ИНФОРМАТИКА

2009 **октябрь-декабрь** **№ 4**

ЗАЩИТА ИНФОРМАЦИИ

УДК 004.056:061.68

Н.А. Деев

МАСКИРОВАНИЕ ИНФОРМАЦИИ НА ОСНОВЕ СМЕШИВАНИЯ СИГНАЛА СО СЛУЧАЙНОЙ И ПСЕВДОСЛУЧАЙНОЙ ПОСЛЕДОВАТЕЛЬНОСТЯМИ

Рассматривается маскирование информации, основанное на формировании и обработке смешанного частотно-модулированного сигнала, произведением двоичных последовательностей, одна из которых псевдослучайная с известным законом формирования, другая – случайная, формируемая с помощью источника физического шума и компаратора. За счет этого обеспечивается энергетическая скрытность. Добавление случайной компоненты позволяет избежать регулярности спектральных составляющих.

Введение

Для организации диспетчерской связи между сотрудниками при охране важных объектов, сопровождении специальных грузов, проведении мероприятий по охране общественного порядка широко используются аналоговые радиостанции с частотной модуляцией. При этом часто возникает потребность защиты речевой информации от прослушивания. Как правило, большинству таких пользователей не требуется ее гарантированная защита, достаточно затруднить разборчивость телефонных переговоров, ведущихся по радиостанциям. Оптимальным решением задачи в данном случае может быть использование технических средств, разработанных на основе аналоговых методов смешивания (скремблирования).

Аналоговое скремблирование относится к классу известных методов маскирования связи и применяется практически во всех современных средствах передачи информации. Суть его состоит в преобразовании исходного речевого сигнала с целью минимизации признаков речевого сообщения, в результате которого этот сигнал становится неразборчивым и неузнаваемым. Необходимым условием такого преобразования является возможность обратного преобразования для восстановления речевого сигнала на приемной стороне [1]. При аналоговом скремблировании возможно преобразование речевого сигнала по амплитуде, частоте и времени. Широко используются способы частотного и временного преобразований речевых сигналов и их комбинации. Амплитудные преобразования при скремблировании не применяются из-за проблем точного восстановления амплитуды речевого сигнала при его обработке.

При частотном преобразовании сигнала используются частотная инверсия сигнала (преобразование спектра сигнала с помощью гетеродина и фильтра), разбиение полосы частот речевого сигнала на несколько сегментов и частотная инверсия спектра в каждом сегменте относительно его средней частоты, разбиение частоты речевого сигнала на несколько сегментов и их частотные перестановки. При временных преобразованиях производится разбиение сигнала на речевые сегменты и их перестановка во времени: инверсия по времени сегментов речи, временные перестановки сегментов речевого сигнала. Комбинированные методы преобразования сигнала предполагают использование одновременно нескольких различных способов скремблирования (как частотных, так и временных), число которых ограничивается, как правило, возможностями технической реализации аналоговых скремблеров.

Различие скремблеров состоит в числе частот инверсии, скорости их изменения и количестве ключей, определяющих длительность перебора возможных комбинаций изменяемых параметров без их повторения. Некоторое представление об уровне защиты информации может дать показатель количества ключевых параметров. Для частотного инвертора ключевым параметром является значение частоты инверсии сигнала. Размерность этого параметра, т. е. число

возможных значений частот инверсии (число ключей) с ощутимыми искажениями, возникающими при прослушивании на соседней частоте, не превышает 20–30.

При временных преобразованиях ключевыми параметрами являются длительность сегмента речи, длительность временного отрезка и правило перестановки временных отрезков в сегменте. Различные сочетания значений этих параметров могут дать возможность реализации нескольких сотен ключей.

Уровень защиты при изменениях параметров преобразования во времени (динамической инверсии) определяется количеством градаций параметра сигнала и длиной ключа, т. е. числом возможных комбинаций параметра, скоростью изменения параметра. Возможно использование миллионов ключевых комбинаций.

