

УДК 621.391

Передача информации сигналами с расширенным спектром и самокодированием

Transmission of information by self-encoded spread spectrum signals

Биккенин Р. / Vikkenin R.

Рафаэль Рифгатович

(tosir@sut.ru)

доктор технических наук, профессор, заслуженный работник высшей школы РФ. ФГБОУ ВО «Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича» (СПбГУТ), профессор кафедры теоретических основ телекоммуникаций. г. Санкт-Петербург

Макаров И. / Makarov I.

Игорь Викторович

(vas7559@yandex.ru)

кандидат технических наук.

СПбГУТ,

преподаватель кафедры теоретических основ телекоммуникаций. г. Санкт-Петербург

Ключевые слова: сигнал с расширенным спектром – the spread spectrum signal; self-encoded spread spectrum communication – связь с расширенным спектром и самокодированием; демодуляция – demodulation; помеха, похожая на сигнал – similar to signal interference.

Предложена процедура формирования сигналов с расширенным спектром путем самокодирования. Показано, что это позволяет повысить безопасность и помехозащищенность передачи данных в условиях помех, похожих на сигнал, когда помеха имеет энергетическое превосходство над сигналом. Найдено выражение для вероятности ошибки, позволяющее оценить помехоустойчивость приема в условиях действия названных помех. Указана перспектива применения полученных результатов в теории и практике совершенствования систем передачи информации.

A procedure for generating self-encoded spread spectrum signals is proposed. It is shown that this makes it possible to increase the safety and noise immunity of data transmission in conditions of interference similar to a signal, when the interference has an energy superiority over the signal. An expression has been found for the error probability, which makes it possible to evaluate the noise immunity of reception under the conditions of the named interference.

The prospect of applying the results obtained in the theory and practice of improving information transmission systems is indicated.

Введение

В настоящее время в ряде систем передачи информации успешно применяются сигналы с расширенным спектром (spread-spectrum, SS), которые в отечественных и иностранных источниках называют шумоподобными

или псевдослучайными [1–4]. Так, в системах семейства стандартов IEEE 802.11 реализован метод расширения спектра на основе «прямой последовательности» (direct sequencing, DS) при использовании последовательностей Баркера. В других системах телекоммуникаций для расширения спектра сигналов применяют псевдослучайные (псевдошумовые) последовательности (ПСП), формируемые с помощью последовательностей максимальной длины (M-последовательностей) либо связанных с ними последовательностями Голда и др. [1–3].

Сигналы с расширенным спектром, обладающие определенной скрытностью и помехозащищенностью в условиях сосредоточенных по спектру (преднамеренных) помех с энергетикой, превышающей сигнал, первоначально применялись в системах связи военного назначения. В настоящее время они находят широкое применение в ряде иных систем передачи информации, в том числе в спутниковой связи, в WiFi, в системах связи с беспилотными летательными аппаратами (БПЛА), в сотовой связи на основе стандартов CDMA (Code Division Multiple Access – множественный доступ с кодовым разделением), поскольку они также способны обеспечивать разделение сигналов по форме и структуре, что позволяет реализовать одновременное функционирование множества абонентов в общей полосе частот и обеспечивать защиту от внутрисистемных и преднамеренных помех.

Названные выше последовательности обладают свойствами, подобными случайным (стохастическим), но на самом деле являются детерминированными, так как формируются посредством известных сдвиговых регистров с обратными связями [1–3]. И здесь имеет место серьезная проблема: по сегменту (отрезку) такой последовательности, равному удвоенному числу ячеек памяти в регистре-формирователе псевдослучайного сигнала, можно восстановить всю

псевдослучайную последовательность, используемую для расширения исходного сигнала [5]. В результате нарушается скрытность шумоподобных сигналов, и они становятся доступными для воздействия на них преднамеренных помех, безопасность передачи сигналов и содержащейся в них информации становится невозможной.

Для обеспечения необходимой скрытности и безопасности передачи сигналов с расширенным спектром можно воспользоваться методом так называемого самокодирования, который впервые был описан в [6] и получил дальнейшее развитие в последующих работах автора данной публикации.

