

**МОДЕЛИРОВАНИЕ СПОСОБА СКРЫТНОЙ ПЕРЕДАЧИ ГРУППЫ
БИНАРНЫХ ПОЛЕЗНЫХ СИГНАЛОВ С ИСПОЛЬЗОВАНИЕМ
ПАКЕТА ПРОГРАММ MATLAB/SIMULINK**

Ю. Б. Нечаев, Б. Н. Воронков, Е. С. Долбилова

Воронежский государственный университет

В статье приводятся результаты моделирования с помощью пакета программ Matlab 6.5 системы радиосвязи, обеспечивающей одновременную скрытную передачу и прием полезных бинарных сигналов пониженной мощности на фоне мощного периодического широкополосного маскирующего сигнала. Описан ряд недостатков данного способа передачи бинарных полезных сигналов и даны рекомендации по их устранению.

**1. ОБЕСПЕЧЕНИЕ СКРЫТНОСТИ
ПЕРЕДАЧИ СИГНАЛОВ:
СУЩЕСТВУЮЩИЕ МЕТОДЫ**

Потребность общества в новых информационных и телекоммуникационных услугах определяет пути развития новых технологий, которые становятся основой современных систем связи. В связи с возрастанием требований к скорости и объему передачи информации, новой тенденцией обеспечения безопасности становится не защита собственно телекоммуникационных систем, а защита информации, циркулирующей в этих системах. В этом случае важным является реализация способов скрытной передачи полезной информации, особенно, если речь идет об информационной безопасности группы передающих устройств. Одним из таких способов является излучение маскирующего широкополосного сигнала в диапазоне частот всей группы полезных сигналов, суммирование полезного и помехового сигналов и последующее подавление маскирующего сигнала при приеме [1, 2].

Использование различных методов подавления маскирующей информации (вырезание необходимого участка частотного спектра после демодуляции маскирующего сигнала или компенсация с задержкой) требуют проведения исследований влияния искажений полезных сигналов на результирующие характеристики радиосвязи.

Известен «Способ маскировки передаваемого сообщения» [1], согласно которому на пере-

дающей стороне полезный сигнал синхронно суммируется с мощным маскирующим сигналом, закон формирования которого известен, поэтому на приемной стороне он может быть отделен от полезного сигнала. При этом маскируется лишь один полезный сигнал, что является недостатком этого способа.

В другом способе передачи замаскированного сигнала [2] при формировании полезного и маскирующего сигналов используют двухканальную схему: по одному каналу передают только маскирующий сигнал, а по второму – сумму этого сигнала, преобразованного по амплитуде и фазе, и полезного сигнала. При приеме срабатывает помехоподавляющий блок, в котором маскирующий сигнал, переданный по первому каналу, подвергают преобразованию, аналогичному преобразованию в передатчике, и вычитают его из суммарного сигнала, переданного по второму каналу. В результате устранения маскирующего сигнала остается только полезный сигнал. Для противника структура полезного сигнала будет скрыта.

Недостаток этого способа состоит в том, что он позволяет замаскировать сигнал только одного передатчика.

**2. СПОСОБ ПЕРЕДАЧИ ГРУППЫ
БИНАРНЫХ ПОЛЕЗНЫХ СИГНАЛОВ**

Для преодоления этого недостатка излучают группу полезных сигналов независимо от маскирующего, спектр которого перекрывает диапазон частот всей группы полезных сигналов. При этом маскирующий сигнал формируют из узкополосного путем расширения его спектра

за счет фазовой или частотной модуляции, закон которой известен «своим» приемникам. На приемной стороне преобразуют все входные, в том числе и маскирующий, сигналы таким образом, что спектр маскирующего сигнала сужают, а спектры остальных входных сигналов расширяют, далее маскирующий сигнал режектируют, а затем восстанавливают полезные сигналы [3]. Однако, при режекции части спектра полезных сигналов происходит искажение этих сигналов. Кроме того, при частотной фильтрации в тракте приемного устройства маскирующий сигнал приобретает паразитную модуляцию, что приводит к формированию боковых составляющих спектра маскирующего сигнала, которые не режектируются и образуют вторичные маскирующие помехи.