При аналоговом скремблировании преобразованный речевой сигнал, обладая свойствами неразборчивости и неузнаваемости, занимает такую же полосу частот спектра, как и исходный сигнал. Присутствие при передаче в канале связи фрагментов исходного речевого сообщения, преобразованного в частотной и (или) временной областях, означает, что возможны перехват и анализ передаваемой информации на уровне звуковых сигналов. Перехват сообщений возможен при применении специальных средств, позволяющих сначала определить ключевую последовательность (т. е. правила изменения параметров преобразования сигнала), а затем подстроиться под найденную ключевую последовательность [2].

Несмотря на высокое качество и разборчивость восстанавливаемой речи, аналоговые скремблеры могут обеспечивать в основном лишь низкий или средний (по сравнению с цифровыми системами) уровень защиты информации, однако их практическая реализация проще и дешевле.

Цифровое скремблирование предполагает дискретизацию исходного аналогового сигнала и передачу его основных компонент путем преобразования их в цифровой поток данных, который смешивается с некоторой псевдослучайной последовательностью, вырабатываемой ключевым генератором по одному из криптографических алгоритмов. Полученное таким образом сообщение с помощью модема передается в канал связи, на приемной стороне производятся обратные преобразования с целью получения открытого речевого сигнала. Реализация цифрового скремблирования на практике оказывается довольно сложной и дорогостоящей.

Основными характеристиками скремблирования являются уровень защиты информации, остаточная разборчивость и качество восстановления сигнала, сложность реализации. Сравнительный анализ характеристик методов аналогового и цифрового скремблирования достаточно подробно описан в литературе [6, 7].

В статье рассматривается защита информации от перехвата за счет увеличения энергетической скрытности канала связи. Классический метод повышения энергетической скрытности за счет снижения спектральной плотности энергии модулирующего сигнала путем расширения его спектра с последующей угловой модуляцией имеет слабое место – характерный колоколообразный спектр сигнала в канале. Этот спектр легко фиксируется средствами радиообнаружения. Если бы спектр сигнала в канале был подобен спектру белого шума, то установить факт сеанса связи было бы трудно. Сформировать такой спектр скремблированного частотно-модулированного сигнала, содержащего речевое сообщение, можно произведением двоичных последовательностей, одна из которых псевдослучайная с известным законом формирования, другая – случайная, формируемая с помощью источника физического шума и компаратора. Особенность предлагаемого скремблирования состоит в том, что кроме энергетической скрытности обеспечивается апериодичность результирующей двоичной скремблирующей последовательности. Добавление случайной компоненты позволяет избежать регулярности спектральных составляющих и тем самым увеличить число ключевых комбинаций. В приемном устройстве осуществляется свертка спектра сигнала за счет его перемножения на синхронизированную псевдослучайную последовательность. Случайная фазовая манипуляция частотно-модулированного сигнала снимается операцией возведения в квадрат.

Согласно основным характеристикам (уровню защиты информации, стоимости и сложности реализации) рассмотренный в статье способ, основанный на скремблировании аналогового частотно-модулированного сигнала псевдослучайной последовательностью, является предпочтительным для использования в системах конвенциальной радиосвязи.

1. Формирование скремблированного частотно-модулированного сигнала

Смешивание частотно-модулированного сигнала с псевдослучайной двоичной последовательностью генератора псевдослучайных чисел является наиболее распространенным способом аналогового скремблирования. В качестве аппаратных реализаций скремблирования часто используют генератор случайных чисел на сдвиговом регистре с линейной обратной связью. Такая технология маскирования информации является достаточно эффективной. Показателем эффективности здесь служит количество операций, затрачиваемых на вычисление очередного элемента псевдослучайной последовательности. Однако остается вероятность несанкционированного доступа к информации при применении специальных средств определения ключевой последовательности и подстройки под найденную ключевую последовательность.

Предлагаемое в статье формирование скремблированного частотно-модулированного сигнала, содержащего речевое сообщение, произведением двоичных последовательностей (псевдослучайной с известным законом формирования и случайной, формируемой с помощью источника физического шума и компаратора) обеспечивает высокую энергетическую скрытность. Это обусловлено тем, что, во-первых, данная технология не имеет пороговых ограничений по помехоустойчивости и позволяет работать «под шумами», а во-вторых, спектр сигнала в канале не имеет характерных ярко выраженных участков. Добавление случайной компоненты позволяет избежать регулярности спектральных составляющих и тем самым увеличивает число ключевых комбинаций до бесконечности.

