

11

## **Экспериментальная система скрытой передачи информации на генераторе с запаздывающей обратной связью с переключением хаотических режимов**

© А.С. Караваев, Д.Д. Кульминский, В.И. Пономаренко,  
М.Д. Прохоров

Саратовский филиал Института радиотехники и электроники  
им. В.А. Котельникова РАН  
E-mail: mdprokhorov@yandex.ru

*Поступило в Редакцию 27 августа 2014 г.*

Разработана и экспериментально реализована система скрытой передачи информации, основанная на генераторе с запаздывающей обратной связью с переключением хаотических режимов. Показана высокая устойчивость системы к шумам и амплитудным искажениям сигнала в канале связи.

Разработка систем передачи информации, основанных на использовании различных видов хаотической синхронизации, привлекает к себе большое внимание [1–11]. Интерес к хаотическим коммуникационным системам обусловлен тем, что хаотические системы обладают широкополосным спектром мощности, позволяют обеспечить высокую скорость передачи информации и допускают возможность простой аппаратурной реализации с большим выбором различных колебательных режимов. Однако наряду с неоспоримыми достоинствами многие системы связи, основанные на явлении хаотической синхронизации, имеют и существенные недостатки, ограничивающие их широкое распространение [3,7]. К таким недостаткам относятся низкая устойчивость

к шумам и искажениям сигнала в канале связи и жесткие требования, предъявляемые к идентичности параметров приемника и передатчика. В [12] нами была предложена и экспериментально реализована система передачи информации с нелинейным подмешиванием информационного сигнала к хаотической несущей, в которой удалось избавиться от отмеченных недостатков за счет построения передатчика и приемника на программируемых микроконтроллерах и использования цифровой линии передачи.

Оригинальная схема передачи информации с переключением хаотических режимов и аналоговым каналом связи, обладающая высокой устойчивостью к шумам, была нами предложена и численно исследована в [13]. Передатчик представлял собой кольцевую систему из двух линий задержки с временами запаздывания  $\tau_1$  и  $\tau_2$ , нелинейного элемента и линейного фильтра низких частот. В качестве информационного сигнала был выбран бинарный сигнал  $m(t)$ , состоящий из последовательности бинарных 0 и 1, который переключал время запаздывания в системе таким образом, что при передаче бинарного 0 время запаздывания в системе равнялось  $\tau_1$ , а при передаче бинарной 1 время запаздывания равнялось  $\tau_1 + \tau_2$ . При нелинейном элементе, обеспечивающем квадратичное преобразование, такой передатчик описывается дифференциальным уравнением с запаздыванием

$$\varepsilon \dot{x}(t) = -x(t) + \lambda - (x(t - (\tau_1 + m(t)\tau_2)))^2, \quad (1)$$

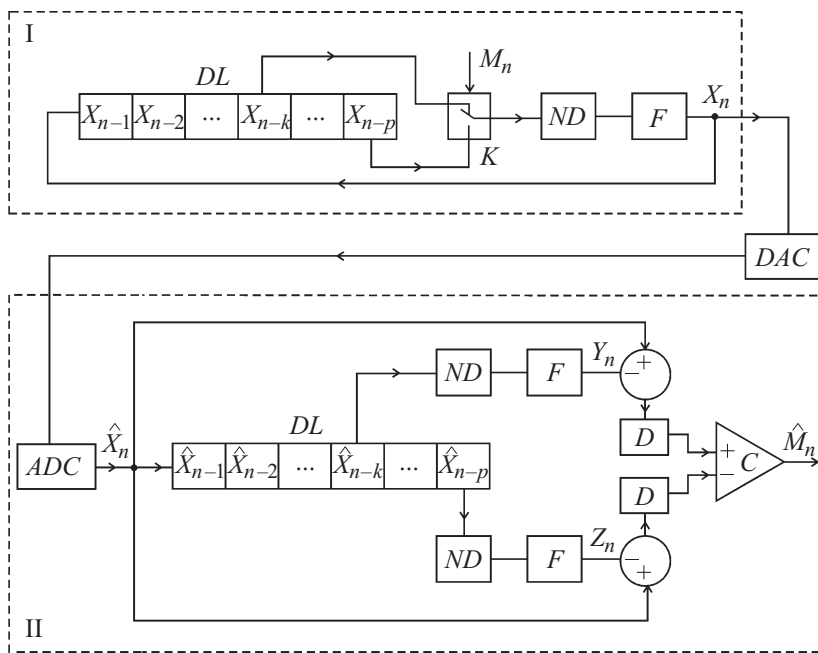
где  $x(t)$  — состояние системы в момент времени  $t$ ,  $\varepsilon$  — параметр, характеризующий инерционность системы,  $\lambda$  — параметр нелинейности. Приемник состоял из 2 ведомых систем с запаздыванием, описываемых уравнениями