Устранение отмеченных недостатков возможно при использовании следующего подхода. Независимым образом излучают совокупность полезных сигналов и периодический маскирующий широкополосный сигнал, основная часть спектра которого перекрывает диапазон частот всей группы полезных сигналов. Несущая частота шумоподобного маскирующего сигнала кратна величине f_0 , обратной длительности одного элемента полезной цифровой информации, передаваемой с помощью двоичных сигналов, манипулированных по амплитуде, фазе или частоте. При этом значения несущих частот (в случае частотно-манипулированного сигнала — манипулируемых частот) полезных сигналов также кратны величине f_0 . Подавление маскирующего сигнала в «своих» приемниках осуществляют методом компенсации с задержкой. То есть, задерживают входную смесь сигналов на время, равное длительности периода маскирующего сигнала, а затем вычитают ее из незадержанной смеси сигналов. Искажения полезных сигналов, возникающие в результате компенсации маскирующего, устраняют в специальных блоках восстановления полезных сигналов, которые включены последовательно с выходами «своих» приемников.

3. ИСПОЛЬЗОВАНИЕ MATLAB И SIMULINK ДЛЯ МОДЕЛИРОВАНИЯ СИСТЕМ РАДИОСВЯЗИ

Simulink — интерактивный инструмент для моделирования, имитации и анализа динамических систем [4]. Он дает возможность строить

графические блок-диаграммы, имитировать динамические системы, исследовать работоспособность систем и совершенствовать проекты. Simulink полностью интегрирован с MATLAB, обеспечивая немедленным доступом к широкому спектру инструментов анализа и проектирования. При моделировании с использованием Simulink реализуется принцип визуального программирования, в соответствии с которым, пользователь на экране из библиотеки стандартных блоков создает модель устройства и осуществляет расчеты. При этом, в отличие от классических способов моделирования, пользователю не нужно досконально изучать язык программирования и численные методы математики, а достаточно владеть информацией, требующейся при работе на компьютере и, естественно, знанием той предметной области, в которой он работает.

При работе с Simulink пользователь имеет возможность модернизировать библиотечные блоки, создавать свои собственные, а также составлять новые библиотеки блоков. Преимущество Simulink заключается также в том, что он позволяет пополнять библиотеки блоков с помощью подпрограмм написанных как на языке MATLAB, так и на языках C++, Fortran и Ada.

Эти преимущества делают Simulink наиболее популярным инструментом для проектирования систем управления и коммуникации, цифровой обработки и других приложений моделирования.

4. МОДЕЛЬ ПЕРЕДАЧИ ГРУППЫ БИНАРНЫХ ПОЛЕЗНЫХ СИГНАЛОВ

Функциональная схема системы связи, в которой реализуется предлагаемый способ, приведена на рис. 1, где обозначено:

I — блок подавления маскирующего сигнала (БПМС);

II — блок восстановления сигнала (ВВС);

11 — один из группы передатчиков полезных сигналов;

1² — передатчик периодического широкополосного маскирующего сигнала;

2¹, 2² — линии (каналы) связи;

3¹, 3² — приемные антенны, суммирующие приходящие сигналы;

4¹ — один из приемников «своей» радиолинии;

4² — приемник «чужой» радиолинии.

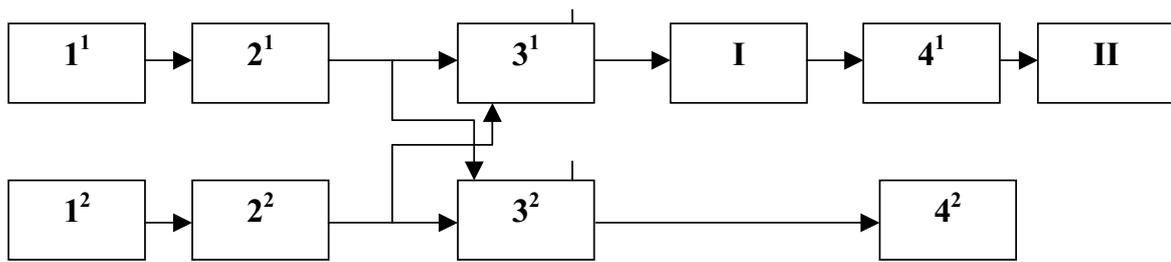


Рис. 1. Функциональная схема системы связи, в которой реализуется предлагаемый способ

В этой системе в качестве примера представлена одна «своя» радиолиния, которых может быть несколько, состоящая из передатчика полезного сигнала 1^1 , линии связи (радиоэфира) 2^1 , приемной антенны 3^1 , блока подавления маскирующего сигнала (БПМС) I, «своего» приемника 4^1 и блока восстановления сигнала (БВС) II.