На передающей стороне сигнал формируется в соответствии со схемой, приведенной на рис. 1.

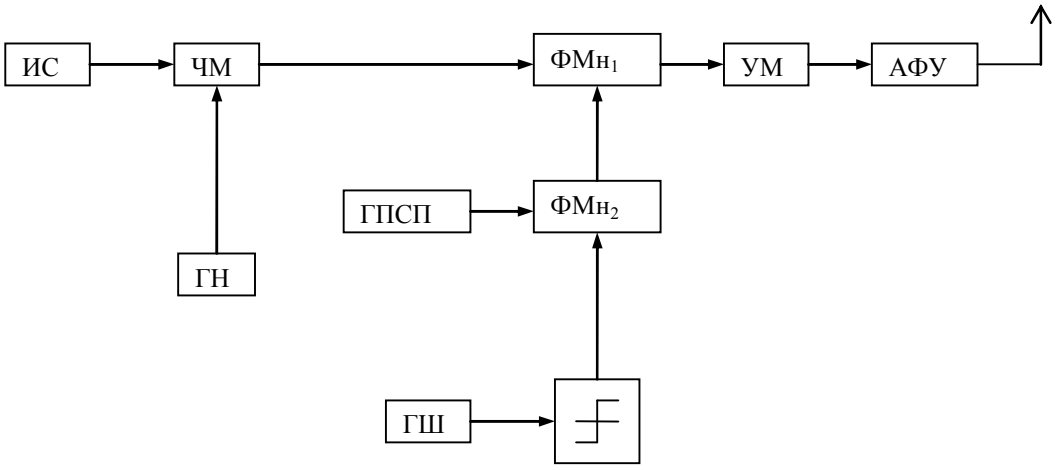

Рис. 1. Структурная схема формирования скремблированного сигнала

Источник речевого сообщения (ИС) аналогового сигнала $\lambda(t)$ формирует низкочастотный сигнал. Генератор несущей частоты (ГН) обеспечивает формирование высокочастотного узкополосного несущего сигнала. В частотном модуляторе (ЧМ) аналоговый сигнал и несущий перемножаются. Сформированный узкополосный частотно-модулированный сигнал поступает на вход фазового манипулятора $ФМн_1$ и подвергается фазовой манипуляции двоичной последовательностью, представляющей комбинацию псевдослучайной двоичной последовательности (ПСП) $g(t-\tau)=\{\pm1\}$ и случайной двоичной последовательности $X(t)=\{\pm1\}$, где τ – случайная задержка. ПСП $g(t-\tau)$ вырабатывается в генераторе ГПСП. Одновременно с ПСП на фазовый манипулятор $ФМн_2$ подается случайная последовательность $X(t)$, вырабатываемая в генераторе ГШ и преобразованная в компараторе в клиппированный шум. На фазовом манипуляторе $ФМн_2$ осуществляется операция перемножения $g(t-\tau)$ и $X(t)$ и образуется двоичная скремблирующая последовательность

$$Y(t-\tau)=g(t-\tau)\cdot X(t). \qquad (1)$$

Здесь полоса спектра последовательности $X(t)$ определяется тактовой частотой $f_T = 1/\tau_Э$, где $\tau_Э$ – длительность элемента ПСП, а также формирующим фильтром, включенным в ГШ.

Сформированный скремблированный частотно-модулированный сигнал, полученный в результате перемножения в $ФМн_1$, усиливается в усилителе мощности (УМ), подается в модуль антенно-фидерного устройства (АФУ) и далее в эфир.

Скремблированный частотно-модулированный сигнал можно представить в виде

$$S(t) = a_0 Y(t-\tau)\cdot\cos[(\omega_0 t + \Psi(t)) + \beta], \tag{2}$$

где a_0 и ω_0 – известные амплитуда и частота сигнала;

$Y(t) = g(t-\tau)\cdot X(t) = \{\pm 1\}$ – скремблирующая последовательность;

β – случайная начальная фаза, равномерно распределенная в интервале $[0,2\pi]$;

$\Psi(t)$ – частота сигнала, медленно изменяющаяся в соответствии с передаваемым сообщением $\lambda(t)$, где $\lambda(t) = d\Psi(t)/dt$.

