01

Устойчивая к шумам система скрытой передачи информации на хаотическом генераторе с запаздыванием с переключаемым временем задержки

© Д.Д. Кульминский,[1,2] В.И. Пономаренко,[1,2] А.С. Караваев,[1,2] М.Д. Прохоров[1]

[1]Саратовский филиал Института радиотехники и электроники им. В.А. Котельникова РАН,
410019 Саратов, Россия,
[2] Саратовский государственный университет,
410012 Саратов, Россия
e-mail: mdprokhorov@yandex.ru

(Поступило в Редакцию 7 мая 2015 г.)

Предложена система скрытой передачи информации, основанная на генераторе с запаздывающей обратной связью с переключением хаотических режимов. Проведены численные и экспериментальные исследования предложенной системы. Построены зависимости вероятности ошибки на бит при передаче бинарного информационного сигнала от отношения сигнал/шум, затухания сигнала в канале связи и длины интервала времени, в течение которого передается один бит. Показана высокая устойчивость системы к шумам и амплитудным искажениям сигнала в канале связи.

Введение

Открытие возможности синхронизации двух связанных идентичных хаотических систем [1] положило начало разработке систем скрытой передачи информации, основанных на использовании различных видов хаотической синхронизации (полной, с запаздыванием, фазовой, обобщенной). Были предложены различные способы передачи информационного сигнала на основе синхронизации хаотических динамических систем: переключение хаотических режимов [2], хаотическая маскировка [3], хаотическая модуляция [4], нелинейное подмешивание информационного сигнала к хаотическому [5] и другие. Перечисленные способы кодирования информации были использованы для разработки многочисленных систем связи с хаотической несущей [6–12]. Однако оказалось, что многие системы связи, использующие хаотические сигналы, характеризуются в действительности ограниченной конфиденциальностью [13–17]. Для того чтобы повысить уровень защиты передаваемой информации, было предложено осуществлять скрытую передачу данных на основе систем с запаздыванием, демонстрирующих хаотическую динамику высокой размерности [18–21]].

Наряду с неоспоримыми достоинствами, такими как широкополосный спектр мощности, высокая скорость передачи информации и простота аппаратурной реализации, многие системы связи, основанные на явлении хаотической синхронизации, имеют и существенные недостатки, ограничивающие их широкое распространение. К таким недостаткам относятся низкая устойчивость к шумам и искажениям сигнала в канале связи и жесткие требования, предъявляемые к идентичности параметров приемника и передатчика [7,9].

В [21] 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. В настоящей работе предлагается и подробно исследуется оригинальная схема передачи информации с переключением хаотических режимов и аналоговым каналом связи, обладающая высокой устойчивостью к шумам, которая достигается за счет введения в приемник дополнительных элементов. Передатчик и приемник схемы построены на основе систем с запаздывающей обратной связью. В экспериментальной схеме они реализованы в цифровом виде на базе программируемых микроконтроллеров, что обеспечивает идентичность их параметров и улучшает качество информационного сигнала на выходе приемника.

1. Схема передачи информации

Блок-схема предлагаемой системы передачи информации на базе генератора с запаздывающей обратной связью с переключаемым временем задержки представлена на рис. 1. Передатчик представляет собой кольцевую систему из двух линий задержки с временами запаздывания τ_1 и τ_2, нелинейного элемента и линейного фильтра низких частот, генерирующую хаотический сигнал. В качестве информационного сигнала выбран бинарный сигнал $m(t)$, состоящий из последовательности бинарных 0 и 1. Информационный сигнал $m(t)$ управляет коммутирующим устройством, которое переключает время запаздывания в системе таким образом, что, когда передается бинарный 0, время запаздывания в системе равно τ_1, а когда передается бинарная 1, время запаздывания в системе равно $\tau_1 + \tau_2$. Такой передатчик описывается дифференциальным уравнением

