ЗАЩИТА ИНФОРМАЦИИ ПРИ ПЕРЕДАЧЕ ЦИФРОВЫХ СООБЩЕНИЙ В CDMA-КАНАЛАХ СВЯЗИ

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

Институт радиотехники и электроники Российской Академии наук
101999, Россия, Москва, К-9, Моховая 11, корп.7, ИРЭ РАН
Tel/Fax: +7(095) 2034693/2038414, E-mail: kalinin@ms.ire.rssi.ru

Аннотация: Реализован способ передачи информации с кодовым разделением абонентских каналов на основе множества хаотических кодов. Методом реконструкции нелинейной динамики построены конечномерные алгоритмы для расчета хаотических сигналов в динамических системах с запаздыванием. В микроволновом диапазоне частот аппаратно реализован модем, осуществляющий расширение и обратное сжатие спектра непосредственно на несущей частоте сигнала. Показано, что цифровая система связи с расширением спектра, в которой для управления модемом используются хаотические коды, обладает высокой помехозащищенностью, скрытностью и обеспечивает надежную и конфиденциальную передачу сообщений в условиях сложной электромагнитной обстановки.

1. Введение

Развитие телекоммуникационных средств нового поколения основано на использовании широкополосных сигналов с большой базой [1-3]. За счет расширения полосы частот несущих сигналов достигается увеличение скорости передачи информации, повышается устойчивость и надежность работы радиоэлектронных систем. Защита передаваемой информации в многоканальных CDMA системах (Code Division Multiple Access Systems) и в беспроводных системах связи с расширением спектра (Wireless Spread Spectrum Systems) осуществляется кодированием сообщений с помощью псевдослучайных последовательностей [1-3]. Применение широкополосных шумоподобных сигналов обеспечивает высокую пропускную способность каналов, позволяет ослабить воздействие многих видов помех, а также бороться с влиянием многолучевого распространения радиоволн [1,3]. Важной особенностью широкополосных систем является высокая скрытность собственных излучений и электромагнитная совместимость с другими радиоэлектронными средствами за счет передачи в эфир непрерывных во времени шумоподобных сигналов с очень низкой спектральной плотностью.

2. Линия связи с расширением спектра на основе хаотических кодов

Реализована линия связи для передачи конфиденциальных сообщений содержит микроволновые передающую и приемную аппаратуру, а также схему для синхронизации хаотических кодов. Сообщение вносится путем модуляции параметров (фаза, частота, амплитуда) несущего высокочастотного сигнала от задающего генератора в передатчике. Кодирование высокочастотного сигнала с информационной составляющей производится хаотическим кодером. С помощью микроволнового фазового модулятора осуществляется кодовое изменение фазы на [0-180] градусов непосредственно на несущей частоте излучаемого сигнала. Рабочий диапазон частот для линии связи составляет от 1800 МГц до 3600 МГц.

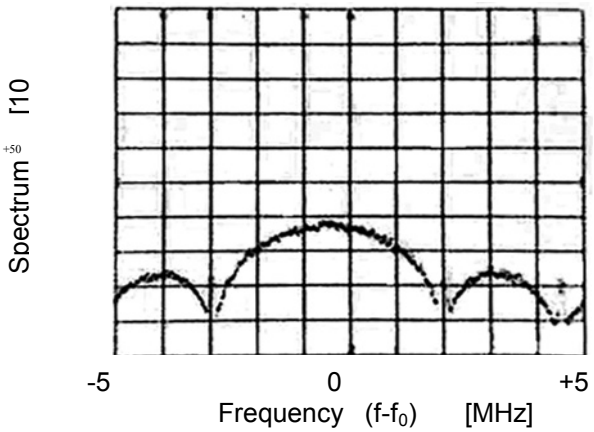

Рис.1. Кодовое расширение спектра сигнала в передатчике

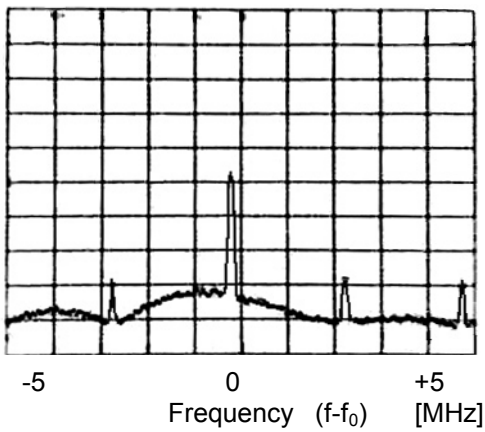

Рис.2. Когерентное сжатие по частоте сигнала в приемнике

Управление фазовым модулятором производится хаотическими бинарными импульсами малой длительности T, которые формируются генератором хаотического кода. Тактовая частота $F_T = 1/T$ для генератора хаотического кода устанавливается кварцевым синтезатором частот с высокой точностью и может выбираться в широких пределах от сотен килогерц до десятков мегагерц. Значение тактовой частоты F_T, установленное синтезатором частот для хаотического кода, определяет полосу частот $\Delta f = 2F_T$ передаваемого в эфир сигнала (рис.1).