2. Алгоритм и структурная схема обработки скремблированного частотно-модулированного сигнала

Смесь сигнала и помехи, принимаемую на входе устройства обработки частотно-модулированного сигнала, можно представить как

$$r(t) = S(t) + n(t), \tag{3}$$

где $S(t)$ – скремблированный частотно-модулированный сигнал; $n(t)$ – помеха, представляющая белый гауссовский шум.

Алгоритм оптимального приема сигнала на фоне помехи сводится к определению уравнений для текущих оценок информационного параметра $\lambda^*(t)$ и параметра задержки $\tau^*(t)$ скремблированного сигнала. Эти уравнения для случая некогерентной обработки сигнала имеют следующий вид [4]:

$$\frac{d\lambda^*(t)}{dt} = -\alpha\lambda^*(t) + \sigma_\lambda^2 \cdot k_0 \frac{\partial L(\tau^*,\lambda^*)}{\partial \lambda^*}; \tag{4}$$

$$\frac{d\tau^*(t)}{dt} = \sigma_\tau^2 \cdot k_0 \frac{\partial L(\tau^*,\lambda^*)}{\partial \tau^*}, \tag{5}$$

где $\lambda^*(t)$ – оценка сообщения, содержащегося в сигнале; α – коэффициент, характеризующий ширину спектра сообщения; $\tau^*(t)$ – оценка задержки скремблирующей последовательности; σ_λ^2 и σ_τ^2 – апостериорные стационарные дисперсии оценок соответствующих параметров; $k_0 = 1/\Delta$ – коэффициент, определяемый временем корреляции Δ сигнала.

Функция $L(\tau^*,\lambda^*)$ в случае слабого (по отношению к помехе) сигнала определяется выражением

$$L(\tau^*,\lambda^*) = \left[\int_{t-\Delta}^{t} r(t)\cdot g(t-\tau^*)\cdot \mathrm{X}^*(t)\exp\left[-j(\omega_0+\lambda^*)t\right]dt\right]^2, \tag{6}$$

где $g(t-\tau^*)$ – синхронизированная псевдослучайная последовательность; $X^*(t)$ – апостериорная оценка случайной последовательности.

В соответствии с уравнениями (4)–(6) построена структурная схема обработки скремблированного частотно-модулированного сигнала (рис. 2).

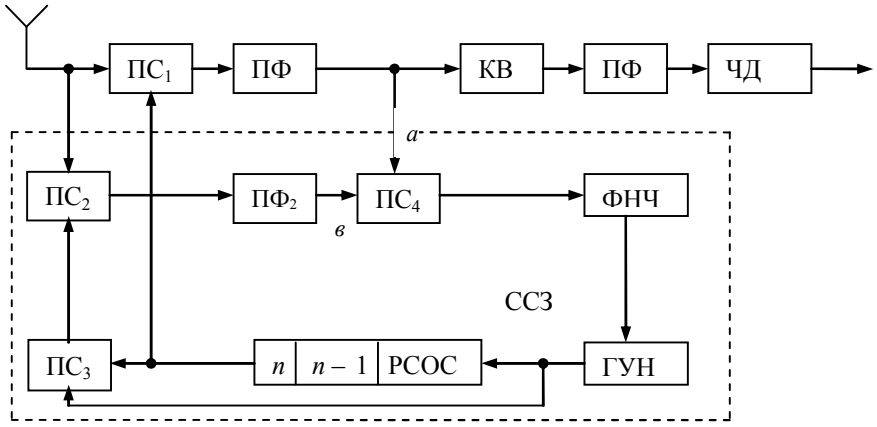

Рис. 2. Схема обработки скремблированного сигнала

Схема устройства обработки скремблированного частотно-модулированного сигнала состоит из перемножителей сигналов $ПС_1$ – $ПС_4$; полосовых фильтров $ПФ_1$ – $ПФ_3$; регистра сдвига с обратной связью (РСОС); фильтра нижних частот (ФНЧ); генератора, управляемого напряжением (ГУН); квадратора (КВ); частотного детектора (ЧД).

