

УДК 621.391.01

ОРТОХАОТИЧЕСКАЯ ПЕРЕДАЧА ДАННЫХ

В. С. Выхованец

**Институт проблем управления им. В.А. Трапезникова РАН,
117997, Москва, ул. Профсоюзная, 65**

Статья поступила в редакцию 14 ноября 2017 г.

Аннотация. В статье рассматриваются методы передачи данных с помощью хаотических сигналов и обсуждаются проблемы хаотической синхронизации. Предложен метод передачи данных, основанный на использовании ортогональных хаотических сигналов. Хаотический сигнал разделяется на импульсы заданной длительности. При передаче текущего хаотического импульса следующий хаотический импульс подвергается ортогонализации или коллинеаризации в зависимости от передаваемых данных. На стороне приемника вычисляется взаимная энергия текущего и предыдущего хаотического импульса, на основании чего принимается решение о передаче одной из трех цифр. Синхронизация битовых интервалов приемника и передатчика осуществляется на основе изменения знака взаимной энергии соседних хаотических импульсов. Приведены функциональные схемы ортохаотического приемника и передатчика. Представлены результаты вычислительного эксперимента по оценке помехоустойчивости описанного метода передачи данных и выполнено сравнение помехоустойчивости метода с помехоустойчивостью амплитудной и фазовой манипуляции при оптимальном приеме сигналов. Показана возможность использования предложенного метода для скрытой передачи данных.

Ключевые слова: широкополосный шумоподобный сигнал, хаотический сигнал, хаотическая синхронизация, ортогонализация и коллинеаризация хаотических импульсов, корреляционный прием.

Abstract. In this paper new and existing approaches are developed to data transfer for chaos-based communication systems. Chaotic communication has many advantages over traditional communication for its broadband, noise like

characteristics. In the traditional communication based on Chaos Shift Keying, synchronization needs to be established between the transmitter and receiver of the system. Due to the extreme sensitivity of initial value of chaotic signal, it is very difficult to achieve synchronization. So this method is difficult to be applied practically. To solve this problem, an Orthochaotic Data Transfer system was proposed, in which chaos synchronization is not necessary. The chaotic signal is divided into pulses of a given duration. When transmitting the current pulse following the previous one is exposed orthogonalization or collinearization depending on transmitted data. On the receiver side the scalar product of the current received pulse and the previous received pulse is calculated and the decision is performed about transfer of one of the three numbers. Synchronization of the receiver and the transmitter are done on the basis of changes in sign of the mutual energy of the neighboring chaotic impulses. The new system was deeply studied and was compared with the Binary Phase Shift Keying modulation. The efficiency of the proposed approach is illustrated with plots of dependences of bit-error rate on signal to noise ratio. It can be clearly seen that the Orthochaotic Data Transfer is realizable in digital secure communication.

Keywords: broadband pseudo noise signal, chaotic signal, chaos synchronization, orthogonalization and collinearization of chaotic pulses, correlation receiving, chaotic digital secure communication.

Введение

Современный период развития средств связи связан с поиском и использованием новых широкополосных шумоподобных сигналов. Одной из актуальных проблем в этой области является синтез больших по мощности ансамблей широкополосных шумоподобных сигналов с хорошими корреляционными и групповыми свойствами [1].

Основной метод получения широкополосных шумоподобных сигналов – это формирование сигналов на основе псевдослучайных последовательностей, которые получают при использовании сдвиговых двоичных регистров с

линейными обратными связями. Такие последовательности обладают рядом существенных недостатков [2]: генерируются малые объемы ансамблей сигналов, номенклатура длин последовательностей невелика, наблюдается нарушения сбалансированности структуры последовательности, взаимно-корреляционные свойства с увеличением объема ансамбля резко ухудшаются.

Использование динамического хаоса позволяет устранить многие из этих недостатков. Явление динамического хаоса состоит в том, что движение детерминированной динамической системы при определенных условиях имеет все свойства шумоподобного процесса. При этом принципиальной особенностью динамического хаоса является его нелинейность, а особенностью генерируемого временного процесса (сигнала) – его непериодичность [3]. Хаотические сигналы обладают свойствами, присущими случайным процессам: имеют сплошной спектр мощности и экспоненциально спадающую корреляционную функцию.