$$\varepsilon \dot{y}(t) = -y(t) + \lambda - (x(t - \tau_1))^2, \quad (2)$$

$$\varepsilon \dot{z}(t) = -z(t) + \lambda - (x(t - \tau_3))^2, \quad (3)$$

где  $\tau_3 = \tau_1 + \tau_2$ . Наличие синхронизации хаотической несущей  $x(t)$  с сигналом  $y(t)$  первой ведомой системы приемника говорит о передаче бинарного 0, а синхронизация  $x(t)$  с сигналом  $z(t)$  второй системы — о передаче бинарной 1.

В данной работе мы усовершенствовали схему, исследованную численно в [13], и впервые реализовали ее в радиофизическом эксперименте. Блок-схема предложенной системы связи представлена на



**Рис. 1.** Блок-схема системы передачи информации: I — передатчик, II — приемник, *DL* — линия задержки, *ND* — нелинейный элемент, *F* — фильтр, *K* — коммутирующее устройство, *DAC* — цифроаналоговый преобразователь, *ADC* — аналого-цифровой преобразователь, *D* — детектор, *C* — компаратор.

рис. 1. Все элементы передатчика реализованы в цифровом виде на базе 8-битного микроконтроллера Atmel ATmega328P. Для повышения быстродействия системы все вычисления в микроконтроллере целесообразно проводить с помощью целочисленной арифметики. Для этого необходимо отмасштабировать переменные и параметры уравнения (1), воспользовавшись следующей логикой. При малых  $\epsilon$  допустимые пределы изменения параметра  $\lambda$ , при которых в системе (1) существует периодический или хаотический аттрактор, составляют от 0 до 2. В этих пределах изменения  $\lambda$  динамическая переменная  $x(t)$  может принимать значения от  $-2$  до  $+2$ . Перейдем к целочисленной арифметике, преобразовав уравнение (1) так, чтобы динамическая переменная размещалась в 16-битной ячейке памяти, т.е. чтобы ее

значения изменялись в диапазоне целых чисел от  $-2^{15}$  до  $2^{15}$ . Для этого введем замену:  $X(t) = cx(t)$ ,  $\Lambda = c\lambda$ , где  $c = 2^{14}$  — масштабный коэффициент. В результате уравнение (1) можно записать в следующем виде:

$$\varepsilon \dot{X}(t) = -X(t) + \Lambda - \frac{(X(t - (\tau_1 + m(t)\tau_2)))^2}{c}. \quad (4)$$

Дифференциальное уравнение (4) можно свести к разностному уравнению, более удобному для программной реализации в микроконтроллере. При передаче бинарного 0 передатчик описывается разностным уравнением (5), а при передаче бинарной 1 — уравнением (6):

$$X_{n+1} = aX_n + b \left( \Lambda - \frac{X_{n-k}^2}{c} \right), \quad (5)$$

$$X_{n+1} = aX_n + b \left( \Lambda - \frac{X_{n-p}^2}{c} \right), \quad (6)$$

где  $n$  — дискретное время,  $a = 1 - \Delta t/\varepsilon$ ,  $b = \Delta t/\varepsilon$ ,  $\Delta t$  — шаг по времени, а  $k = \tau_1/\Delta t$  и  $p = \tau_3/\Delta t$  — времена задержки в единицах шагов дискретизации.

Линия задержки передатчика имеет 2 отвода, которые соответствуют дискретным временам запаздывания  $k$  и  $p$  соответственно (рис. 1). Бинарный информационный сигнал  $M_n$  управляет коммутирующим устройством, которое переключает время запаздывания таким образом, что, когда передается бинарный 0, время запаздывания в системе равно  $k$ , а когда передается бинарная 1, время запаздывания равно  $p$ . Сигнал ( $X_{n-k}$  или  $X_{n-p}$ ) с выхода линии задержки поступает на нелинейный элемент, обеспечивающий квадратичное преобразование, а затем проходит низкочастотный цифровой фильтр Баттерворта первого порядка, имеющий постоянную времени  $\varepsilon$ . Динамическая переменная  $X_n$ , наблюдаемая на выходе фильтра, подается на вход линии задержки, замыкая кольцо обратной связи, а также через внешний цифро-аналоговый преобразователь (ЦАП) передается в аналоговый канал связи.