В [6] предложено полностью отказаться от генераторов псевдослучайных последовательностей. Вместо этого для расширения спектра сигнала предлагается применять последовательности посылок, вырабатываемых самим источником цифровой информации, т. е. реализовать самокодирование. Стохастичность появления посылок на выходе источника дискретных (цифровых) сигналов при самокодировании может быть обеспечена соответствующими методами шифрования данных [6]. В результате последовательность двоичных посылок, применяемая для расширения спектра сигнала, после шифрования становится практически случайной, ее посылки будут независимыми друг от друга и появляются с вероятностью $1/2$, что соответствует закону распределения случайных величин Бернулли. Иными словами, расширяющая последовательность в течение сеанса связи не будет повторяться, что и позволит обеспечивать скрытность и безопасность передачи данных в условиях действия специально создаваемых преднамеренных помех.

Кроме того, реализация расширения спектра сигналов методом самокодирования автоматически снимает проблему специальной рассылки абонентам и наличия у них одинаковых исходных ключевых данных на передающей и приемной сторонах для синхронного формирования расширяющих псевдослучайных последовательностей и обеспечение их недоступности (секретности) для посторонних лиц. В отличие от этого, если в классической системе с расширенным спектром при помощи ПСП секрет-

ность ключевых данных не обеспечена, то на передаче и приеме невозможно формировать идентичные псевдослучайные последовательности, и о свертке расширенного спектра сигнала не может быть и речи.

В настоящее время в ряде систем цифровой передачи данных применяется шифрование информации. К их числу принадлежат и системы сотовой связи, реализованные на основе стандарта GSM, услугами которой пользуются абоненты через операторов компаний «Мегафон», «Билайн», «МТС», «Теле-2» и др. Поэтому далее будем полагать, что источник сигналов (информации) вырабатывает (после шифрования) практически случайную последовательность двоичных посылок.

На приемной стороне при обработке поступающих сигналов с расширенным спектром процедура сжатия, обратная расширению, реализуется подобным образом. С этой целью принимаемые двоичные посылки используются в составе последовательности, управляющей процедурой восстановления данных [6].

При формировании псевдослучайных (шумоподобных) сигналов с расширенным спектром в настоящее время, как правило, применяются фазовые методы модуляции [3,8], в частности, относительная фазовая модуляция (ОФМ), в иностранной литературе именуемая differential phase shift Keying (DPSK). В настоящей работе также будем рассматривать этот вид модуляции.

На рис. 1 представлена обобщенная структурная схема системы передачи дискретных сигналов с расширенным путем самокодирования спектром.

Сформированная источником сообщений (ИС) после соответствующего шифрования случайная последовательность двоичных посылок подается на вход перемножителя передачи (ПП) и одновременно в регистр сдвига (РС) с заданной скоростью. По управляющему (тактовому) сигналу содержимое каждой ячейки переписывается в следующую по порядку ячейку памяти. Далее с помощью мультиплексора (МП) осуществляется последовательное считывание посылок сигнала с выходов каждой очередной ячейки памяти. Мультиплексор, выполняющий роль коммутатора, поочередно подключает все входы к одному выходу. При этом