Для передачи данных с помощью хаотических сигналов используется несколько базовых методов [4]: хаотическая маскировка, переключение хаотических режимов, модуляция управляющих параметров передающего генератора, нелинейное подмешивание информационного сигнала к хаотическому сигналу и др. Недостатками этих методов является их низкая эффективность по отношению к оптимальным методам корреляционного приема когерентных сигналов. Это связано с тем, что реализация передачи данных сталкивается со сложностью воспроизведения формы хаотического сигнала в приемнике для его корреляционной обработки.

Известен также метод, который позволяет с помощью процедуры Карунена-Лоэва (метод главных компонент) для аттракторов динамических систем синтезировать базис, воспроизводящий структуру аттрактора и позволяющий представить фрагмент хаотического сигнала (хаотический импульс) через набор ортогональных сигналов с числом, равным размерности пространства вложения аттрактора [5]. Фактически речь идет о некогерентном приеме хаотических импульсов, который основан на выделении основных

колебательных мод, характерных только для хаотических колебаний данного типа. Недостатком этого метода является возможность определения только факта наличия или отсутствия хаотического импульса на входе приемника без учета его фазы и длительности.

Другая группа методов для передачи данных использует хаотические сигналы нескольких генераторов хаоса для формирования взаимно ортогональных хаотических сигналов методом Грамма-Шмидта [6, 7]. Для демодуляции сигнала на стороне приемника ему последовательно передаются как исходные ортогональные сигналы, так и суммарный сигнал, несущий данные. В этом случае возможен корреляционный прием и выделение ортогональных компонентов из принимаемого сигнала, каждый из которых переносит отдельный бит сообщения. Недостатком этих методов является необходимость передачи исходных ортогональных сигналов, а также сложность выделения компонентов из смеси нескольких хаотических сигналов в условиях шума.

Настоящая статья посвящена корреляционному приему хаотических сигналов. Рассматриваемый метод близок относительно методу манипуляции шумовыми [8, с. 218] и хаотическими [9, 10] сигналами, однако отличается от последних тем, что манипуляция выполняется не сдвигом фазы опорного сигнала, а ортогонализацией и коллинеаризацией хаотических импульсов методом Грамма-Шмидта.

Рассматриваемый метод также близок многопозиционной манипуляции ортогональными хаотическими сигналами от нескольких генераторов, формируемыми методом Грамма-Шмидта [6, 7], но отличается от последнего тем, что для повышения помехоустойчивости используется максимизация взаимной энергии хаотических импульсов, обеспечивается передача троичного числа за один тактовый интервал, а задача восстановления ортогональных сигналов на стороне приемника решается путем использования относительного метода манипуляции.

Постановка задачи

Пусть задан сигнал χ , полученный от некоторого генератора динамического хаоса и разбитый на интервалы длительности T :

$$\chi_i(t) \quad (t \in [0, T], i = 0, 1, \dots), \quad (1)$$

где χ_i – хаотические импульсы, t – время.

Рассмотрим векторное пространство [11, с. 32], в котором заданы операции сложения, умножения на константу, скалярное произведение и норма:

$$z(t) = x(t) + y(t);$$

$$z(t) = \alpha x(t);$$

$$(x, y) = \int_0^T x(t)y(t) dt;$$

$$\|x\| = \sqrt{(x, x)},$$

где операции сложения и умножение выполняются в некотором поле F ; x, y, z – хаотические импульсы (1); α – константа, $\alpha \in F$.

Выполним процедуру ортогонализации Грамма-Шмидта [12, с. 431] последовательности из $N+1$ импульсов (1) в заданном векторном пространстве:

$$\gamma_i = \chi_i - \sum_{j=0}^{i-1} \frac{(\chi_i, \chi_j)}{(\chi_j, \chi_j)} \chi_j \quad (i = \overline{0, N}). \quad (2)$$

В результате получим ортогональные импульсы γ_i такие, что

$$\int_0^T \gamma_i(t)\gamma_j(t) dt = \begin{cases} 0, & i \neq j; \\ p_i, & i = j \end{cases} \quad (i, j = \overline{0, N}), \quad (3)$$

где p_i – энергия импульса γ_i .

После нормализации (2) могут быть получено множество ортонормированных хаотических импульсов

$$\varphi_i = \frac{1}{\|\gamma_i\|} \gamma_i \quad (i = \overline{0, N}) \quad (4)$$

с единичной энергией.