«Чужой» приемник 4^2 , играющий роль разведприемника, принимает смесь сигналов с выхода приемной антенны 3^2 .

Передатчик периодического широкополосного маскирующего сигнала 1^2 , по сути, является передатчиком заградительной помехи, которая кроме маскировки сигналов в своей полосе частот может подавлять «чужие» приемники.

Усилитель мощности и передающая антенна не имеют принципиального значения, поэтому на рис.1 не показаны.

Пусть T — длительность одного элемента цифровой информации. Тогда периодический широкополосной маскирующий сигнал, представляющий собой последовательность повторяющегося во времени сегмента произвольного широкополосного колебания длительностью $n \cdot T$ (где n — величина кратности), будет иметь значение несущей частоты N/T (где N — величина кратности). Значения несущих частот полезных сигналов должны быть равны значениям M/T (где $M = (N \pm m)$ — величина кратности, $m = 0, 1, 2, \dots$ — целое положительное число, $m < N$). В этом случае все полезные сигналы, находящиеся в полосе частот маскирующего сигнала, оказываются замаскированными спектральными составляющими последнего.

Произведено моделирование данной схемы повышения скрытности с помощью пакета программ Matlab 6.5/Simulink. На рисунке 2 приведена общая схема системы связи. Блок

Desired Signal Transmitter отвечает за генерацию полезного сигнала, в блоке Masking Signal Transmitter формируется широкополосный маскирующий сигнал, а блок Receiver — за прием и восстановление сигнала.

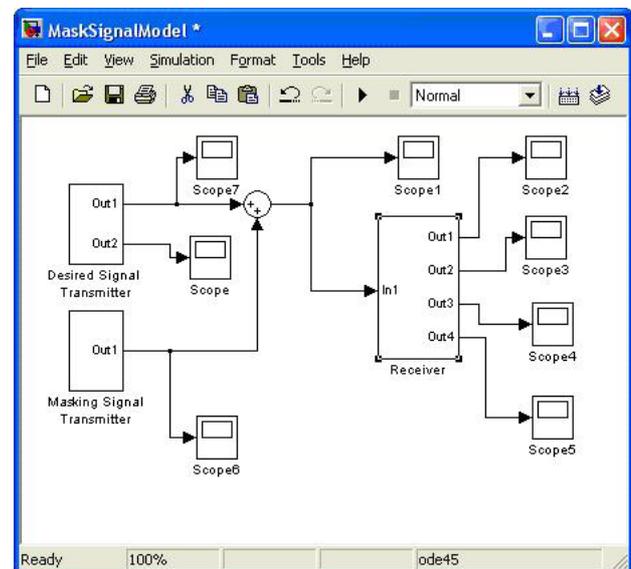


Рис. 2. Общая схема системы связи

Модель формирования полезного сигнала приведена на рис.3, где блок Information shaper отвечает за генерацию псевдослучайных последовательностей бинарных импульсов, блок Carrier Frequency Oscillator — генератор высокочастотного сигнала, блок Clock rate Generator — генератор тактовой частоты. Несущая частота полезного сигнала 9,9 МГц. Исходя из приведенной модели, полезный сигнал можно записать следующим образом:

$$\begin{aligned}
 U_s(t) &= \\
 &= 0.005 * \sum_{m=2}^{N-1} \hat{q}_m \sin(\omega_n t + \varphi_n) \times \\
 &\times \{1[t - m\tau_n] - 1[t - (m + 1)\tau_n]\},
 \end{aligned}$$

где N — количество импульсов периодической цифровой информации на одном периоде; τ_n — длительность одного импульса; \hat{q}_m в соответствии с передаваемой цифровой информацией; ω_n — круговая, несущая частота полезного сигнала; φ_n — начальная фаза.