Операция дифференцирования по τ^* в уравнении (5) реализуется за счет формирования на входе $ПС_2$ последовательности типа «Манчестер»:

$$M(t) = g(t - \tau^*) \cdot m(t - \tau^*). \qquad (7)$$

В этом выражении меандр колебаний тактовой частоты $m(t)$ и ПСП $g(t - \tau^*)$ перемножаются в $ПС_3$.

Схема слежения за задержкой (ССЗ) обеспечивает управление ГУН и осуществляет квазикогерентную обработку фазоманипулированного частотно-модулированного сигнала за счет перемножения в $ПС_4$ сигналов с выходов прямого $ПС_1$ и дифференциального $ПС_2$ каналов. КВ в цепи ЧД обеспечивает снятие фазовой манипуляции с частотно-модулированного сигнала и последующее детектирование в частотном детекторе.

В отличие от известных технических решений в данном случае работоспособность ССЗ обеспечивается за счет снятия случайной фазовой манипуляции в $ПС_4$. Случайная последовательность, выделенная полосовым фильтром $ПФ_1$, подается на вход (*а*) $ПС_4$. Выделение частотно-модулированного сигнала осуществляется после КВ, который снимает случайную фазовую манипуляцию. $ПФ_3$ и ЧД настроены на вторую гармонику частотно-модулированного сигнала.

3. Моделирование маскирования информации в среде MATLAB Simulink

Моделирование маскирования информации на основе скремблирования частотно-модулированного сигнала произведением двоичных последовательностей (псевдослучайной с известным законом формирования и случайной, формируемой с помощью источника физического шума) проведено в среде MATLAB Simulink (рис. 3).

Результаты компьютерного моделирования представлены на рис. 4–9. На рис. 4 изображена информационная последовательность, модулирующая частоту радиосигнала, спектр которого показан на рис. 5. При скремблировании частотно-модулированного сигнала произведением ПСП и клиппированного шума спектр расширяется (рис. 6 и 7).

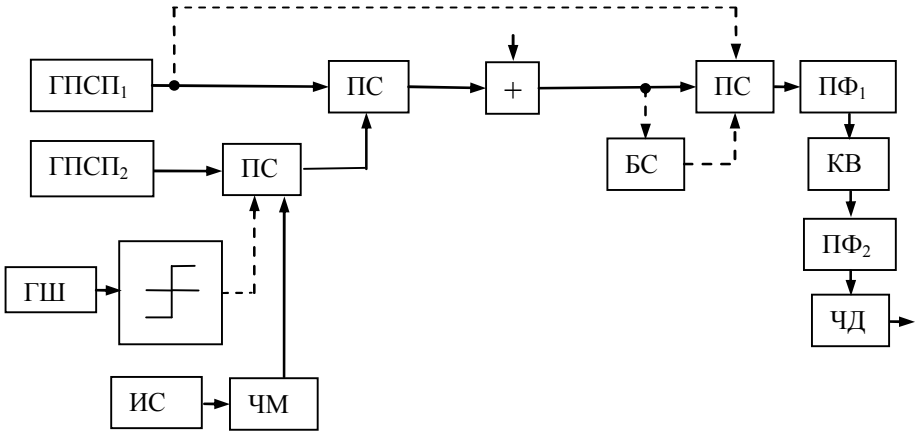

Рис. 3. Структурная схема модели формирования и обработки скремблированного частотно-модулированного сигнала псевдослучайной и шумовой последовательностями: ГШ – генератор гауссовского шума; + – сумматор сигналов и шума; БС – блок синхронизации