Уравнения (3) позволяет реализовать корреляционный прием хаотических сигналов, при котором хаотические импульсы непосредственно следуют друг за другом или в виде взвешенной суммы образуют более сложный сигнал. Однако для такого приема необходимо иметь копии всех переданных хаотических импульсов на стороне приемника, что технически трудно реализуемо [13].

Рассмотрим относительный метод манипуляции хаотическим сигналом, при котором решение о передаче того или иного бита данных принимается коррелятором на основании обработки текущего и предыдущего принятого хаотического импульса.

Ортохаотическая передача данных

Выходной сигнал передатчика при передаче данных $\rho_i \in \{-1, +1\}$ сформируем в соответствии с (2) следующим рекуррентным уравнением:

$$\begin{cases} \rho_0 = 0; \\ \varphi_0 = 0, \end{cases} \quad \begin{cases} \gamma_i = \chi_i + \rho_i(\chi_i, \varphi_i)\varphi_i; \\ \varphi_{i+1} = \frac{\gamma_i}{\sqrt{(\gamma_i, \gamma_i)}}, \end{cases} \quad (i = \overline{1, N}), \quad (5)$$

где χ_i – входные хаотические импульсы от генератора хаоса, γ_i – модулированные хаотические импульсы, φ_i – ортонормированные выходные хаотические импульсы с единичной энергией.

Найдем из (5) взаимную энергию двух соседних выходных импульсов φ_i и φ_{i+1} ,

$$(\varphi_{i+1}, \varphi_i) = \int_0^T \varphi_{i+1}(t)\varphi_i(t) dt = (\chi_i, \varphi_i)[1 + \rho_i]. \quad (6)$$

Из (6) следует, что $\rho_i = -1$ выходной импульс φ_{i+1} ортогонален φ_i , а при $\rho_i = +1$ – коллинеарен ему, т.е. взаимная энергия соседних импульсов обнуляется или удваивается в зависимости от передаваемого бита данных.

Величина взаимной энергии (χ_i, φ_i) , фигурирующая в формуле (6), определяет помехоустойчивость передачи данных при наличии помех в канале связи. Чем больше эта величина, тем больше помехоустойчивость. На рис. 1 приведена зависимость модуля взаимной энергии соседних хаотических

импульсов (χ_{i-1}, χ_i) при различных базах B для генератора хаоса, построенного на основе логистического отображения [14], где база импульса – это произведение его полосы частот F на длительность T . Из рисунка видно, что модуль взаимной энергии меньше энергии импульсов во много раз. В соответствии с (5) следует ожидать аналогичного поведения и взаимной энергии (χ_i, φ_i) .

Для повышения помехоустойчивости выходного сигнала передатчика необходимо максимизировать взаимную энергию (χ_i, φ_i) . Для этого можно использовать максимизатор взаимной энергии хаотических импульсов, описываемый следующим уравнением:

$$\chi_i(t) = \begin{cases} +\xi_i(t), & \xi_i(t) \times \varphi_i(t) \geq 0; \\ -\xi_i(t), & \xi_i(t) \times \varphi_i(t) < 0, \end{cases} \quad (7)$$

где ξ_i – хаотические импульсы, получаемые от генератора хаоса, φ_i – выходные хаотические импульсы передатчика.

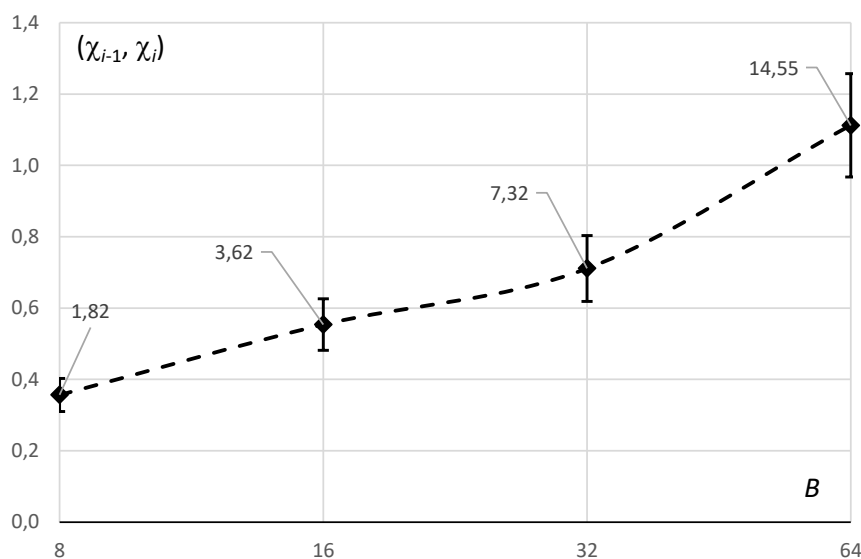


Рис. 1. Взаимная энергия соседних хаотических импульсов при различных базах и энергии

