

СИСТЕМА СВЯЗИ С РАСШИРЕНИЕМ СПЕКТРА НА ОСНОВЕ ХАОТИЧЕСКИХ БИНАРНЫХ КОДОВ

Беляев Р.В., Калинин В.И., Кислов В.В., Колесов В.В.

Институт радиотехники и электроники Российской Академии наук
103907, Россия, Москва, Моховая 11, ИРЭ РАН
Tel/Fax: +7-095-2034693/2038414, E-mail: belyaev@mail.cplire.ru

Реферат. Рассмотрены перспективные направления развития систем передачи информации, использующих сложные сигналы с большой базой. Обсуждаются преимущества систем связи с расширением спектра. В микроволновом диапазоне частот предложена аппаратная реализация модема, осуществляющего расширение и обратное сжатие спектра непосредственно на несущей частоте сигнала. Фазовая манипуляция передаваемого сигнала производится с использованием хаотических бинарных кодов, которые формируются цифровым процессором. Реализован способ передачи информации с помощью хаотических кодовых сигналов. Экспериментально исследовано влияние задержки кода на процесс выделения информации при свертке принятого сигнала. Показано, что цифровая система связи с расширением спектра и динамической сменой хаотических кодов обладает высокой помехозащищенностью и повышенной конфиденциальностью при передаче данных в условиях сложной электромагнитной обстановки.

1. Введение

Широкополосные устройства связи с расширением спектра находят все большее применение в телекоммуникационных системах различного назначения. При фазовой манипуляции псевдослучайным кодом достигается эффективное расширение спектра передаваемых сигналов. Широкополосные системы с низкой спектральной плотностью излучения обладают электромагнитной совместимостью с другими одновременно работающими средствами и в том числе с узкополосными.

Сложные сигналы с расширением спектра на основе хаотических кодов сложно обнаружить в эфире и выделить из них полезную информацию обычными средствами радиоперехвата, ведущими прием без кодового сжатия сигналов во времени. Для систем связи с кодовым расширением спектра удастся осуществить статистическое разделение лучей при многолучевом распространении сигналов, что особенно важно для устойчивой мобильной связи в условиях плотной городской застройки. Восстановление информации при свертке во времени широкополосных сигналов возможно, когда интенсивность принимаемых сигналов значительно меньше помех. Высокая помехозащищенность систем связи с кодовым расширением спектра позволяет надежно осуществлять передачу сообщений при сложной электромагнитной обстановке.

2. Математические алгоритмы для создания бинарных хаотических кодов

Идентификация сообщений собственным кодом позволяет осуществить кодовое разделение и кодовую адресацию для всех абонентов в сети связи. База сигнала определяет реальный объем системы сигналов и характеризует помехозащищенность системы связи с расширением спектра. Создание большого ансамбля бинарных хаотических кодов осуществляется простым математическим алгоритмом вида

$$\begin{aligned} y_k &= \text{sign}[F(x_k)] \\ x_k &= (1 - \exp(-h))\text{sign}[F(x_{k-N})] + \exp(-h)x_{k-1} \end{aligned} \quad (1)$$

на основе которого вычисляются хаотические процессы y_k в сильно неравновесной динамической системе с запаздыванием [1]. Здесь параметр h означает шаг дискретизации по теореме отсчетов Котельникова, а целое число N определяет количество отсчетов на времени запаздывания в динамической системе. Количество отсчетов N на времени запаздывания является размерностью вложения для множества хаотических кодов y_k по теореме Такенса о реконструкции динамики [2]. Хаотический код y_k полностью воспроизводится в приемном устройстве при точном задании N начальных отсчетов для порождающего алгоритма (1). При неточном задании начальных отсчетов даже малая ошибка приводит к экспоненциальному расхождению возмущенной и заданной траекторий и по истечении малого времени возмущенный код полностью отличается от заданного кода. При этом восстановление передаваемой информации на основе возмущенного кода становится невозможным. Точное задание N начальных отсчетов определяет идентификатор абонента и одновременно является ключом при восстановлении конфиденциального сообщения.