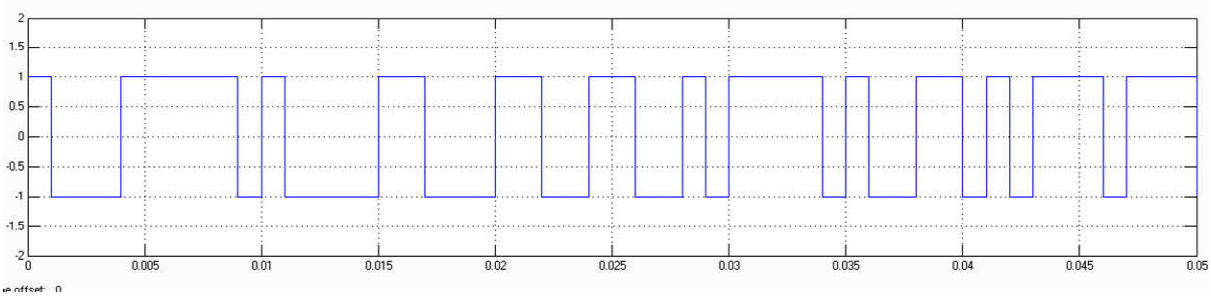

Рис. 4. Информационная последовательность

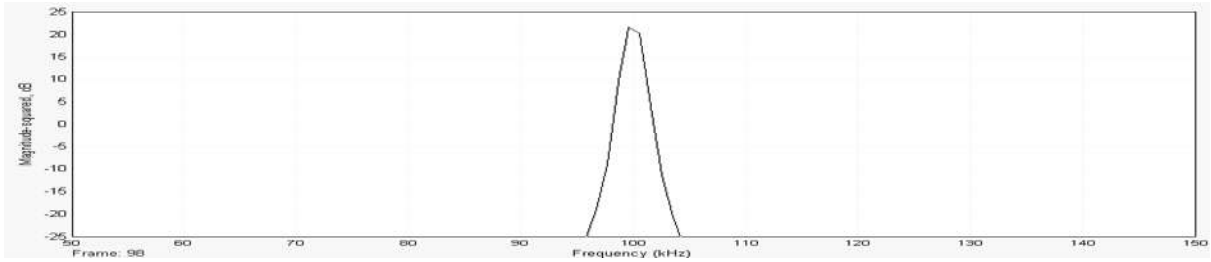

Рис. 5. Спектр сигнала на выходе ЧМ

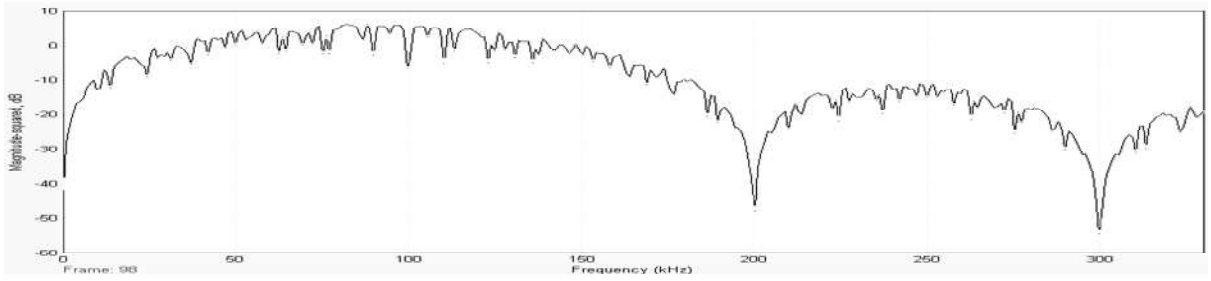

Рис. 6. Спектр сигнала, скремблированного двумя ПСП

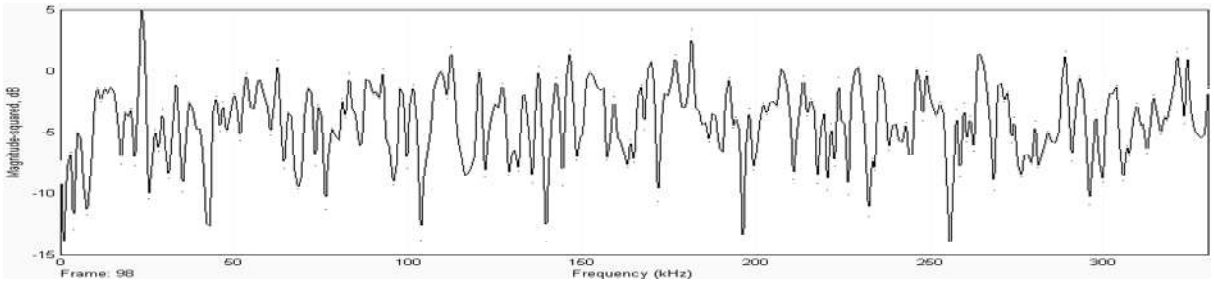

Рис. 7. Спектр сигнала, скремблированного ПСП и шумовой последовательностью

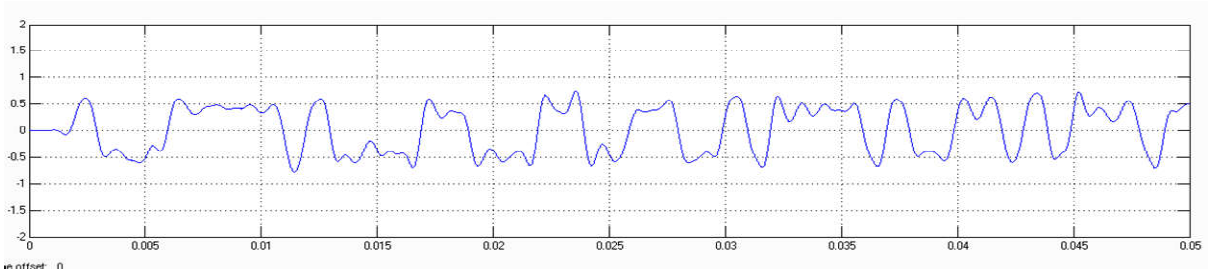

Рис. 8. Информационная последовательность, выделенная на выходе ЧД
(скремблирование двумя ПСП)

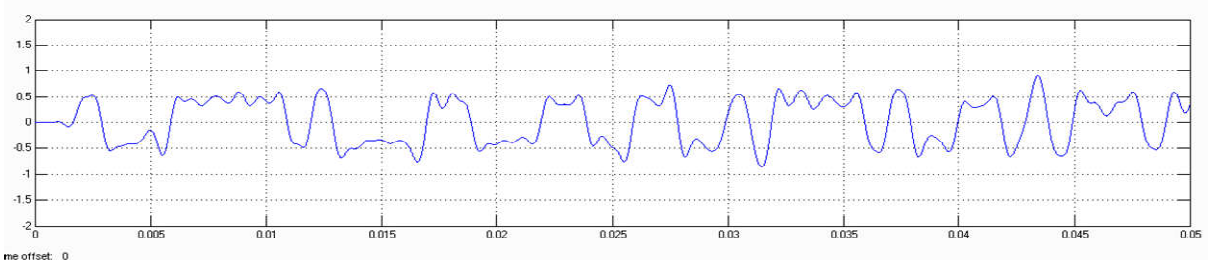

Рис. 9. Информационная последовательность, выделенная на выходе ЧД
(скремблирование ПСП и шумовой последовательностью)

Результат компьютерного моделирования разработанных алгоритмов (рис. 7), подтверждает энергетическую скрытность сигнала, а отсутствие регулярности спектральных составляющих в скремблированном частотно-модулированном сигнале – его структурную скрытность. Форма сигнала на выходе ЧД (рис. 8 и 9) подтверждает качественное выделение информационной последовательности.

Для оценки качества выделения сообщения при скремблировании частотно-модулированного сигнала используется вероятность P_e ошибки воспроизведения элемента информационной последовательности. Эта вероятность определяется отношением сигнал/шум q_2 на выходе $\Pi\Phi_2$. Для некогерентного приема частотно-модулированного сигнала вероятность ошибки воспроизведения элемента информационной последовательности составляет [8]

$$P_e = 0{,}5\ exp[-q_2/4]. \tag{8}$$

Отношение сигнал/шум q_2 определяется отношением сигнал/шум q_1 на выходе $\Pi\Phi_1$ и полосой $\Delta f_{чм}$ скремблированного частотно-модулированного сигнала:

$$q_2 = \frac{q_1^2}{1+2q_1} \cdot \frac{\Delta f_1}{\Delta f_{пф_2}} \approx \frac{1}{2} q_1 \cdot \frac{\Delta f_1}{\Delta f_{пф_2}}. \tag{9}$$