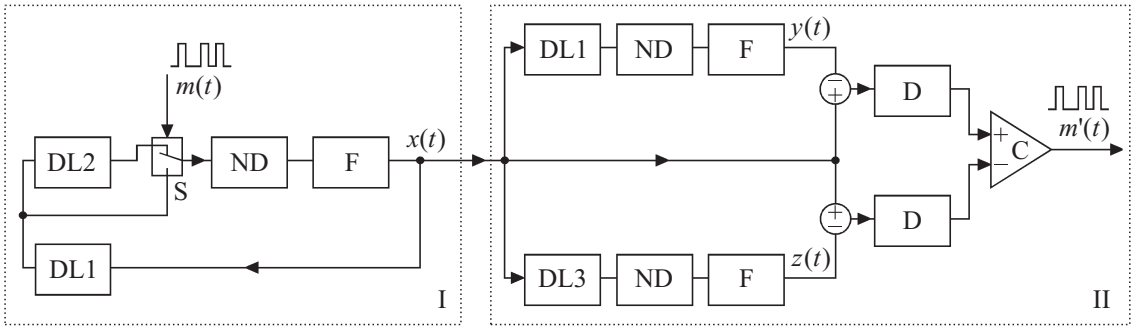

Рис. 1. Блок-схема системы передачи информации с переключением времени задержки: I — передатчик, II — приемник, DL1, DL2, DL3 — линии задержки, ND — нелинейный элемент, F — фильтр, S — коммутирующее устройство, D — детектор, C — компаратор.

первого порядка с запаздыванием

$$\varepsilon \dot{x}(t) = -x(t) + f\Big(x\big(t - (\tau_1 + m(t)\tau_2)\big)\Big), \qquad (1)$$

где $x(t)$ — состояние системы в момент времени t, f — нелинейная функция, ε — параметр, характеризующий инерционность системы. Таким образом, информационный сигнал изменяет параметры передающей системы и соответственно определяет свойства хаотического сигнала, передаваемого в канал связи. Отметим, что в интересах конфиденциальности передачи данных сигналы передатчика должны иметь сходные спектральные и статистические свойства при τ_1 и $\tau_1 + \tau_2$.

Приемник состоит из двух ведомых систем с запаздыванием, одна из которых имеет линию задержки с временем запаздывания τ_1, а вторая — с временем запаздывания $\tau_3 = \tau_1 + \tau_2$ (рис. 1). Параметры фильтров и нелинейных элементов этих систем идентичны соответствующим параметрам передатчика. Расположенный после фильтра вычитатель разрывает цепь обратной связи в каждой из ведомой систем приемника. Входным сигналом для обеих систем с запаздыванием приемника является хаотическая несущая $x(t)$ передатчика. Их уравнения имеют следующий вид:

$$\varepsilon \dot{y}(t) = -y(t) + f\big(x(t - \tau_1)\big), \qquad (2)$$

$$\varepsilon \dot{z}(t) = -z(t) + f\big(x(t - \tau_3)\big). \qquad (3)$$

Параметры передатчика и приемника должны быть выбраны таким образом, чтобы синхронизация с сигналом $x(t)$ в каждый момент времени могла наблюдаться на выходе только одной из ведомой систем. В случае если передается бинарный 0, сигнал $y(t)$ на выходе первой ведомой системы с запаздыванием при отсутствии шума в канале связи синхронизуется с сигналом $x(t)$. В результате имеем $y(t) = x(t)$, и сигнал на выходе вычитателя первой ведомой системы равен 0. В этом случае синхронизация между $x(t)$ и выходным сигналом $z(t)$ второй ведомой системы приемника отсутствует. Так как $z(t) \neq x(t)$, сигнал на выходе вычитателя второй ведомой системы отличен от 0. Если передается бинарная 1, то $y(t) \neq x(t)$, а $z(t) = x(t)$. В результате сигнал на выходе первой ведомой системы отличен от 0, а на выходе второй — равен 0.

На описанном принципе основана работа большинства известных схем связи с переключением хаотических режимов. Однако присутствие шума в канале связи препятствует установлению полной синхронизации между приемником и передатчиком. В результате на выходе вычитателей обеих ведомых систем приемника сигнал всегда отличен от 0, что затрудняет восстановление передаваемого бинарного сигнала.