3. Структура модема при цифровой обработке сигналов

В микроволновом диапазоне разработан модем на основе мостовой схемы фазовращателя с фиксированным сдвигом фазы на одно из возможных состояний $\varphi = \pi/2, \pi/4, \pi/8, \pi/16$ [3]. Переключение фазосдвигающих отрезков микро полосковой линии производится высокочастотными $p-i-n$ диодами с малым временем релаксации не превышающим 5 наносекунд. Диапазон перестройки рабочей частоты для модема превышает октаву. Управление $p-i-n$ диодами в схеме фазовращателя осуществляется хаотическими бинарными кодами, которые формируются программируемым цифровым процессором согласно математическому алгоритму (1). Для каждого абонента программным способом устанавливается собственный хаотический код за счет выбора N - мерного вектора начальных отсчетов [4]. Многомерный цифровой массив, задающий вектор начальных отсчетов, является идентификационным параметром абонента. Программируемый кодер для формирования индивидуальных хаотических кодов создан на основе быстродействующей ПЛИС-технологии.

4. Передача информации

Передаваемая цифровая информация вносится путем частотной модуляции несущей частоты 2600 МГц (рис.1а). Операция кодового расширения спектра для ЧМ сигнала, несущего информацию, выполняется фазовым модулятором в схеме передающего модема непосредственно на несущей частоте сигнала. Излучаемый передатчиком сигнал с информационной составляющей имеет непрерывный шумовой спектр (рис.1б), основная доля энергии которого заключена в полосе частот $\Delta f = 2 F_T$. Тактовая частота F_T хаотических бинарных кодов устанавливается синтезатором частот в схеме модема и в эксперименте выбирается равной $F_T = 1$ МГц. Информационное сообщение представляет собой последовательность двоичных символов в виде импульсов тока с тактовой частотой 20 кГц.

Размерность N числового идентификатора или вектора начальных отсчетов выбирается не менее $N > 7$. Это важное условие для порождающего алгоритма (1) обеспечивает устойчивый режим многомерного хаоса при формировании кодов с хорошими корреляционными и статистическими свойствами. Передаваемый широкополосный сигнал с информационной составляющей имеет непрерывный шумовой спектр (рис.1б) и по своей структуре практически неотличим от случайного процесса с той же полосой частот.

Цифровой процессор кодера функционирует в циклическом и аperiodическом режимах. При циклическом формировании хаотические коды повторяются с заданным периодом. В аperiodическом режиме цифровой процессор генерирует непрерывную и не повторяющуюся последовательность хаотических символов. Таким способом осуществляется динамическая смена кодов в течение всего времени передачи данных. Разработанная система передачи данных с динамической сменой кодов практически исключает возможность криптографического раскрытия сообщений согласно результатам Шеннона [5].

В приемнике информация выделяется после устранения относительной задержки принятого и опорного кодов и сжатия по частоте широкополосного сигнала. В эксперименте передача данных ведется с динамической сменой кодов за счет непрерывной генерации неperiodических последовательностей. Копия хаотического бинарного кода формируется в приемнике цифровым процессором на основе порождающего алгоритма (1) при точном задании N - мерного числового идентификатора или вектора начальных отсчетов. Обратное преобразование принятого ФМ-сигнала осуществляется фазовым демодулятором, который восстанавливает фазу сигнала используя в качестве управляющего сигнала копию хаотического кода. Сжатие принятого сигнала по частоте возможно только при задержке принятого и опорного кодов в пределах длительности одного такта. Эффективность свертки принятого сигнала в зависимости от временного сдвига кодов иллюстрируется энергетическими спектрами для декодированных принятых сигналов (рис.1в-1е). На рис.1в представлен спектр сигнала на выходе демодулятора при синхронизации принятого и опорного кодов, когда задержка кодов $\tau = 0$ отсутствует. Спектр восстановленного сигнала содержит информационную составляющую подобную спектру ЧМ-сигнала на выходе информационного модулятора в передатчике (рис.1а). При отсутствии активных помех уровень информационных составляющих превышает почти на 40 дБ собственные шумы приемника и на 35 дБ выше паразитных составляющих с тактовой частотой $F_T = 1$ МГц. При длительности одного символа $T = 1/F_T = 1$ мкс задержка опорного кода всего на $\tau = 0.1T = 0.1$ мкс приводит к уменьшению на 14 дБ информационной составляющей в спектре до уровня 26 дБ относительно шумового пьедестала (рис.1г). При задержке опорного кода на $\tau = 0.3T$ (рис.1д) и $\tau = 0.5T$ (рис.1е) уровень информационной составляющей снижается до 15 дБ и 7 дБ соответственно. Одновременно с ростом задержки