Распространив действие уравнения (7) на всю временную ось получаем уравнение, описывающего изменение знака исходного хаотического сигнала $\xi(t)$ в зависимости от знака выходного сигнала $\varphi(t)$:

$$\chi(t) = \begin{cases} +\xi(t), & \text{sign}(\xi(t)) = \text{sign}(\varphi(t)); \\ -\xi(t), & \text{sign}(\xi(t)) \neq \text{sign}(\varphi(t)), \end{cases} \quad (8)$$

где sign – функция знака:

$$\text{sign}(x) = \begin{cases} 0, & x \geq 0; \\ 1, & x < 0. \end{cases} \quad (9)$$

Уравнение (8) максимизирует взаимную энергию (χ_i, φ_i) , делая ее положительной. Однако возможно преобразование исходного хаотического сигнала, при котором величина (χ_i, φ_i) будет отрицательной:

$$\chi(t) = \begin{cases} +\xi(t), & \text{sign}(\xi(t)) \neq \text{sign}(\varphi(t)); \\ -\xi(t), & \text{sign}(\xi(t)) = \text{sign}(\varphi(t)). \end{cases} \quad (10)$$

Совместное использование уравнений (8) и (10) позволяет организовать передачу данных ρ_i , имеющих не два, а три значения: $\rho_i \in \{-1, 0, +1\}$. При передаче значения 0 взаимная энергия обнуляется благодаря ортогонализации текущего выходного хаотического импульса по отношению к предыдущему, а при передаче значений +1 и -1 – становится соответственно положительной и отрицательной. В этом случае формулы (8) и (10) с учетом (9) преобразуются в следующее уравнение максимизации модуля взаимной энергии:

$$\chi(t) = \begin{cases} +\xi(t), & \text{sign}(\xi(t)) \oplus \text{sign}(\varphi(t)) \oplus \text{sign}(\rho_i) = 0; \\ -\xi(t), & \text{sign}(\xi(t)) \oplus \text{sign}(\varphi(t)) \oplus \text{sign}(\rho_i) = 1, \end{cases} \quad (11)$$

где \oplus – логическая операция «сумма по модулю два».

В итоге формула (6) для взаимной энергии двух соседних выходных импульсов φ_i и φ_{i+1} принимает следующий вид:

$$(\varphi_{i+1}, \varphi_i) = 2(\chi_i, \varphi_i)\rho_i. \quad (12)$$

Следует ожидать, что использование уравнения (11) сохранит хаотические свойства исходного сигнала $\xi(t)$.

Ортохаотический передатчик

Структурная схема ортохаотического передатчика, реализующего формулы (5) и (11), приведена на рис. 2.