Для увеличения помехоустойчивости схемы мы модифицировали ее, руководствуясь следующими соображениями. При наличии шума в канале связи дисперсия сигнала на выходе вычитателя синхронизованного контура приемника (имеющего такое же время задержки, как у передатчика) близка к дисперсии шума канала связи, а дисперсия сигнала на выходе вычитателя несинхронизованного контура (время задержки которого отличается от времени задержки в приемнике) оказывается близкой к дисперсии хаотической несущей. Принимая во внимание, что уровень шума канала связи в общем случае существенно меньше уровня хаотической несущей, мы можем точно восстановить скрытое сообщение даже при достаточно высоком уровне шума. Для этого мы добавили в приемник новые элементы — два детектора и компаратор (рис. 1). Детекторы оценивают дисперсию поступающего на их вход разностного сигнала, а компаратор вычисляет разность $r(t)$ значений на выходах детекторов и формирует восстановленный информационный сигнал $m'(t)$. Если $r(t) \leq 0$, то на выходе компаратора имеем бинарный 0, в противном случае — бинарную 1.

2. Численное исследование системы связи

Проиллюстрируем работу предложенной системы передачи информации в численном эксперименте. В качестве передатчика возьмем генератор с запаздывающей обратной связью, имеющий квадратичную нелинейность $f(x) = \lambda - x^2$, где λ — параметр нелинейности,

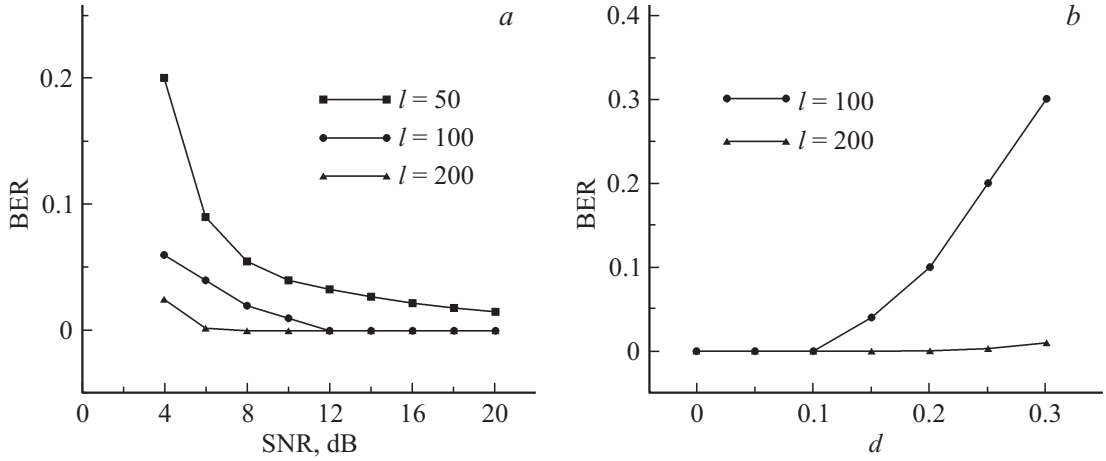

Рис. 2. Зависимости вероятности ошибки на бит от отношения сигнал/шум (a) и от затухания сигнала в канале связи (b).

и фильтр низких частот в виде фильтра Баттерворта первого порядка с частотой среза $f_c = 1/\varepsilon$. В этом случае уравнение передатчика имеет вид

$$\varepsilon \dot{x}(t) = -x(t) + \lambda - \Big(x\big(t - (\tau_1 + m(t)\tau_2)\big)\Big)^2. \quad (4)$$

В приемнике обе ведомые системы с запаздыванием имеют такую же нелинейность и такой же фильтр, как и передатчик. Эти системы описываются уравнениями

$$\varepsilon \dot{y}(t) = -y(t) + \lambda - \big(x(t - \tau_1)\big)^2, \quad (5)$$

$$\varepsilon \dot{z}(t) = -z(t) + \lambda - \big(x(t - \tau_3)\big)^2. \quad (6)$$

Выберем следующие параметры системы: $\tau_1 = 100$, $\tau_2 = 10$, $\tau_3 = 110$, $\lambda = 1.9$, $f_c = 0.5$ $(\varepsilon = 2)$. При этих параметрах передатчик генерирует хаотический сигнал. Каждый бит информационного сигнала $m(t)$ будем передавать в течение интервала времени l. Этот же интервал времени будем использовать для оценки дисперсии сигналов, поступающих на вход детекторов приемника.