τ наблюдается увеличение уровня, как шумового пьедестала, так и паразитных составляющих на кратных F_T частотах в спектре вследствие неполной свертки принятого сигнала. При увеличении задержки опорного кода свыше длительности одного такта $\tau > T$ информационная составляющая в спектре неразличима на фоне шума и восстановление передаваемой информации становится невозможным. Проведенный эксперимент по передаче данных с динамической сменой хаотических кодов показал, что эффективное восстановление полезной информации происходит только при малой задержке $\tau < 0.5T$ опорного кода. Результаты эксперимента по передаче информации в системе связи с расширением спектра и динамической сменой кодов свидетельствуют о необходимости точной синхронизации опорного кода в приемнике.

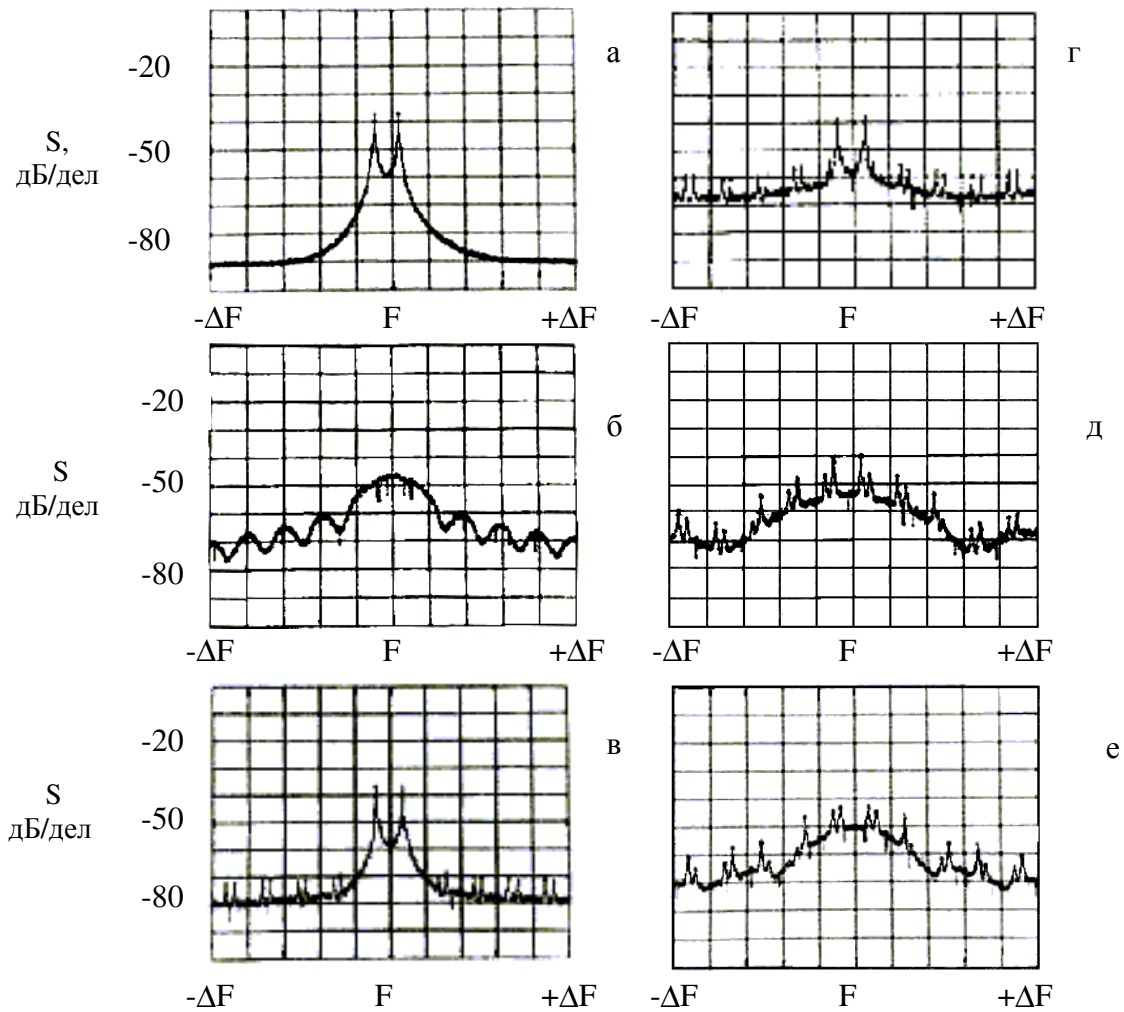


Рис.1 Преобразование спектра сигнала при прохождении по каналу связи
 а-спектр информационного ЧМ-сигнала; б-спектр передаваемого сигнала с кодовым расширением спектра и информационной составляющей; в-спектр восстановленного сигнала после демодулятора при полной синхронизации; спектры восстановленного сигнала с информационной составляющей при рассинхронизации (τ) между кодерами модулятора и демодулятора: $\tau = 0.1 T$ (г), $\tau = 0.3 T$ (д), $\tau = 0.5 T$ (е), где T - период повторения импульсов кодирующей последовательности.

Средняя частота диапазона развертки $F=2600$ МГц, Полуширина диапазона развертки по оси $X \Delta F = 5$ МГц. Тактовая частота импульсов генератора хаотической кодовой последовательности $F_{\text{такт}} = 1$ МГц, частота. Частота девиации информационного сигнала 0.5 МГц равная $F_{\text{такт}}/2$. Частота информационных импульсов $F_m = 20$ кГц. Цена деления по оси $Y - 10$ дБ/дел.

5. Заключение

Цифровая система связи с расширением спектра и динамической сменой хаотических кодов обладает высокой помехозащищенностью и повышенной конфиденциальностью при передаче данных в условиях сложной электромагнитной обстановки, воздействия сильных помех и многолучевого распространения сигналов. Быстродействующие цифровые процессоры на основе конечномерных алгоритмов с нелинейной динамикой создают большой ансамбль хаотических бинарных кодов, что позволяет практически осуществить кодовое разделение большого числа абонентов. Передача данных с динамической сменой хаотических кодов затрудняет возможность криптографического раскрытия конфиденциальных сообщений.