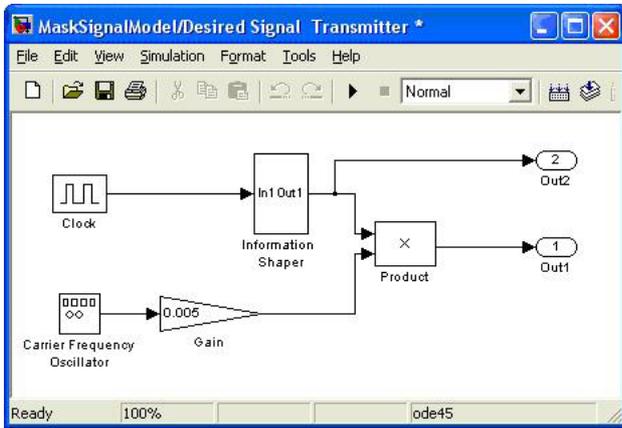


Рис. 3. Модель формирования полезного сигнала

Модель формирования маскирующего сигнала приведена на рис. 4, где блоки PRS-Generator1 и PRS-Generator2 отвечают за генерацию псевдослучайных последовательностей бинарных импульсов, блок Carrier Frequency Oscillator — генератор высокочастотного сигнала, блок Clock rate Generator — генератор тактовой частоты. Несущая частота маскирующего сигнала 10 МГц. Маскирующий сигнал можно представить следующим образом:

$$U_M(t) = \sum_{m=0}^{N-1} q_m \sin(\omega_0 t + \varphi_0) \{1[t - m\tau_0] - 1[t - (m+1)\tau_0]\},$$

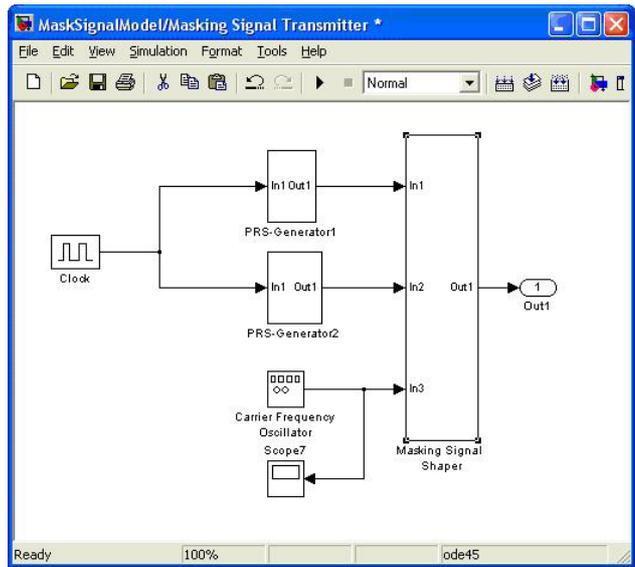


Рис. 4. Модель формирования маскирующего сигнала

где N — количество импульсов псевдослучайной последовательности периодического маскирующего сигнала; τ_0 — длительность дискрета маскирующего ФМн сигнала; q_m в соответствии с кодом фазоманипулированного сигнала; ω_0 — несущая частота маскирующего сигнала; φ_0 — начальная фаза. При этом: $\tau_n = 15\tau_0$.

На рисунке 5 изображена модель приемника предлагаемой системы. Подавление маскирующего сигнала осуществляется методом компенсации с задержкой. Для этого входную смесь сигналов задерживается на время, равное периоду маскирующего ФМн сигнала, а затем вычитается из незадержанной смеси сигналов. Устранение появляющихся в результате компенсации с задержкой искажений полезного сигнала осуществляется в блоке восстановления