Приемник в схеме реализован на основе такого же программируемого микроконтроллера, что и передатчик. Поступающий из канала связи аналоговый сигнал оцифровывается встроенным аналого-цифровым преобразователем (АЦП) микроконтроллера приемника с частотой дискретизации 1 kHz ( $\Delta t = 1$  ms). Сигнал  $\hat{X}_n$  с выхода АЦП подается на вход линии задержки, отводы которой соответствуют временам

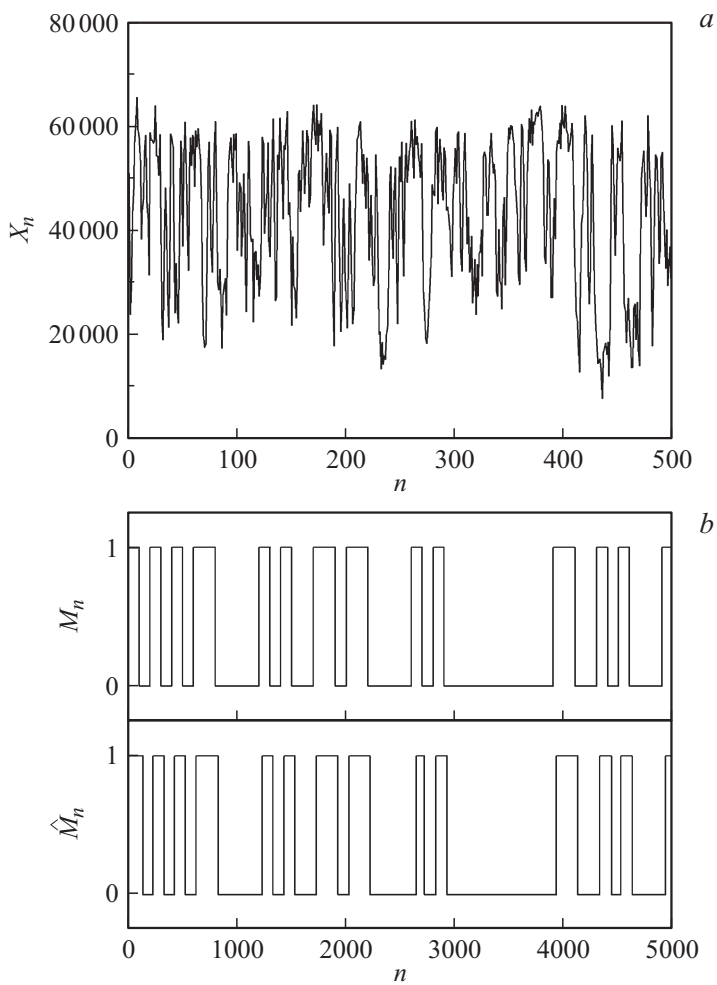
запаздывания  $k$  и  $p$  соответственно (рис. 1). Задержанные сигналы  $\hat{X}_{n-k}$  и  $\hat{X}_{n-p}$  проходят через нелинейные элементы и фильтры, идентичные реализованным в передатчике. Расположенный после фильтра вычитатель разрывает цепь обратной связи каждого из контуров приемника, описываемых уравнениями

$$Y_{n+1} = aY_n + b \left( \Lambda - \frac{\hat{X}_{n-k}^2}{c} \right), \quad (7)$$

$$Z_{n+1} = aZ_n + b \left( \Lambda - \frac{\hat{X}_{n-p}^2}{c} \right). \quad (8)$$