Схема управления устанавливает режим передачи сообщений с заданным расширением спектра и кодовым разделением абонентских каналов. Шумоподобный сигнал с расширением спектра, в котором полезная информация распределена по всему спектру частот, излучается антенной передатчика в окружающее пространство.

На приемной стороне шумоподобный сигнал с широким спектром частот принимается антенной и поступает на вход фазового демодулятора. Демодулятор приемника выполнен по той же микрополосковой схеме, что и модулятор передатчика. Управление демодулятором производится хаотическими бинарными импульсами от собственного генератора хаотичес-кого кода в приемнике. По закону хаотической последовательности производится обратное преобразование фазы непосредственно на высокой несущей частоте принятого сигнала. В декодере приемника аппаратно реализован тот же математический алгоритм генерации хаотического кода, что в кодере передатчика. При синхронизме во времени опорного кода в приемнике и кода поступившего сигнала имеет место когерентное восстановление фазы несущего сигнала. В результате фазовой демодуляции и полного восстановления фазы осуществляется когерентное сжатие спектра принятого широкополосного сигнала. Спектр восстановленного сигнала на выходе демодулятора в приемнике подобен спектру информа-ционного сигнала (рис.2). Необходимым условием сжатия сигнала в приемнике с последующим восстановлением сообщений является точная синхронизация во времени принятого и воспроизведенного в приемнике хаотических кодов.

3. Защита передаваемой информации

Важным условием, предъявляемым к современным телекоммуникационным средствам, является обеспечение скрытности и конфиденциальности связи [1,3]. Скрытность функционирования беспроводных систем связи (Wireless Spread Spectrum Systems) повышается за счет кодового расширения спектра передаваемых в эфир непрерывных излучений с очень низкой спектральной плотностью. Защита передаваемой информации от несанкционированного доступа достигается кодированием сообщений с помощью длинных непериодических псевдослучайных последовательностей (ПСП) или за счет динамической смены во времени кодирующих последовательностей.

При создании систем с кодовым разделением абонентских каналов (CDMA) важным является выбор математических алгоритмов, порождающих большой ансамбль ПСП. Формируемые псевдослучайные последовательности должны обладать нужными статистическими и спектральными свойствами, а также хорошими авто и взаимно корреляционными характеристиками. Особые требования предъявляются в отношении большого объема ансамбля ортогональных ПСП, что необходимо для одновременной и устойчивой работы многих пользователей в общей пространственной зоне. Математические алгоритмы должны генерировать множество статистически независимых псевдослучайных кодов большой длительности и высокой структурной сложности, чтобы обеспечить конфиденциальность при передаче информации [1-3].

Известные методы формирования псевдослучайных последовательностей обладают определенными недостатками и не всегда способны удовлетворить в полной мере требованиям, предъявляемым к большой системе сигналов. Так в семействе псевдослучайных последовательностей максимального периода на основе функций Адамара велика вероятность появления пар ПСП с высоким уровнем взаимной корреляции и большим числом (достигающим трети длины ПСП) совпадающих символов [1].

В ряде работ последнего времени предложен новый класс псевдослучайных сигналов – широкополосных хаотических сигналов, которые имеют принципиально иную физическую природу на основе явления динамического хаоса [2]. Хаотические математические алгорит-мы порождают множество ПСП, которые наиболее полно отвечают требованиям по защите передаваемой информации. К достоинствам подобных алгоритмов относятся легкость программно-аппаратного воспроизведения и необходимость передачи для синхронизации сообщений только ограниченного набора начальных данных, однозначно определяющих начало вычислений по алгоритму. Хаотический кодер разработан на основе быстродейст-вующих устройств цифровой обработки сигналов (ЦОС), с помощью которых аппаратно реализован математический алгоритм для генерации хаотических бинарных кодов. Матема-тический нелинейный алгоритм представляет собой систему разностных дифференциальных уравнений, описывающих хаотическое поведение динамической нелинейной системы с запаздыванием. В хаотическом кодере предусмотрены специальные режимы для генерации хаотических кодов. В циклическом режиме формируются повторяющиеся

последователь-ности хаотических кодов заданной длительности. В апериодическом режиме имеет место непрерывная генерация не повторяющихся хаотических кодов произвольной длительности. Режим генерации непериодических хаотических кодов предназначен для динамической смены во времени кодовых последовательностей при передаче сообщений. Согласно теоретическим исследованиям Шеннона в результате быстрой динамической смены во времени случайных кодов становится невозможным несанкционированный перехват кодиро-ванных сообщений в реальном времени с помощью всегда ограниченных вычислительных ресурсов, даже очень большой производительности, которыми может располагать аппарату-ра перехвата [4]. Динамическая смена во времени хаотических кодов применяется для надежной защиты передаваемых сообщений от несанкционированного доступа.