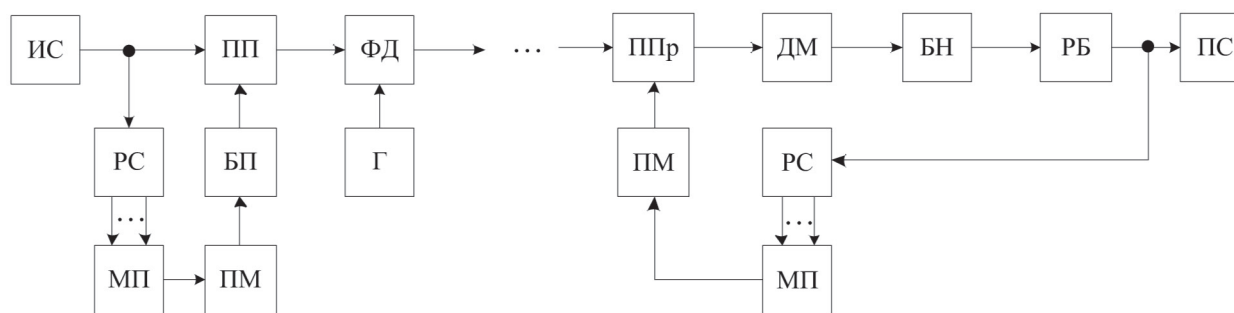


Рис. 1. Структурная схема системы с расширенным спектром и самокодированием

скорость считывания информационных посылок сигнала с регистра сдвига задается больше, чем скорость поступления управляющих (тактовых) сигналов в n раз. В результате на каждую информационную посылку от источника сообщений будет приходиться n коротких посылок, сформированных при помощи мультиплексора. Эти посылки далее будем называть «чипами».

Последовательность «чипов» затем поступает в перемежитель (ПМ), где осуществляется их перемеживание (перемежение), что приводит к равномерному и независимому друг от друга распределению «чипов» в расширяющей последовательности. В перемежитель «чипы» записываются по столбцам, а считываются по строкам из двумерного массива данных. Таким образом обеспечивается формирование случайной расширяющей последовательности посылок, что и позволяет обеспечить скрытность и безопасность передачи данных при действии преднамеренных помех.

С выхода перемежителя (ПМ) «чипы» со скоростью, в n раз большей скорости передачи информационных посылок от источника (ИС), поступают на блок перекодирования (БП) относительной фазовой модуляции. Здесь в соответствии с правилом ОФМ осуществляется перекодирование. При появлении каждого очередного нулевого «чипа» его полярность сохраняется, с появлением каждого очередного единичного «чипа» его полярность изменяется на противоположную. Далее эти «чипы» со скоростью, в n раз

больше информационной скорости передачи данных, подаются на второй вход перемножителя передачи (ПП), таким образом на одну информационную посылку будет приходиться n «чипов».

В результате в момент поступления в перемножитель информационной посылки сигнала от источника сообщений будет формироваться шумоподобный (практически случайный) сигнал. Иными словами, происходит расширение спектра исходного сигнала вследствие преобразования каждой очередной информационной посылки сигнала в совокупность n «чипов», при этом длительность каждого из них в n раз меньше длительности исходного информационного сигнала, т. е. $T_c = T_i / n$, где T_c – длительность «чипа», T_i – длительность исходной информационной посылки сигнала, выдаваемой источником сообщений (ИС). Величина n будет называться базой сформированного сложного сигнала с расширенным спектром.

После прохождения фазового модулятора (ФМ), на который одновременно подается несущее колебание от генератора (Г), образуется последовательность посылок сигнала с относительной фазовой модуляцией (ОФМ) и с расширенным спектром. При этом реализуется равномерность и независимость появления очередной посылки от предыдущих посылок сигнала, что и будет обеспечивать более высокую скрытность и безопасность передачи сигналов по сравнению с существующими системами с расширенным спектром.