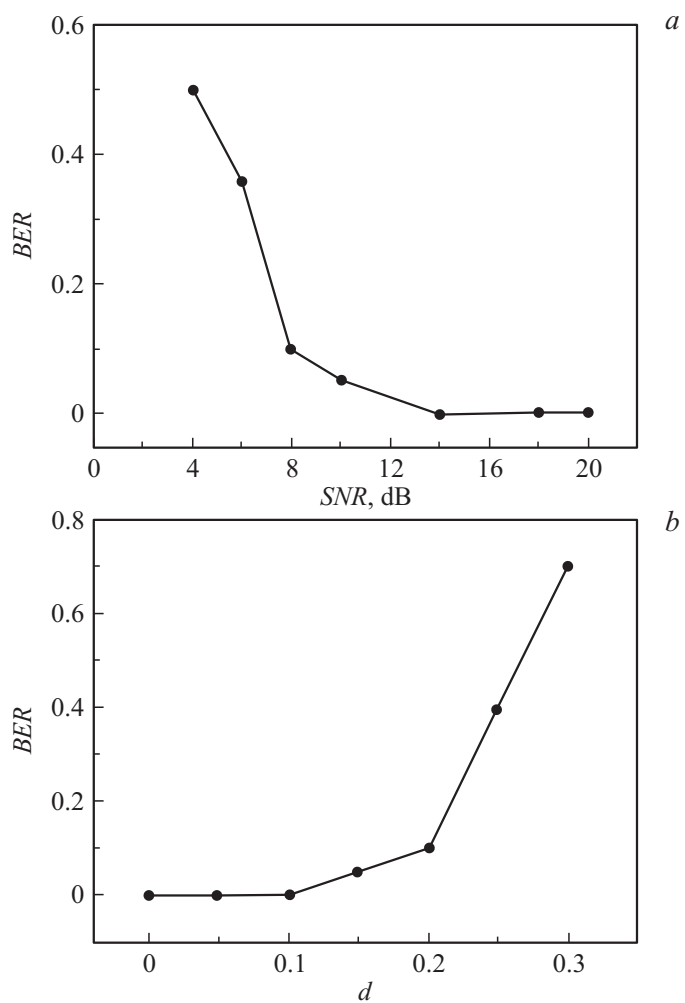
Если передается бинарный 0, то в отсутствие шумов с сигналом  $\hat{X}_n$  синхронизуется выходной сигнал  $Y_n$  первого контура приемника. В результате имеем  $Y_n = \hat{X}_n = X_n$  и сигнал на выходе вычитателя первого контура равен 0. При этом отсутствует синхронизация  $\hat{X}_n$  и выходного сигнала  $Z_n$  второго контура приемника. Поскольку  $Z_n \neq \hat{X}_n$ , сигнал на выходе вычитателя второго контура отличен от 0. Если передается бинарная 1, то  $Y_n \neq \hat{X}_n$ , а  $Z_n = \hat{X}_n$ . В результате на выходе вычитателя первого контура приемника сигнал отличен от 0, а на выходе вычитателя второго контура равен 0. Однако наличие шумов мешает установлению режима полной синхронизации приемника и передатчика. В результате на выходе вычитателей обоих контуров приемника сигнал всегда отличен от 0, что затрудняет восстановление передаваемого бинарного сигнала. При наличии шума в канале связи дисперсия сигнала на выходе вычитателя синхронизованного контура приемника близка к дисперсии шума канала связи, а дисперсия сигнала на выходе вычитателя несинхронизованного контура оказывается близкой к дисперсии хаотической несущей.

Принимая во внимание, что уровень шума канала связи в общем случае существенно меньше уровня хаотической несущей, мы добавили в приемник детекторы и компаратор для увеличения помехоустойчивости схемы (рис. 1). Детекторы оценивают дисперсию поступающего на их вход разностного сигнала по 100 значениям, накопленным в кольцевом буфере в оперативной памяти микроконтроллера. Реализованный программно компаратор вычисляет разность  $R_n$  значений на выходах детекторов и формирует восстановленный информационный сигнал  $\hat{M}_n$ . Если  $R_n \leq 0$ , то на выходе компаратора имеем бинарный 0, в противном случае — бинарную 1.



**Рис. 2.** *a* — фрагмент временной реализации хаотического сигнала  $X_n$ . *b* — фрагменты временных реализаций передаваемого информационного сигнала  $M_n$  и сигнала  $\hat{M}_n$ , выделенного на выходе приемника.

Проиллюстрируем работоспособность предложенной схемы, задав следующие параметры передатчика:  $\lambda = 1.9$ ,  $\Delta t/\varepsilon = 0.5$ ,  $k = 100$ ,  $p = 110$ . На рис. 2, *a* представлен фрагмент временной реализации



**Рис. 3.** *a* — зависимость вероятности ошибки на бит от отношения сигнал/шум. *b* — зависимость вероятности ошибки на бит от амплитудных искажений сигнала в канале связи. В каждом случае передавалась случайная последовательность из  $10^5$  битов.