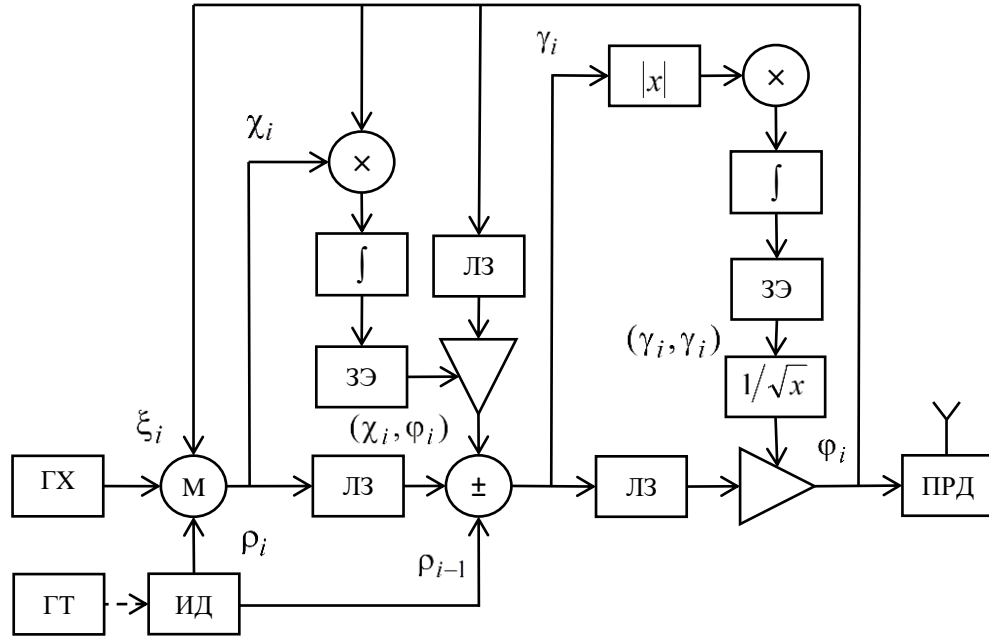


Рис. 2. Ортохаотический передатчик: ГХ – генератор хаоса, ГТ – генератор тактов, М – максимизатор модуля взаимной энергии, ИД – источник данных, ЛЗ – линия задержки на один битовый интервал, $|x|$ – выпрямитель сигнала, \times – одноквадрантный умножитель, \int – интегратор со сбросом, \pm – модулятор, ЗЭ – аналоговый запоминающий элемент, \triangleright – усилитель с изменяемым коэффициентом усиления, ПРД – передающий блок.

Хаотический сигнал $\xi(t)$ от генератора хаоса ГХ поступает в максимизатор взаимной энергии М, на второй вход которого подается задержанный на один битовый интервал и нормализованный выходной сигнал передатчика $\varphi(t)$.

Максимизированный хаотический импульс χ_i задерживается на один битовый интервал, в течение которого вычисляется его взаимная энергия по отношению к предыдущему переданному хаотическому импульсу φ_i , который также задерживается на время вычисления взаимной энергии.

Вычисленное значение взаимной энергии (χ_i, φ_i) в начале каждого такта запоминается в ЗЭ и используется в течение всего такта как величина, задающая коэффициент усиления задержанного выходного импульса φ_i . Предыдущий выходной импульс φ_i , масштабированный взаимной энергией (χ_i, φ_i) , поступает на вход модулятора \pm , управляемого сигналом ρ_i от источника данных ИД.

Полученный в результате модуляции сигналом ρ_i хаотический импульс γ_i задерживается на один битовый интервал, в течение которого вычисляется его энергия (γ_i, γ_i) , которая после преобразования в блоке $1/\sqrt{x}$ служит для нормализации этого импульса и преобразования его в выходной импульс φ_i . Для вычисления энергии хаотического импульса γ_i используется одноквадрантный умножитель, на вход которого подается сигнал с выпрямителя $|x|$.

Так как энергия (γ_i, γ_i) всегда положительная, то реализация блока $1/\sqrt{x}$ может быть легко осуществлена на основе логарифматора, масштабирующего усилителя и антилогарифматора.

Для задания моментов смены сигнала ρ_i , а также для сброса интеграторов и стробирования элементов задержки служит генератор тактов ГТ.

Одна из реализаций выходного ортохаотического сигнала передатчика приведена на рис. 3, где первый переданный хаотический импульс – стартовый.

Ортохаотический приемник

Переданные данные ρ_i на приемной стороне детектируются так:

$$\rho_i = \begin{cases} -1, & (\psi_{i-1}, \psi_i) \leq -\varepsilon; \\ 0, & |(\psi_{i-1}, \psi_i)| < \varepsilon; \\ +1, & (\psi_{i-1}, \psi_i) \geq +\varepsilon, \end{cases} \quad \varepsilon = (\psi_{i-1}, \psi_{i-1})/2, \quad (13)$$

где ψ_i (ψ_{i-1}) – текущий (предыдущий) принятый хаотический импульс вместе с помехой из канала связи; ε – пороговое значение взаимной энергии.