Для моделирования шума в канале связи к временному ряду хаотического сигнала передатчика $x(t)$ добавлялся гауссовский шум с нулевым средним, отфильтрованный в полосе частот хаотической несущей. Для различных уровней шума мы восстанавливали бинарный информационный сигнал $m'(t)$ на выходе приемника и строили зависимости вероятности ошибки на бит (BER) от отношения сигнал/шум (SNR), где под сигналом понимается хаотический сигнал, передаваемый в канал связи.

На рис. 2, a построены зависимости BER от SNR для различных значений l. На этом и всех последующих графиках величина BER рассчитывалась при передаче случайной последовательности, содержащей 10^5 бинарных символов 0 и 1. При $l = 100$ и $l = 200$ сигнал сообщения выделяется без ошибок при $\mathrm{SNR} \geq 12\,\mathrm{dB}$ и $\mathrm{SNR} \geq 8\,\mathrm{dB}$ соответственно. То есть предложенная схема демонстрирует более высокую помехоустойчивость, чем большинство других систем передачи информации, использующих хаотическую синхронизацию для передачи скрытого сообщения [7,9].

В реальном канале связи всегда происходит затухание сигнала, которое может оказаться критичным для работы системы передачи информации. Действительно, многие системы связи, особенно хаотические системы с нелинейным подмешиванием и системы с переключением хаотических режимов, имеют низкую устойчивость к искажениям сигнала в канале связи. Для исследования устойчивости предложенной схемы к амплитудным искажениям сигнала мы меняли затухание сигнала в канале связи.

На рис. 2, b построены зависимости BER от параметра $d = (A_t - A_r)/A_t$, где A_t и A_r — амплитуды сигналов на выходе передатчика и входе приемника соответственно. При $l = 100$ и $l = 200$ бинарный информационный сигнал на выходе приемника выделяется без ошибок при $d \leq 0.1$ и $d \leq 0.15$ соответственно. Значение $d = 0.1$ соответствует затуханию сигнала примерно на 1 dB. При таком уровне затухания сигнала в канале связи другие схемы с переключением хаотических режимов и схемы с нелинейным подмешиванием оказываются неработоспособными [9].

Следует отметить, что рассмотренная схема связи, как и все схемы с переключением хаотических режимов, имеет ограничение на скорость передачи информации. Это связано с возникновением переходных процессов после каждого переключения хаотических режимов. После переключения времени задержки в передатчике требуется некоторое время на установление синхронизации между передатчиком и одной из ведомых систем с запаздыванием в приемнике. Скорость передачи информации можно увеличить, уменьшив характерные временные масштабы системы или уменьшив длину временного интервала, в течение которого передается каждый бит. Однако в последнем случае это может привести к увеличению BER при выделении информационного сигнала в приемнике.

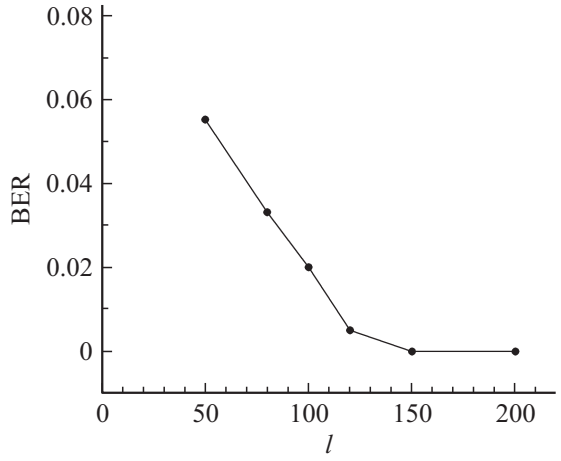

Рис. 3. Зависимость вероятности ошибки на бит от длины интервала времени, в течение которого передается один бит.