хаотического сигнала  $X_n$  на выходе передатчика. Поскольку значения  $k$  и  $p$  близки друг другу, соответствующие им участки сигнала  $X_n$  визуально неразличимы, т.е. определить, какой из бинарных символов (0 или 1) передается в канал связи, затруднительно. Временная реализация передаваемого бинарного сигнала  $M_n$  приведена на рис. 2, *b*. Длительность участков с бинарным 0 или 1 кратна 100 ms. Восстановленный информационный сигнал  $\hat{M}_n$  на выходе приемника также показан на рис. 2, *b*. Видно, что информационный сигнал восстанавливается точно, но с некоторой задержкой, величина которой зависит от параметров детекторов.

Для исследования устойчивости предложенной системы передачи информации к шумам и амплитудным искажениям сигнала в канале связи мы разработали специализированную электронную схему, позволяющую добавлять в канал связи шум заданной интенсивности, формируемый генератором шума. На рис. 3, *a* приведена экспериментальная зависимость вероятности ошибки на бит (BER) при передаче бинарного сигнала  $M_n$  от отношения сигнал/шум (SNR), где под сигналом понимается хаотический сигнал, передаваемый в канал связи, а под шумом — добавляемый в канал гауссовский шум, отфильтрованный в полосе частот хаотической несущей. При  $\text{SNR} \geq 14$  dB сигнал  $\hat{M}_n$  выделялся без ошибок.

На рис. 3, *b* приведена зависимость BER от  $d = (A_t - A_r)/A_t$  — амплитудных искажений сигнала в канале связи, где  $A_t$  и  $A_r$  — амплитуды сигналов на выходе передатчика и входе приемника соответственно. При  $d \leq 0.1$  бинарный информационный сигнал на выходе приемника выделялся без ошибок. Таким образом, предложенная нами экспериментальная система передачи информации с переключением хаотических режимов имеет высокую устойчивость к шумам и амплитудным искажениям сигнала в канале связи.

Работа выполнена при поддержке РФФИ, грант № 14-12-00324.

## Список литературы

- [1] Pecora L.M., Carroll T.L. // Phys. Rev. Lett. 1990. V. 64. N 8. P. 821–824.
- [2] Parlitz U., Chua L.O., Kocarev L. et al. // Int. J. Bifurcation and Chaos. 1992. V. 2. N 4. P. 973–977.
- [3] Дмитриев А.С., Панас А.И. Динамический хаос: новые носители информации для систем связи. М.: Физматлит, 2002. 252 с.



- [4] *Chen J.Y., Wong K.W., Cheng L.M., Shuai J.W.* // *Chaos*. 2003. V. 13. N 2. P. 508–514.
- [5] *Tao Y.* // *Int. J. Comput. Cogn.* 2004. V. 2. N 2. P. 81–130.
- [6] *Argyris A., Syvridis D., Larger L.* et al. // *Nature*. 2005. V. 437. N 7066. P. 343–346.
- [7] *Короновский А.А., Москаленко О.И., Храмов А.Е.* // *УФН*. 2009. Т. 179. В. 12. С. 1281–1310. [*Koronovskii A.A., Moskalenko O.I., Hramov A.E.* // *Physics – Uspekhi*. 2009. V. 52. N 12. P. 1213–1238.]
- [8] *Короновский А.А., Москаленко О.И., Храмов А.Е.* // *ЖТФ*. 2010. Т. 80. В. 4. С. 1–8. [*Koronovskii A.A., Moskalenko O.I., Hramov A.E.* // *Tech. Phys.* 2010. V. 55. N 4. P. 435–441.]
- [9] *Nguimdo R.M., Colet P., Larger L., Pesquera L.* // *Phys. Rev. Lett.* 2011. V. 107. N 3. P. 034 103.
- [10] *Kye W.-H.* // *Phys. Lett. A*. 2012. V. 376. N 40–41. P. 2663–2667.
- [11] *Stankovski T., McClintock P.V.E., Stefanovska A.* // *Phys. Rev. X*. 2014. V. 4. N 1. P. 011 026.
- [12] *Ponomarenko V.I., Prokhorov M.D., Karavaev A.S., Kulminskiy D.D.* // *Nonlinear Dyn.* 2013. V. 74. N 4. P. 1013–1020.
- [13] *Пономаренко В.И., Караваев А.С., Глуховская Е.Е., Прохоров М.Д.* // *Письма в ЖТФ*. 2012. Т. 38. В. 1. С. 103–110. [*Ponomarenko V.I., Karavaev A.S., Glukhovskaya E.E., Prokhorov M.D.* // *Tech. Phys. Lett.* 2012. V. 38. N 1. P. 51–54.]