Работа выполнена при поддержке Российского фонда фундаментальных исследований, проект № 98-02-16722 и № 00-07-90147. .

Литература

1. Ю.В. Гуляев, В.Я. Кислов, В.В. Кислов, Новый класс сигналов для передачи информации – широкополосные хаотические сигналы // ДАН. 1998. Т.359. № 6. С. 750-754.
2. F. Takens. Detecting strange attractor in turbulence, Lecture Notes in Mathematics, 898, pp.366-381, 1981.
3. Р.В. Беляев, В.И. Калинин, В.В. Колесов. Реализация широкополосного цифрового канала связи на основе сложнокодированных сигналов с большой базой. LV научная сессия, посвященная дню радио, «Радиотехника, электроника и связь на рубеже тысячелетия», 17-19 мая 2000 года, Москва, Труды конференции, С. 200.
4. Р.В. Беляев, Г.М. Воронцов, В.В. Колесов. Цифровой генератор случайного сигнала для кодирования информации в системах связи с расширением спектра. LV научная сессия, посвященная дню радио, «Радиотехника, электроника и связь на рубеже тысячелетия», 17-19 мая 2000 года, Москва, труды конференции, С. 201.
5. С.Е. Shannon. A Mathematical Theory of Communication. // Bell. System Techn. J., 1948. V.27, No 3, P. 379-423.



COMMUNICATION SYSTEM WITH SPREAD SPECTRUM ON THE BASIS OF CHAOTIC BINARY CODES

Belyaev R.V., Kalinin V.I., Kislov V.V., Kolesov V.V.

Institute of Radioengineering and Electronics Russian Academy of Science
103907, Russia, Moscow, Mokhovaja 11, IRE RAS
Tel/Fax: +7-095-2034693/2038414, E-mail: belyaev@mail.cplire.ru

Abstract

Perspective guidelines of development system for transmitting information by complex signals with a large base were considered. It was discussed an advantages of communication system with spread spectrum. In microwave frequency band it was proposed and realized spectrum compression directly on carrier frequency. The phase manipulation of transmitting signals was processed with using of chaotic binary codes generated by digital processor. There was realized the method of transmitting information with chaotic binary signals. Effects of code delay on detecting information by convolution of receiving signals was examined experimentally. It was shown that digital communication system with spread spectrum and dynamical changing of chaotic codes has high level of noise immunity and high confideliity of data transmission at complex electromagnetic environment.