Полоса пропускания полосового фильтра $ПФ_2$ согласована со спектром частотно-модулированного сигнала $\Delta f_{пф2} \approx \Delta f_{чм}$. В свою очередь,

$$q_1 = q_{вх} \cdot \frac{\Delta f}{\Delta f_1}, \tag{10}$$

где $\Delta f_1 = 1/\tau_{кор}$ – полоса пропускания полосового фильтра $ПФ_1$; $\tau_{кор}$ – время корреляции процесса X(t); $\Delta f = 1/\tau_э$ – ширина спектра скремблированного сигнала; $\tau_Э$ – длительность элемента ПСП.

Полоса спектра ПСП значительно больше полосы спектра шумовой последовательности. При обработке обеспечивается корреляционная свертка спектра скремблированного сигнала до полосы шумовой последовательности. Отношение сигнал/шум в этой полосе в N раз больше, чем на входе. Таким образом, на входе КВ, снимающего с частотно-модулированного сигнала скремблирующую шумовую последовательность, спектр имеет такую же полосу, как у исходного частотно-модулированного сигнала. Требуемая вероятность ошибки $P_e < 10^{-5}$ обеспечивается при $q_{вх} < 1$, если $\Delta f >> \Delta f_{чм}$.

Заключение

В статье рассмотрены алгоритмы формирования и обработки широкополосных сигналов, отличающиеся от известных применением случайной и псевдослучайной скремблирующих последовательностей.

За счет существенной разницы полос скремблированного и исходного частотно-модулированного сигналов для требуемой достоверности приема может быть допущено отношение сигнал/шум в полосе скремблированного сигнала $q_{вх} << 1$ и обеспечена высокая энергетическая скрытность системы передачи информации.

Список литературы

1. Torrieri, D.J. Priciples of secure communication systems / D.J. Torrieri. – Dedham : Artech House Inc., 1981. – 306 p.

2. Овчинников, А.М. Устройства защиты информации для средств УКВ-радиосвязи / А.М. Овчинников, А.С. Лазин // Специальная техника. – 1998. – № 3. – С. 27–30.

3. Чекатков, А.А. Методы и средства защиты информации / А.А. Чекатков, В.А. Хорошко. – М. : Юниор, 2003. – 594 с.

4. Тихонов, В.И. Оптимальный прием сигналов / В.И. Тихонов. – М. : Радио и связь, 1983. – 512 с.

5. Варакин, Л.Е. Системы связи с шумоподобными сигналами / Л.Е. Варакин. – М. : Радио и связь, 1985. – 384 с.

6. Деев, Н.А. Широкополосная система связи с подавителем комплекса помех / Н.А. Деев, Я.Б. Кусык // Известия Белорусской инженерной академии. – 2002. – № 2. – С. 7–8.

7. Чердынцев, В.А. Проблемы защиты информации в каналах радиосвязи / В.А. Чердынцев, Н.А. Деев // Докл. Второй Белорусско-российской науч.-техн. конф. «Технические средства защиты информации». – Минск : БГУИР, 2004. – С. 51–54.

8. Чердынцев, В.А. Радиотехнические сигналы / В.А. Чердынцев. – Минск : Вышэйшая шк., 1988. – 369 с.

Поступила 16.04.09

Объединенный институт проблем информатики НАН Беларуси,
Минск, Сурганова ,6
e-mail: dna@newman.bas-net.by

N.A. Deev

INFORMATION MASKING ON THE BASIS OF SIGNAL SCRAMBLING BY RANDOM AND PSEUDO-RANDOM SEQUENCES

The information masking on the basis of generating and processing the scrambled frequency modulated signals by way of multiplication of two binary sequences is considered. The first sequence employed is the pseudorandom one with known rule of generation, the second one is random sequence generated with the help of physical random noise generator and a comparator which provides the energetic security. It is shown that adding random components allow avoiding regularity of spectral components.