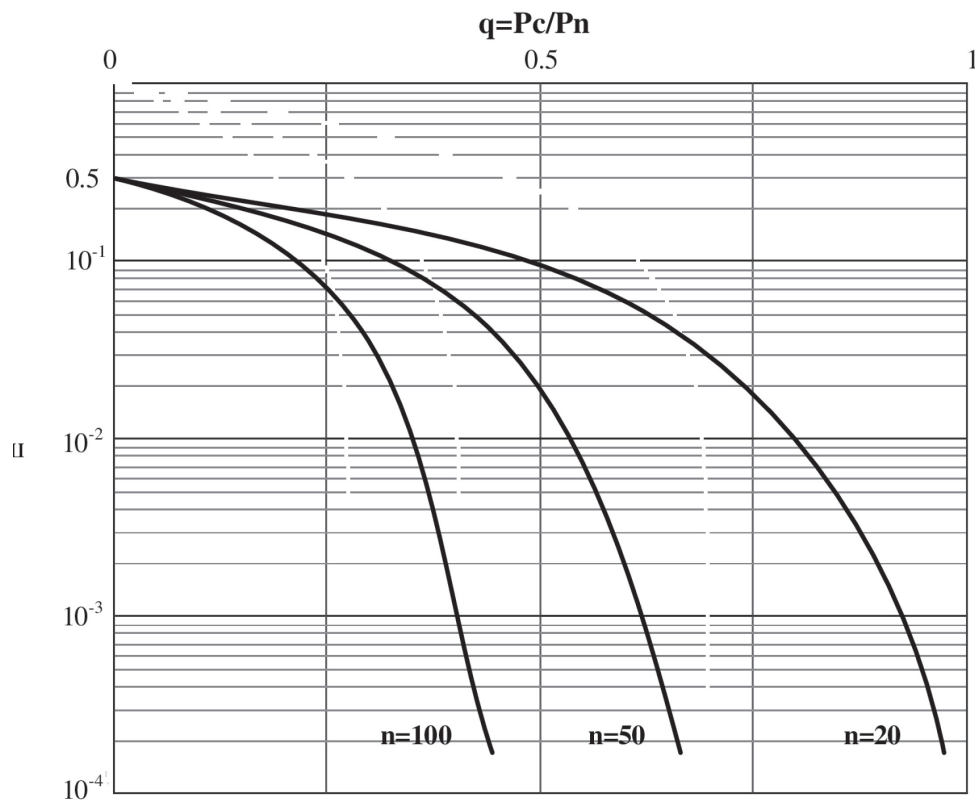


Рис. 2. Зависимости вероятностей ошибок в системе с расширенным спектром и самокодированием

Таким образом, на передающей стороне формируются сигналы вида

$$S(t) = U_c \sum_{k=1}^n \pi_k(t) \text{rect}(t - (k-1)T) \sin[\omega t + \varphi_c], \quad (1)$$

где $\text{rect}(t - (k-1)T)$ – единичный импульс фиксированной длительности $T_c = T_n / n$, который определяет временной интервал каждого очередного «чипа» сложного псевдослучайного ОФМ сигнала,

$$\pi_k(t) = \begin{cases} (-1)^{\varepsilon_k}, & t \in [(k-1)T_n, kT_n], \quad k = \overline{1, n} \\ 0, & t \notin [(k-1)T_n, kT_n], \end{cases}$$

$\varepsilon_k \in \{0, 1\}$ – дискретная величина, связанная с k -м элементом расширяющей последовательности, поступающей на второй вход перемножителя (ПП), при этом $\varepsilon_k = \varepsilon_{k-1} \oplus \gamma_k$, в соответствии с правилом перекодирования ОФМ ($\gamma_k \in \{0, 1\}$ – последовательность «чипов» сигнала на выходе блока перекодирования ОФМ).

Псевдослучайность сигнала здесь понимается в том смысле, что расширяющая спектр сигнала последовательность «чипов» должна быть известна на приемной стороне, в противном случае не может быть восстановления исходного сигнала. Постороннему (незаконному) наблюдателю (противнику) передаваемый сигнал должен представляться как чисто случайный вследствие его неповторяемости в течение сеанса передачи данных.

На приемной стороне аддитивная смесь поступающего сигнала с помехами перемножается в перемножителе приема (ППр) на сформированную в приемнике после прохождения через регистр сдвига (РС), мультиплексор (МП) и перемежитель (ПМ) последовательность «чипов», аналогичную расширяющей последовательности на передаче. В результате с принимаемого сигнала снимается расширяющая последовательность, и он вновь будет представлять собой информационный сигнал в виде посылок «0» или «1», часть элементов которого искажены помехой.

Поскольку постановщик помех не владеет знаниями о законе изменения расширяющей последовательности, накладываемой на сигнал на передаче, то он может воздействовать помехой только наугад с целью нарушения процесса передачи сигналов. Поэтому в результате совместных преобразований с сигналом преднамеренная помеха принимает вид, подобный естественному шуму канала связи, т. е. становится практически случайным (стохастическим) процессом.