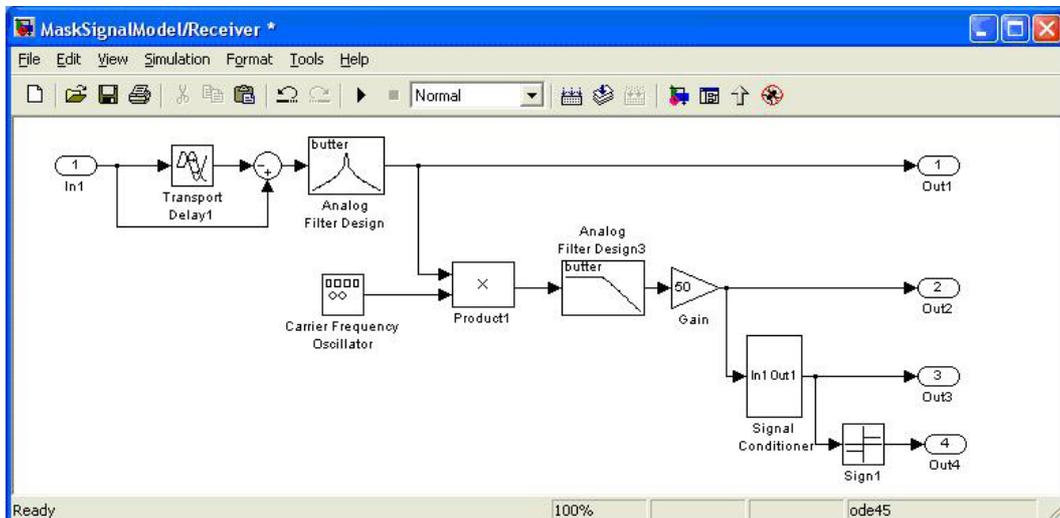


Рис. 5. Модель приемника сигнала

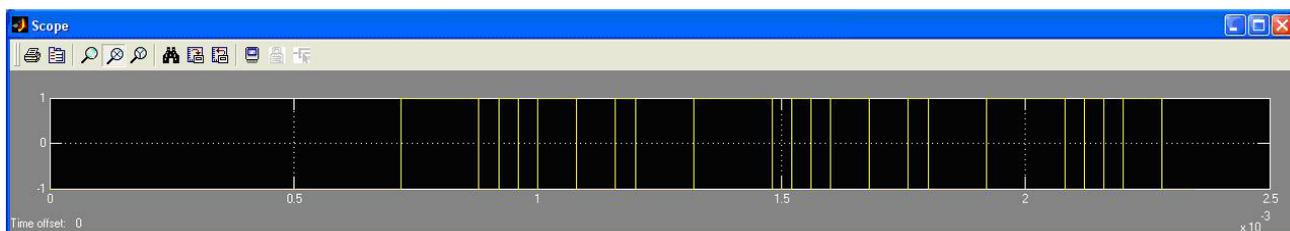
сигнала Signal Conditioner. На рисунке 6 можно проследить восстановление полезного сигнала в приемнике.

В полученной модели существует возможность изменения ряда параметров: времени задержки при подавлении маскирующего колебания, коэффициентов усиления при передаче и приеме, полос пропускания и типов фильтров, что позволило провести эксперименты по оценке влияния их на скрытность передачи.

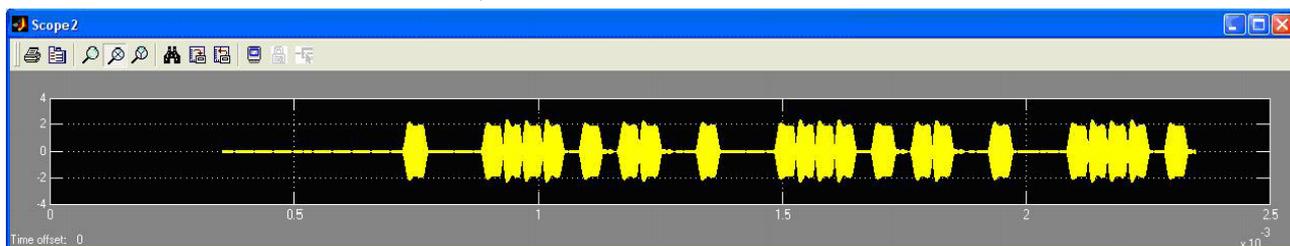
5. РЕЗУЛЬТАТЫ МОДЕЛИРОВАНИЯ

Результаты моделирования данной системы радиосвязи с использованием пакета программ Matlab 6.5/Simulink подтвердили работоспособность предлагаемого способа повышения скрытности передачи совокупности двоичных полезных сигналов, манипулированных по амплитуде, фазе или частоте.

В ходе исследования данной схемы было выявлено, что при использовании в качестве



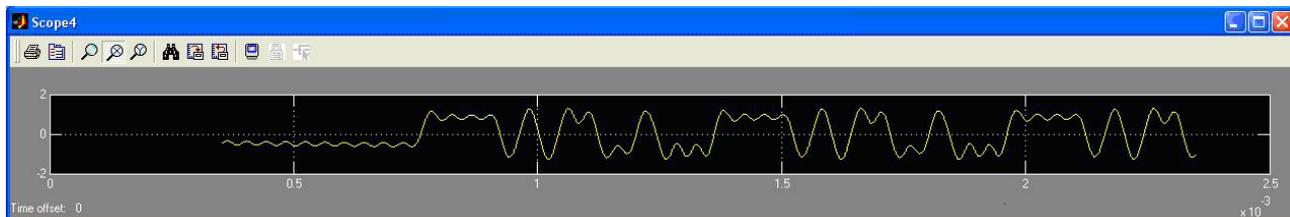
а) исходный полезный сигнал;