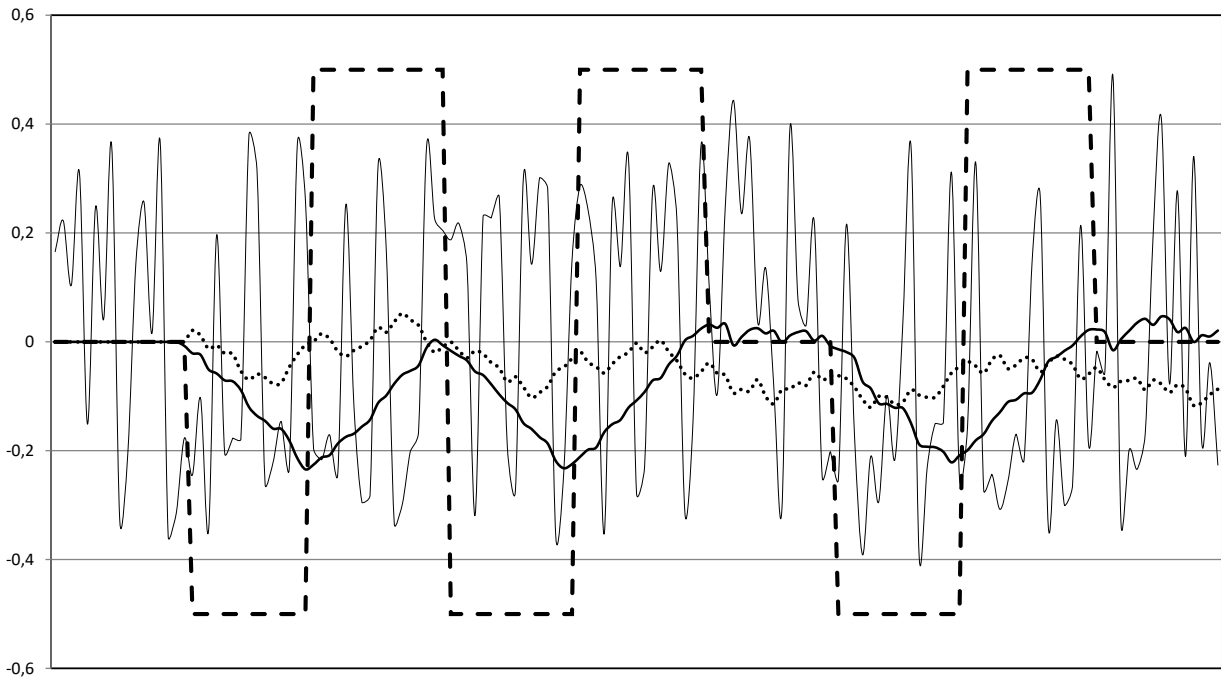


Рис. 3. Ортохаотический сигнал (тонкая линия) при передаче данных $-1+1-1+1 0-1+1 0$ (штриховая линия) и изменение его взаимной энергии при длительности задержки T (толстая линия) и $0,75T$ (пунктирная линия)

Структурная схема ортохаотического приемника, реализующего формулы (13), приведена на рис. 4.

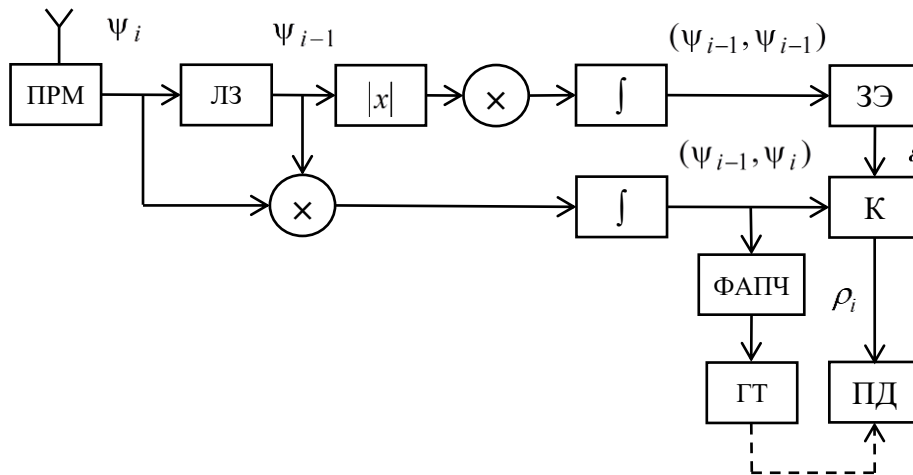


Рис. 4. Ортохаотический приемник: ПРМ – приемный блок, ЛЗ – линия задержки, \times – умножитель, \int – интегратор со сбросом, ЗЭ – аналоговый запоминающий элемент, ГТ – генератор тактов, ФАПЧ – блок фазовой автоподстройки частоты, К – компаратор, ПД – получатель данных.