Дальнейшие преобразования сигнала на приеме производятся любым известным методом, в частности, это может быть некогерентная обработка в корреляционном ОФМ демодуляторе (ДМ), на выходе которого включен блок накопления (БН) информационной посылки, состоящей из n «чипов». Для окончательной регистрации в решающем блоке (РБ) принимаемый сигнал сравнивается с заданной пороговой

величиной. При превышении порога регистрируется сигнал, соответствующий информационному символу «0», в противном случае принимается решение о приеме информационного сигнала «1». Принятый сигнал далее поступает к получателю сообщений (ПС).

Одновременно с принятием решения о регистрации очередной информационной посылки по цепи обратной связи текущая посылка подается во входную часть приемного устройства, последовательно проходя, как и на передаче, регистр сдвига (РС), мультиплексор (МП) и перемежитель (ПМ). Иными словами, методом самокодирования на приеме по аналогии с передающей стороной формируется последовательность «чипов», с помощью которой осуществляется «свертка» сигнала с расширенным спектром.

Оценим теперь степень повышения безопасности и помехоустойчивости системы с расширенным спектром и самокодированием в условиях действия организованных преднамеренных помех, имеющих структуру, похожую на сигнал, и превышающих их по мощности.

Будем полагать, что на передающей стороне формируются сигналы вида (1), а преднамеренная помеха может быть представлена выражением, которое похоже на сигнал (1)

$$N(t) = U_n (-1)^{\delta} \sin(\omega t + \varphi_n), \quad (2)$$

где $\delta \in \{0, 1\}$ – равновероятные и взаимонезависимые случайные величины, определяющие дискретную фазовую модуляцию помехи.

В [7] показано, что для дискретных фазомодулированных сигналов оптимальной преднамеренной помехой является также дискретное фазомодулированное колебание, частота и длительность посылок которого совпадают с аналогичными параметрами сигнала. При противофазной и более мощной помехе в демодуляторе она и будет регистрировать ее вместо передаваемого сигнала. Выражение (2) как раз и соответствует названному условию, т. е. помеха по форме напоминает сигнал, но закон ее формирования отличается от сигнала вследствие применения для его генерирования расширяющей последовательности, вырабатываемой методом саморасширения.

Пусть в ОФМ-демодуляторе, который можно синтезировать на основе правила максимального правдоподобия, реализуется следующая процедура обработки сигнала с расширенным спектром [8]

$$\text{sign } \lambda = \text{sign} \sum_{k=1}^n (-1)^{\gamma_k} (X_k X_{k-1} + Y_k Y_{k-1}), \quad (3)$$

где

$$X_{k-1} = \int_{(k-1)T}^{kT} z(t) \cos \omega t dt, \quad X_k = \int_{kT}^{(k+1)T} z(t) \cos \omega t dt, \\ Y_{k-1} = \int_{(k-1)T}^{kT} z(t) \sin \omega t dt, \quad Y_k = \int_{kT}^{(k+1)T} z(t) \sin \omega t dt,$$

sign λ означает определение полярности величины выходного информационного сигнала, если $\lambda > 0$, то регистрируется информационная посылка «0», при $\lambda < 0$ – посылка «1», $z(t)$ – аддитивная смесь сигнала и помехи на очередном «чипе».

После подстановки значений компонент сигнала (1) и помехи (2) в выражение (3) и преобразований получим

$$\lambda = nq + \sum_{k=1}^n \sqrt{q} (a_k + b_k) + a_k b_k = nq + \sum_{k=1}^n z_k,$$

где $q = P_c / P_n$ – отношение мощностей сигнала P_c и помехи P_n , $a_k = (-1)^{\varepsilon_k + \delta_{k-1}}$, $b_k = (-1)^{\varepsilon_k + \delta_k}$, ε_k и δ_k – определены ранее,

$$z_k = \begin{cases} 2\sqrt{q} + 1, & a_k = b_k = +1 \\ -2\sqrt{q} + 1, & a_k = b_k = -1 \\ -1, & a_k \neq b_k = +1 \\ -1, & a_k \neq b_k = -1 \end{cases}$$

Математическое ожидание и дисперсия величины λ в этом случае равны соответственно

$$M\{\lambda\} = nq, \quad D\{\lambda\} = n(2q + 1).$$

Используя гауссовскую аппроксимацию, которая вытекает из характера случайных преобразований в процессе обработки принимаемого сигнала в демодуляторе, получаем окончательное выражение для вероятности ошибки приема сигнала с расширенным спектром:

$$P_{\text{ош}} \approx 1 - F\left(\sqrt{\frac{nq^2}{2q+1}}\right), \quad (4)$$

где $F(x) = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^x e^{-t^2/2} dt$ – интеграл вероятностей

или гауссовская функция ошибок [1].