На рис. 3 приведена зависимость BER от длины l интервала времени, в течение которого передается один бит, построенная при $\mathrm{SNR} = 8\,\mathrm{dB}$ и $d = 0$. В области малых значений l с уменьшением l наблюдается рост BER. С другой стороны, при высоких уровнях шума в канале связи можно улучшить качество восстановления информационного сигнала, увеличив величину l, что приведет к уменьшению BER.

3. Экспериментальная реализация схемы передачи информации

Предложенная система передачи информации на основе генератора с запаздывающей обратной связью с переключением хаотических режимов реализована нами в радиофизическом эксперименте. Для обеспечения полной идентичности параметров передатчика и приемника все элементы схемы реализованы в цифровом виде на базе простых 8-битных программируемых микроконтроллеров семейства Atmel megaAVR.

Для повышения быстродействия системы все вычисления в микроконтроллере целесообразно проводить с помощью целочисленной арифметики. Для этого необходимо отмасштабировать переменные и параметры уравнения (4), воспользовавшись следующей логикой. При малых ε допустимые пределы изменения параметра λ, при которых в системе (4) существует периодический или хаотический аттрактор, составляют от 0 до 2. В этих пределах изменения λ динамическая переменная $x(t)$ может принимать значения от -2 до $+2$. Перейдем к целочисленной арифметике, преобразовав уравнение (4) так, чтобы динамическая переменная размещалась в 16-битной ячейке памяти, т.е. чтобы ее значение изменялось 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 (4) можно записать в следующем виде:

$$\varepsilon \dot{X}(t) = -X(t) + \Lambda - \frac{\big(X - (t - (\tau_1 + m(\tau)\tau_2))\big)^2}{c}. \quad (7)$$

Дифференциальное уравнение (7) можно свести к разностному уравнению, более удобному для программной реализации в микроконтроллере. При передаче бинарного 0 передатчик описывается разностным уравнением (8), а при передаче бинарной 1 — уравнением (9)

$$X_{n+1} = aX_n + b\left(\Lambda - \frac{X_{n-k}^2}{c}\right), \quad (8)$$

$$X_{n+1} = aX_n + b\left(\Lambda - \frac{X_{n-p}^2}{c}\right), \quad (9)$$

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

Блок-схема экспериментальной системы передачи информации представлена на рис. 4. Линия задержки передатчика имеет 2 отвода, которые соответствуют дискретным временам запаздывания k и p соответственно. 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 частоту среза $f_c = 1/\varepsilon$. Динамическая переменная X_n, наблюдаемая на выходе фильтра, подается на вход линии задержки, замыкая кольцо обратной связи, а также через цифроаналоговый преобразователь 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 аналогоцифровым преобразователем (АЦП) микроконтроллера приемника с частотой дискретизации 1 kHz ($\Delta t = 1\,\mathrm{ms}$). Сигнал $\hat{X}_n$ с выхода АЦП подается на вход линии задержки, отводы которой соответствуют временам запаздывания k и p соответственно (рис. 4). 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

$$Y_{n+1} = aY_n + b\left(\Lambda - \frac{\hat{X}_{n-k}^2}{c}\right), \quad (10)$$

$$Z_{n+1} = aZ_n + b\left(\Lambda - \frac{\hat{X}_{n-p}^2}{c}\right). \quad (11)$$