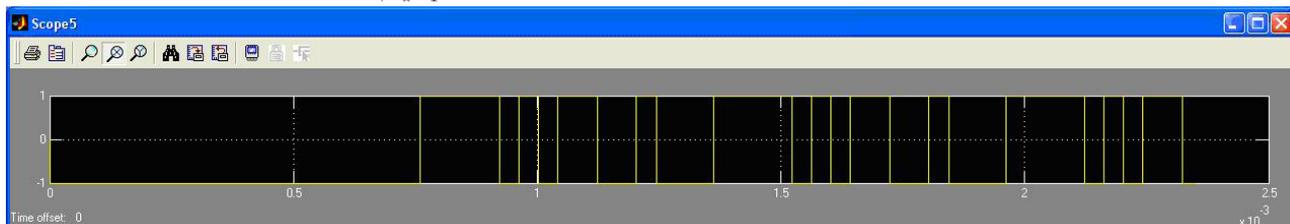
б) форма сигнала после компенсации с задержкой;



в) форма сигнала после фазового детектора;



г) форма сигнала после блока восстановления;



д) полностью восстановленный полезный сигнал

Рис. 6. Формы исходного полезного сигнала

метода подавления широкополосного маскирующего колебания «компенсации с задержкой» происходит искажение первого периода полезной бинарной информации. При вычитании задержанной смеси сигналов из незадержанной невозможно однозначно определить первую группу одинаковых битов первого периода полезной бинарной информации. Восстановление следующих информационных бит первого периода происходит без искажений. Данный недостаток предлагается устранять объявлением первых двух бит «служебными». Комбинация служебных бит может принимать только два значения либо «01», либо «10». Таким образом, при приеме искажаются только эти два бита и полезная информация восстанавливается полностью.

Проведенные эксперименты показали, что для подавления маскирующего сигнала в приемнике достаточно обладать информацией только о периоде данного сигнала. Также в ходе исследования данной схемы было выяснено, что при подавлении сигнала изменение времени задержки менее чем на $\Delta T = \pm 0.000025$ с практически не влияет на эффективность подавления маскирующего сигнала и восстановление полезного сигнала. Таким образом, можно сделать вывод, что защищенность данного способа передачи сигналов напрямую зависит только от значений периодов передаваемых сигналов и дальнейшего повышения скрытности можно добиться путем внесения аperiodичности.

Аperiodичность сигналов может быть достигнута при использовании стеганографических подходов, например, введением преднамеренных искажений как в полезный, так и в маскирующий сигнал, либо нелинейной фильтрацией маскирующего широкополосного колебания при излучении. При этом возможное определение противником несущей частоты маскирующего сигнала и даже закона модуля-

ции не гарантирует достаточную степень подавления этого мощного сигнала без знания секретной искажающей функции. Противоположный характер искажений в приемниках «своей» радиолинии позволит, при реализации метода компенсации маскирующего сигнала, осуществить подавление маскирующего сигнала и однозначно восстановить полезную информацию.

ЗАКЛЮЧЕНИЕ

Проведено компьютерное моделирование системы радиосвязи, обеспечивающей скрытную передачу группы бинарных полезных сигналов. На полученной модели подтверждена работоспособность способа, описанного в [3]. В ходе экспериментов был выявлен ряд недостатков. Во-первых, происходит искажение первого периода полезной бинарной информации, вызванное применением метода компенсации с задержкой. Данный недостаток предлагается устранять путем введения двух служебных бит. Во-вторых, для подавления широкополосного маскирующего колебания достаточно иметь информацию только о его периоде. Для усиления защиты предлагается разрушать периодическую во времени структуру маскирующего сигнала, т.е. при помощи преднамеренных искажений добиваться его аperiodичности.

ЛИТЕРАТУРА

1. Заявка ФРГ № OS 3605350, Н 04 1/02, 1987 г.
2. Кальянов Э.В. Передача информации при использовании кодирования маскирующих хаотических колебаний // Радиотехника и электроника, 2002, т. 47, №4.- С. 469.
3. Патент РФ № 2232475, приоритет 10.04.2003 г., опубл. 10.07.2004 г., БИ № 19.
4. Дьяконов, Вл.. MATLAB. Обработка сигналов и изображений : Спец. справ. / Вл. Дьяконов, И. Абраменкова . — СПб. и др. : Питер, 2002 . — 602 с.

*Статья принята к опубликованию
25 октября 2007 г.*