Для синхронизации битовых интервалов приемника и передатчика используется блок ФАПЧ, на вход которого подается сигнал взаимной энергии прямого и задержанного входного хаотического сигнала (рис. 3). Из рисунка видно, что при близкой частоте тактовых генераторов приемника и передатчика рассогласование их фаз и частот может легко устраняться стандартной схемой фазовой автоподстройки частоты. Единственное требование, которое необходимо соблюдать, – это использование одинаковых линий задержки в приемнике и передатчике (см. рис. 3, пунктирная линия).

Для предотвращения срыва битовой синхронизации при передаче длинных последовательностей, состоящих из одних и тех же знаков данных, может быть использованы специальные методы кодирования данных, предотвращающие появление таких последовательностей.

Использование порогового значения взаимной энергии, равное значению половины энергии предыдущего хаотического импульса позволяет не нормировать приемный тракт по коэффициенту усиления, а также осуществлять прием сигнала при наличии замираний в канале связи.

Помехоустойчивость ортохаотической передачи данных

Результаты вычислительного эксперимента по оценке помехозащищенности относительной ортохаотической передачи данных при различных базах хаотических импульсов $B \in \{8, 16, 32, 64\}$ показаны на рис. 5, где также приведены соответствующие графики 90-процентных доверительных интервалов ДИ8, ДИ16, ДИ32 и ДИ64.

Там же для сравнения отображена теоретическая зависимость вероятности ошибки амплитудной (АМ) и фазовой манипуляции (ФМ) при оптимальном приеме сигналов [15, с. 235].

Заключение

Хорошие корреляционные и спектральные свойства хаотических сигналов позволяют строить эффективные средства связи, работающие при малых отношениях сигнал-шум. Хаотические сигналы обладают высокой

чувствительностью к начальным условиям и значительными различиями в разные моменты времени наблюдения, что позволяет сформировать множество ортогональных хаотических сигналов.

Известно, что хаотические сигналы имеют структурированные аттракторы (фазовые портреты), отличающие их от шума. Последовательная относительная ортогонализация и коллинеаризация хаотических импульсов позволяет скрыть фазовый портрет исходного генератора хаоса и обеспечить схожесть статистических и динамических характеристик выходного сигнала с аналогичными характеристиками шума.