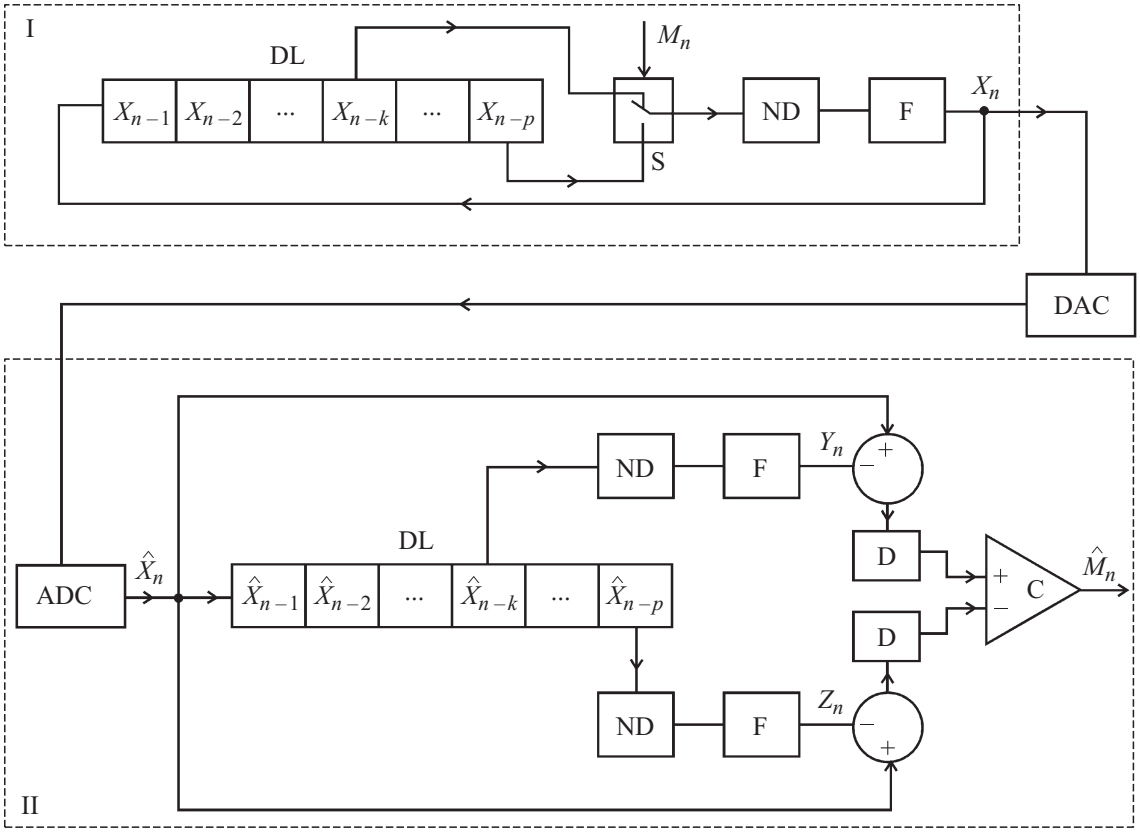

Рис. 4. Блок-схема экспериментальной системы передачи информации: I — передатчик, II — приемник, DL — линия задержки, ND — нелинейный элемент, F — фильтр, S — коммутирующее устройство, DAC — цифроаналоговый преобразователь, ADC — аналогоцифровой преобразователь, D — детектор, C — компаратор.

Детекторы оценивают дисперсию поступающего на их вход разностного сигнала по 100 значениям, накопленным в кольцевом буфере в оперативной памяти микро-контроллера. Расположенный после детекторов компаратор вычисляет разность R_n значений на их выходах и формирует восстановленный информационный сигнал $\hat{M}_n$. Если $R_n \le 0$, то на выходе компаратора имеем бинарный 0, в противном случае — бинарную 1.

Представленная на рис. 4 схема была впервые экспериментально реализована в нашей недавней работе [22]. Однако техническим недостатком экспериментального макета являлось наличие постоянного смещения сигнала в канале связи. Это смещение снижало устойчивость схемы к шумам и приводило к ухудшению качества приема информационного сигнала. При высоких уровнях шума величина BER в экспериментальной схеме была на порядок выше, чем при численном моделировании (разд. 2). Результаты численного исследования схемы, впервые проведенного в настоящей работе, позволили выявить и устранить причину потери качества информационного сигнала на выходе экспериментальной системы.

Мы усовершенствовали экспериментальную установку, добавив в нее схему подстройки постоянного смещения сигнала в канале связи. Это позволило на порядок уменьшить величину BER при высоких уровнях шума и в разы уменьшить BER при большом затухании сигнала. Для исследования устойчивости экспериментальной системы передачи информации к шумам и амплитудным искажениям сигнала в канале связи была разработана специализированная электронная схема, позволяющая добавлять в канал связи шум заданной интенсивности, формируемый генератором шума, и менять затухание сигнала.