Результаты вычислений вероятностей ошибок $P_{\text{ош}}$ по (4) для случая наиболее опасного воздействия преднамеренной помехи, когда она является противофазной по отношению к сигналу и превышает его по мощности, представлены на рис. 2. Здесь показаны графические зависимости вероятностей ошибок при базах сигнала $n = 20, 50, 100$ и отношениях сигнал/помеха $0 < q = P_c / P_n < 1$. Видно, что при помехе, вдвое превышающей сигнал по мощности $q = P_c / P_n = 0,5$, вероятности ошибки имеют величины при базах сигнала $n = 20 P_{\text{ош}} = 5,7 \cdot 10^{-2}$, $n = 50 P_{\text{ош}} = 6,2 \cdot 10^{-3}$, $n = 100 P_{\text{ош}} = 1,93 \cdot 10^{-4}$.

Таким образом ясно, что реализация расширения спектра сигнала методом самокодирования позволяет обеспечить необходимую помехоустойчивость передачи сообщений при повышенной скрытности и безопасности передаваемых сигналов в отличие от клас-

сического расширения спектра при использовании псевдослучайных последовательностей, которые не обладают необходимой защищенностью от вскрытия их структуры.

Метод расширения спектра при самокодировании может быть использован при организации связи в радиосети по типу систем радиовещания. В этом случае может работать одна передающая станция, а прием осуществлять некоторое множество приемных станций, которые не потребуется обеспечивать исходными ключевыми данными перед каждым сеансом передачи сообщений, в том числе в условиях действия преднамеренных помех. Названные радиосети могут применяться для передачи важных сигналов оповещений: о стихийных бедствиях, об экстремальных ситуациях, угрожающих жизни и здоровью населения определенных территорий. Подобным образом можно передавать мореплавателям навигационные сообщения и другую важную информацию в условиях воздействия преднамеренных помех со стороны третьих незаконных лиц.

Литература

1. Скляр, Б. Цифровая связь. Теоретические основы и практическое применение / Б. Скляр ; пер. с англ. под ред. А.В. Назаренко. – Изд. 2-е, испр. – Москва : Издательский дом «Вильямс», 2003. – 1104 с.
2. Ипатов, В. Широкополосные системы и кодовое разделение сигналов / В. Ипатов. – Москва : Техносфера, 2007. – 488 с.
3. Помехозащищенность систем радиосвязи с расширением спектра прямой модуляцией псевдослучайной последовательностью / В.И. Борисов, В.М. Зинчук, А.Е. Лимарев, В.И. Шестопалов. – 2-е изд. перераб. и доп. – Москва : РадиоСофт, 2011. – 550 с.
4. Голдсмит, А. Беспроводные коммуникации / А. Голдсмит. – Москва : Техносфера, 2011. – 904 с.
5. Диксон, Р. К. Широкополосные системы / Р.К. Диксон. – Москва : Связь, 1979. – 304 с.
6. Nquen, L. Self-Encoded Spread Spectrum Communications / L. Nquen // IEEE Military Communications. Conference Proceedings, Atlantic City, NJ, USA. – 1999. – Vol. 1. – P. 182–186.
7. Агафонов, А. А. Методология и результаты синтеза и оценки преднамеренных помех приемникам дискретных сигналов / А.А. Агафонов, К.Ю. Ложкин, В.Н. Поддубный // Радиотехника и электроника. – 2003. – Т. 48, № 8. – С. 956–962.
8. Биккенин, Р. Р. Оценка эффективности обработки шумоподобных сигналов с относительной фазовой модуляцией на удлинённом интервале в условиях наихудших помех / Р.Р. Биккенин, А.А. Андрюков // Информация и Космос. – 2015. – № 3. – С. 6–12.