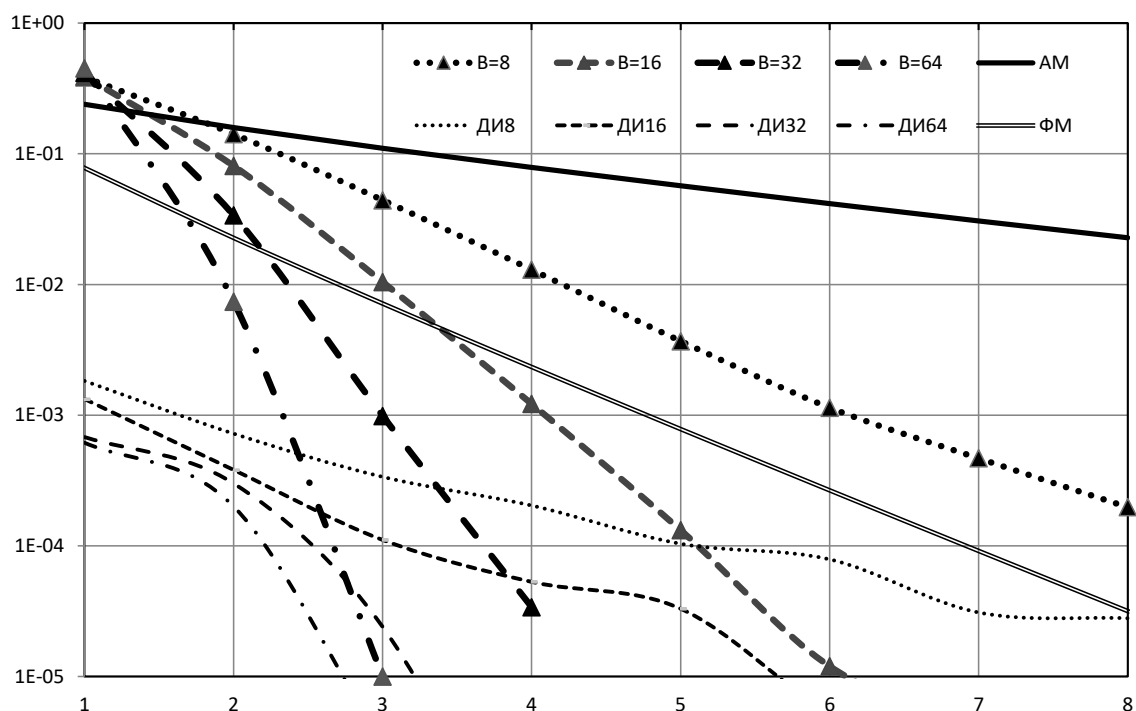


Рис. 5. Зависимость вероятности ошибочного приема одного бита данных от отношения сигнал-шум при различных базах хаотических импульсов

Вычислительный эксперимент показал, что при обнаружении хаотических сигналов на фоне пассивных помех применима традиционная корреляционная обработка, а получаемые при этом вероятности ошибочного приема одного бита при достаточном отношении мощности сигнала к мощности шума в полосе частот приемника лучше, чем при оптимальном приеме сигналов с амплитудной и фазовой манипуляцией.

Для увеличения скрытности передачи можно использовать заранее согласованное изменение длительности хаотических импульсов. Не видится также препятствий для использования генератора шума вместо задающего генератора хаотических сигналов.

Литература

1. Варакин Л.Е. Системы связи с шумоподобными сигналами. М.: Радио и связь, 1985. – 384 с.
2. Кислов В.Я., Колесов В.В., Беляев Р.В. Применение хаотических сигналов в информационных технологиях // Радиоэлектроника. – 2009. – Т. 1, № 1-2. – С. 23–31.
3. Шустер Г. Детерминированный хаос. – М.: Мир, 1988. – 240 с.
4. Дмитриев А.С., Панас А.И. Динамический хаос: Новые носители информации для систем связи. – М.: Физматлит, 2002. – 252 с.
5. Дмитриев А.С., Касьян Г.А., Кузьмин Л.В. Согласованная фильтрация хаотических сигналов // Изв. ВУЗов. Прикладная нелинейная динамика. – 2003. – № 3. – С. 157–164.
6. Yang T.C., Wren T.J. Orthogonal chaotic vector shift keying in digital communications // IET Communications. – 2010. – Vol. 4(6). – P. 739-753.
7. Venkatesh S., Poonam S. Multi User Chaos Based DS-CDMA System Using Orthogonal Chaotic Vector // International Conference On Electronics Systems (ICES'2011). – P. 339-342.
8. Петрович Н.Т., Размахнин М.К. Системы связи с шумоподобными сигналами. – М.: Советское радио, 1969. – 232 с.
9. Sushchik M., Tsimring L.S., Volkovskii A.R. Performance Analysis of Correlation-Based Communication Schemes Utilizing Chaos // IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications. – 2000. – Vol. 47 (12). – P. 1684-1691.

10. Schimming T., Hasler M. Optimal Detection of Differential Chaos Shift Keying // IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications. – 2000. – Vol. 47 (12). – P. 1712-1719.

11. Теория электрической связи: Учебник для вузов / Под ред. Д.Д. Кловского. – М.: Радио и связь, 1999. – 432 с.

12. Корн Г., Корн Т. Справочник по математике для научных работников и инженеров. – М.: Наука, 1973. – 832 с.

13. Короновский А.А., Москаленко О.И., Храмов А.Е. О применении хаотической синхронизации для скрытой передачи информации // Успехи физических наук. – 2009. – Т. 179. – №12. – С. 1281-1310.

14. Генерация хаоса / Под общ. ред. А.С. Дмитриева. – М: Техносфера, 2012. – 424 с.

15. Окунев Ю.Б. Цифровая передача информации фазомодулированными сигналами. М.: Радио и связь, 1991. – 296 с.

Ссылка на статью:

В. С. Выхованец. Ортохаотическая передача данных. Журнал радиоэлектроники [электронный журнал]. 2017. №12. Режим доступа: <http://jre.cplire.ru/jre/dec17/4/text.pdf>