4. Исследование экспериментальной системы передачи информации

Проиллюстрируем работоспособность модифицированной экспериментальной схемы, задав такие же значения параметров, как при численном исследовании системы: $k = 100$, $p = 110$, $\lambda = 1.9$, $\Delta t/\varepsilon = 0.5$. На рис. 5, *a* представлен фрагмент временной реализации 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. 5, *b*. Каждый бит передается в течение интервала времени $l = 100\,\text{ms}$, соответствующего

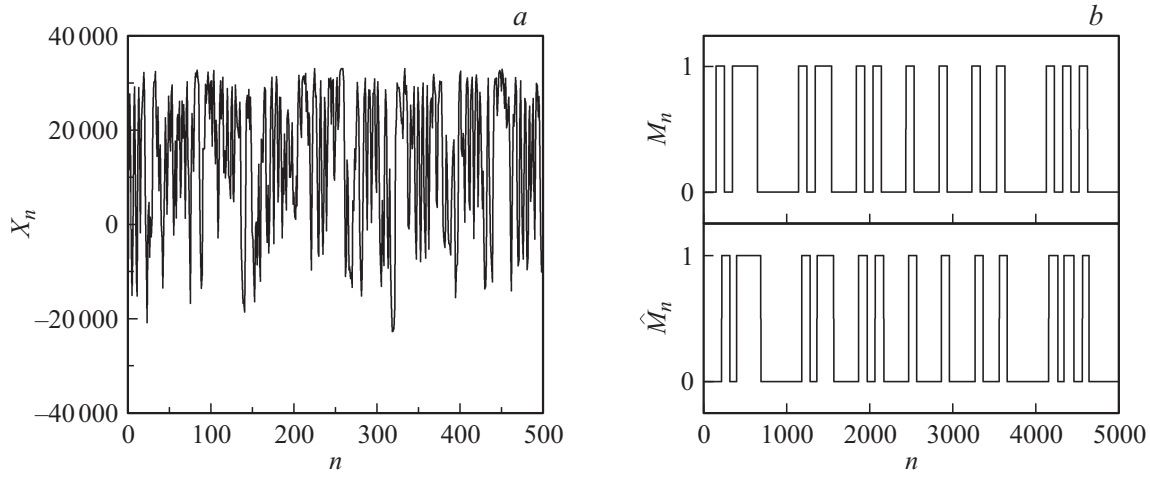

Рис. 5. Фрагменты временных реализаций хаотического сигнала X_n — *a* и информационных сигналов M_n и $\hat{M}_n$ — *b*.

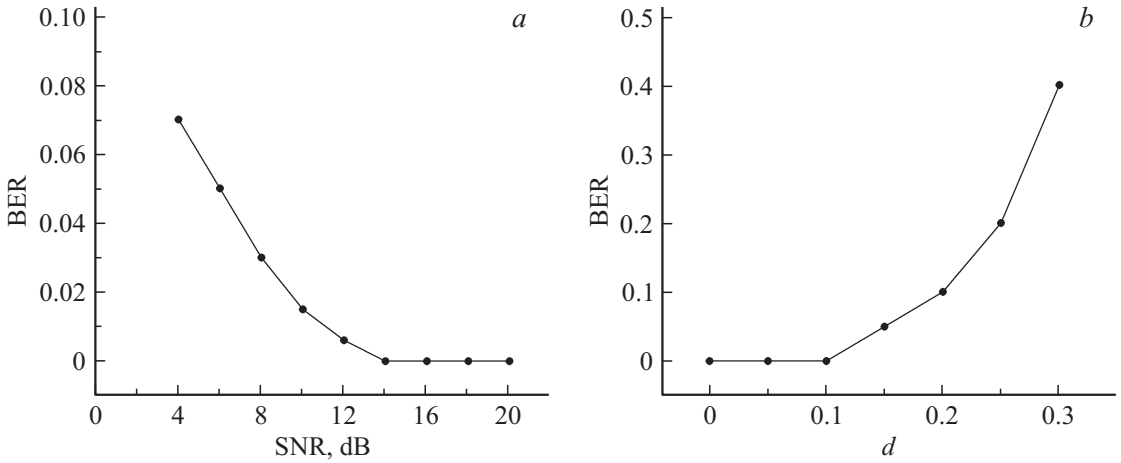

Рис. 6. Экспериментальные зависимости вероятности ошибки на бит от отношения сигнал/шум (*a*) и от затухания сигнала в канале связи (*b*)

100 шагам дискретного времени *n*. Восстановленный информационный сигнал $\hat{M}_n$ на выходе приемника также показан на рис. 5, *b*. Видно, что информационный сигнал восстанавливается точно, но с некоторой задержкой, величина которой зависит от параметров детекторов.