The wide frequency band spread spectrum communication devices are finding the more and more wide application. The effective spreading of transmitting signals spectrum are obtained by phase modulation with chaotic binary codes. The high frequency band system with low density of spectrum radiation has electromagnetic compatibility with other at the same time operating systems including the low-band one's.

The complex signals with spread spectrum on the base of chaotic codes are difficult to detect and extract off information by means of common radio interception facility without using code convoluton in time. For the communication system with code spread spectrum it is possible to realize statistical beam division in condition of many-beams propagation. The recovery (восстановление) of information under spectrum compression (свертка) in time of such type wide-band signals (для таких систем) is possible when the intensity of receiving signals are significantly low then noise level. High level of noise immunity and noise interference (помехозащищенности) system of communications with chaotic coding spread spectrum permite to realize reliable transmission of message in complex electromagnetic environment.

The identification of message by it's own code permit to realize code division and code addressing for all users of communication network. The base of signals defines (определяет) real volume of whole signal system and characterizes noise immunity noise protection (помехозащищенность) of communication system with spread spectrum. The generation of great ensemble of binary chaotic codes is realizing by simple mathematical algorithm

$$y_k = \text{sign}[F(x_k)]$$
$$x_k = (1 - \exp(-h)) \text{sign}[F(x_{k-N})] + \exp(-h)x_{k-1} \quad (1)$$

On the base of (1) there were calculated the chaotic processes y_k in strong nonequilibrium dynamic system with delay [1]. Here it is: h - is a step of sampling in accordance with Kotelnikov's theorem of samples, N is an integer number defining number of samples on delay time in dynamical system. By Takens theorem on reconstruction this number N is defining the dimension of embedding (размерность вложения) for the (множества) set chaotic codes [2]. The chaotic code y_k is complitly regenerated in receiver in case of precise defining (задание) N string values of samples for algorithm (1). The incorrect values of one's in receiver will lead to exponential evolving (отклонение, расхождение) between code sequences in transmitter and in receiver after a quick time.

On the basis of algorithm (1) it was designed oscillator of chaotic binary code sequence with PLM-technology. The digital channel of data transmission was realized with using for spreading spectrum chaotic binary code sequence with repeat frequency 1 MGz [3]. The carrier frequency of system is 2600 MGz and binary information pulses has frequency band 20 kGz. Processes of spreading spectrum in transmitter and its next time compression in receiver were realized on identical FM-devices with p-i-n diodes. Under the action of chaotic code pulses these diodes switch long line sections providing phase modulation. It was studied effect of controllable phase shift between chaotic code sequence in transmitter and receiver on the recovery information in the last one. It was shown that effective information recovery in receiver is possible only when the time- shift between base (опорный) code sequence and the one in receiver $\tau < 0.5 T$. Here T is a period of coding pulse clock rate. In accordance with Shannon's results the designed system of data communication with dynamical codes changing practically excludes possibility of cryptographic revelation of message [4].

Conclusion

The digital communication system with spread spectrum and dynamical chaotic changing of codes has the high level of noise and interference rejection (помехозащищенность) and high confidentiality in processes of data transmission in condition of complex electromagnetic environment. High rate digital processors on the base of finite - dimensional algorithm with nonlinear dynamic is generating a great ensemble chaotic binary codes sequences what is the base for possibility to divide a great number of users.

This study has been made with support of Russian Fond of Fundamental Research, grants N98-02-16722 and N 00-07-90147.

Reverence

1. Yu.V.Guljaev, V.Ya. Kislov, V.V.Kislov. The New Class of Signals for Information Transmittance - Wide Band Chaotic Signals // Doclady Akademii nauk (Reports of Russian Academy of Science). 1998.V.359. N 6. P.750-754.
2. F.Takens. Detecting strange attractor in turbulence, Lecture Notes in Mathematics, 898, P.366-381,1981.
3. R.V.Belyaev, V.I.Kalinin, V.V.Kolesov. The Realization Wide- Band Digital Channel on the Base of Complex - coded Signal with the Big Base. LV -Anniversary Scientific session Radio, "Radiotechnika,Electronika i Sviaz na rubeje 2000".17-19 May 2000, Moscow, trudi konferencii. P.201.
4. C.E.Shenon. Mathematical Theory of Communication//Bell.System Techn. J., 1948.V.27., N 3, P.379-423.