2400 Гц.

Для обеспечения устойчивости и заданной скорости сходимости адаптивных фильтров ИФ и ПФ требуется нормирование энергии сигналов на входах фильтров.

Коэффициенты адаптации $u_c$ и $u_p$ могут быть неодинаковыми и изменяться во времени в зависимости от режима приемника. Например, в процессе приема сигнала настройки корректора $u_c$ = 0.01 и $u_p$ = 0.01, в процессе приема данных – $u_c$ = 0.005 и $u_p$ = 0.001.

Перед периодом адаптации по настроечной последовательности (train) производится оценка мощности $p_c$ входного сигнала несущей, которая затем используется для вычисления коэффициента адаптации, и отклонения нормирующего коэффициента от единицы. На последующих этапах обработки входной сигнал умножается на множитель $k_0$ :

$$k_0 = \frac{1}{\sqrt{p_c}}$$

Оценка $p_c$ считается единичной мощностью, относительно которой рассчитывается $u_c$ как

$$u_c = \frac{u_{c0}}{pk_0^2},$$

где $u_{c0}$ имеет типовое значение 0.003.

В рабочем режиме сигнал ошибки **e** представляет собой не что иное, как комплексный восстановленный сигнал **s^**.

Для преобразования **s^** в действительный сигнал осуществляется кратное повышение частоты дискретизации, интерполяция фильтром НЧ и возврат спектра сигнала на условную несущую $f_{cs}$:

Для предотвращения “перескоков” отсчетов восстановленного сигнала на величину порядка $2^d$ при определенных сочетаниях значений отсчетов исходного сигнала, гаммы и ошибки амплитуда исходного сигнала должна быть ограничена так, чтобы сумма исходного сигнала и максимального значения ошибки не превышала $2^d$. Это достигается умножением отсчетов исходного сигнала на множитель $q$<1 и умножением восстановленных отсчетов на величину $1/q$. Типовое значение $q$ составляет 0.8 для уровня ошибки –24 дБ.

Существенное уменьшение шума в паузах достигается применением кодирования отсчетов исходного сигнала по логарифмическому закону перед выполнением суммирования (1) и потенцирования восстановленных отсчетов после вычитания (2). В практической реализации выполнялось преобразование отсчетов в соответствии с μ-законом компандирования при μ=64. Такое преобразование при практически незаметном возрастании ошибки на больших уровнях сигнала уменьшает шум в паузах на 12 - 15 дБ.

Помимо описанных функций, модулярный преобразователь должен исполнять некоторый протокол начала и окончания сеанса связи, поддержания неразрывности сеанса связи, ретренинг при существенном изменении характеристик канала, передачу служебной информации, в общем, ряд обычных функций модема, требования к реализации которых могут быть заимствованы из соответствующих

рекомендаций ITU-T или разработаны специально для конкретных каналов связи.

**Выводы**

Особым свойством модулярного преобразования является трансформация искажений любого рода в канале передачи в шум, близкий к нормальному. Уровень шума не зависит от амплитуды передаваемого речевого сигнала и пропорционален приведенной ошибке (в модемах - ошибка принятия решения). Ошибка при восстановлении сигнала модулярного преобразования определяется продуктами нелинейных преобразований в тракте передачи, энергетическими потерями в полосе сигнала, ошибкой корректора из-за ограниченной длины импульсной характеристики фильтра, ошибкой подавителя сигнала эхо, вычислительными ошибками и, наконец, уровнем мощности шума в канале.

Достоинством модулярного преобразования, по сравнению с вокодерными системами, является передача “чистой” речи, т. е. не подвергнутой сжатию. Показатели разборчивости, естественности и узнаваемости у модулярных аппаратов защищенной связи наивысшие среди рассматриваемых классов. Характерные вокодерные искажения речевого сигнала заменяются при модулярном преобразовании шумовым сигналом, к которому в наилучшей степени адаптируется слух человека. Сигнал $s(t)$ может иметь произвольную природу, в частности, это может быть факсимильный или модемный сигнал.

Метод защиты сигналов на основе модулярного преобразования реализован как один из режимов в изделиях «КРИПТОН-4М7» и «СЕКМОД-К» предприятия ООО НВФ «Криптон». Реализация метода требует около 10 MIPS для 32-х разрядного процессора цифровой обработки сигналов. Испытания изделий показали высокую степень защиты и качество передачи речевых сигналов, а также сигналов передачи данных и факсимильных сообщений, для скоростей передачи до 9600 бит/с и каналов связи с приведенной ошибкой до -24 дБ (ошибка принятия решения, вклад в которую вносит шум, нелинейность и дисперсия всего тракта передачи сигнала, а также ошибки метода и конечной длины и разрядности вычислений). Требования к каналу для передачи модулярного сигнала примерно соответствуют требованиям к модемной передаче данных со

скоростью 9600 - 12000 бит/с (хорошее качество достигается на подавляющем большинстве соединений городских АТС).

Аудиторные испытания, которым подвергались изделия, проводились по методу мнений [4] (методика, близкая к определению показателя MOS) и подтвердили высокое качество речевой связи с использованием защиты на основе модулярного преобразования. Показатель был равен 3.9 для открытого канала связи и 3.7 для закрытого модулярным преобразованием. Для сравнения укажем, что для защищенного вокодерного канала с алгоритмом сжатия речи класса CELP, реализованным в составе этих же изделий, со скоростью передачи 9600, 4800 и 2400 бит/с значения показателя MOS составили соответственно 3.3, 2.4 и 2.1.

Наиболее эффективное ожидаемое применение криптографически защищенной передачи сигналов на основе модулярного преобразования предполагается на цифровых каналах связи при повышенных требованиях абонентов к качественным характеристикам передачи речи, таким, как естественность звучания речи и узнаваемость диктора.

**Литература**

1. Кнут. Д. Искусство программирования для ЭВМ. Т.2. Получисленные алгоритмы. Пер. с англ. / Под ред. К.И. Бабенко. - М.: Мир, 1977.
2. Куреши Ш. Адаптивная коррекция. ТИИЭР, 1985, т. 73, №5, с. 5-49.
3. Feistel H. Cryptography and computer privacy. Sci. Amer. 228, 5 (May 1973), 15-23.
4. В. Вемян. Передача речи по сетям электросвязи. М: Радио и связь, 1985.