Применение в телекоммуникационных системах широкополосных хаотических сигналов позволяет повысить помехоустойчивость, скрытность, конфиденциальность и надежность передачи информации при наличии сильных помех и искажений в каналах связи.

Работа выполнена при финансовой поддержке Российского фонда фундаментальных исследований (проект № 00-07-90147 и проект № 01-07-90349).

Литература

1. Andrew J., Viterby. CDMA: Principles of Spread Spectrum Communication. – New York: Addison-Wesley Publishing Company, 1996.

2. 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.

3. Р.В. Беляев, В.И. Калинин, В.В. Колесов, Формирование шумоподобной несущей в системах связи с расширением спектра // Радиотехника и электроника, 2001, Т.46, № 2, С.214-223.

4. C.E. Shannon. A Mathematical Theory of Communication. Bell. System Techn. J., 1948. V.27, No 3, P. 379-423.

INFORMATION SECURITY OF TRANSMITTING DIGITAL MESSAGE BY CDMA-CHANNELS

Gulyaev Yu., Kislov V., Kalinin V., Kolesov V., Belyaev R.

The Institute of Radio-Engineering and Electronics Russian Academy of Science
Russia, 101999, Moscow, K-9, Mokhovaya 11, block 7, IRE RAS
Tel/Fax :+7(095) 2034693/2038414, E-mail: kalinin@ ms.ire.rssi.ru

Annotation: There was realized the method of transmitting information with code division multiple access system on the basis of the chaotic code's manifold. The methods of reconstruction dynamic of nonlinear systems with delay were used to create the finite dimension algorithms for calculation chaotic signals. In microwave band there was realized in hardware an endec making expansion and convolution encoding with direct processing on a carrier frequency. It was shown that the digital communication system with the chaotic codes has high level of noise immunity, secrecy and guarantee a reliability and a confidentiality in a complex electromagnetic environment.

The important condition of contemporary telecommunication systems functioning is a guarantee of communications secrecy and confidentiality. The secrecy of wireless communication spread spectrum systems is rising up by applying spectrum expansion of transmitting an continuous radiation with very low level of spectral density. The security of the transmitting information with unapproved admission is achieved by coding the message with long nonperiodic pseudo-random sequences or by dynamical changing in time such type sequences.

Recently there was proposed a new class of pseudo–random wide–band chaotic signals having fundamentally different character and basing on phenomena of dynamical chaos. [2]. The chaotic mathematical algorithms generate a great number of pseudo-random sequences fully corresponding to secrecy requirements of transmitting information. The advantage of these algorithms are an easiness of their software- hardware implementation and necessity of transmitting for synchronization only a shot set of data unambiguously defining a start of computation. On the basis of fast-acting digital chips there have been design such type of endec realizing by hardware the mathematical algorithm generating chaotic binary codes.

There were provided for special modes of generating chaotic codes. In cycling mode there were generated repeating sequences of chaotic codes with defined time length. In non-cyclic mod there is non-stop generation non-recurrent sequences of chaotic codes with defined duration. This one is intended for working in mode with dynamical changing of keys. In accordance with Shenon's theoretical results in conditions of fast dynamical changing in time of chaotic key-sequences it is impossible to unapproved admission in real time to transmitted encoded information with help of always limited computational resources (even with very high processing power) of pickup equipment [4].

Applying in communication systems wide-band chaotic signals are provided to rise up noise-immunity, secrecy, confidentiality and reliability of transmitted information in conditions of heavy noise and artifacts in communication channels.

References

1. Andrew J., Viterby. CDMA: Principal of Spread Spectrum Communications.-New York: Addison-Wesley Publishing Company, 1996.
2. Gulyaev Yu.V., Kislov V.Ya., Kislov V.V., New class of signals for transmitting informa-tion- wide-band chaotic signals. Reports .Academy of Sciences. 1998. V.359.№ 6. P.750-754.
3. Belyaev R.V., Kalinin V.I., Kolesov V.V., Forming noise-like carrier in system of spread spectrum communication. J.Comm. Technology Electronics. 2001 .V.46. № 2. P.214-223.
4. C.E. Shannon A Mathematical Theory of Communication // Bell System Techn. J. 1948. V.27. № 27, P.379-423.