На рис. 6, *a* приведена экспериментальная зависимость BER от отношения сигнал/шум, 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 SNR $\geq$ 14 dB сигнал $\hat{M}_n$ выделяется без ошибок. То есть в реальной экспериментальной установке удается получить почти такую же высокую помехоустойчивость, как и при численном моделировании (рис. 2, *a*). По устойчивости к шуму предложенная нами экспериментальная схема в несколько раз превосходит остальные экспериментальные системы передачи информации, использующие хаотическую синхронизацию для передачи скрытого сообщения через аналоговый канал связи [7,9].

На рис. 6, *b* приведена экспериментальная зависимость BER от параметра *d*. Также как и в модельной систе-

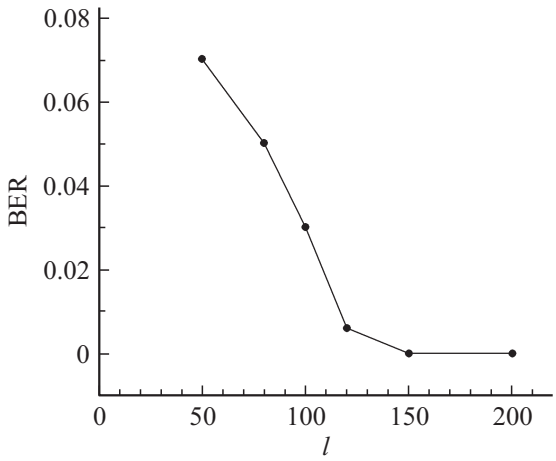

Рис. 7. Экспериментальная зависимость вероятности ошибки на бит от длины интервала времени, в течение которого передается один бит.

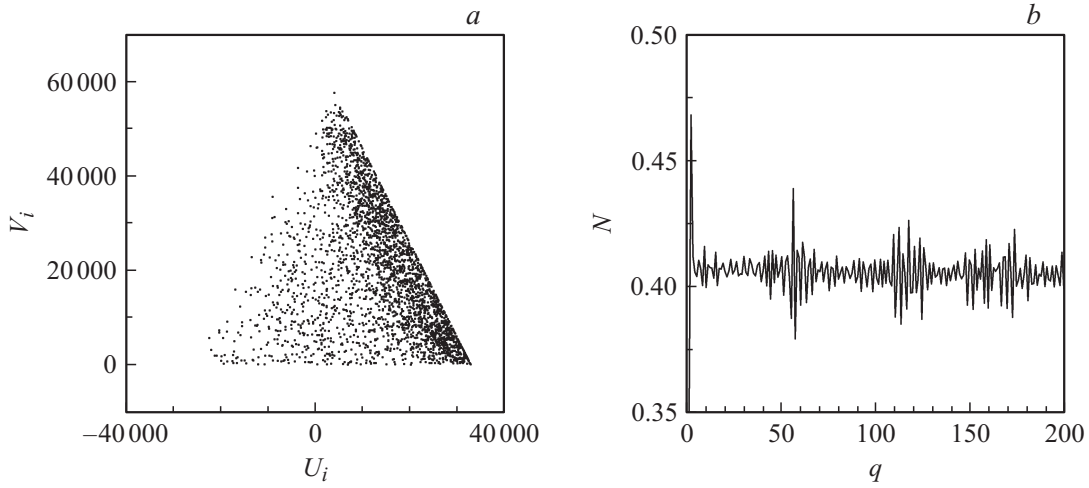

Рис. 8. *a* — отображение последования для экспериментальной системы передачи информации, *b* — число N пар экстремумов в экспериментальном временном ряде на удалении q друг от друга, нормированное на общее число экстремумов.

ме (рис. 2, *b*), при $d \leq 0.1$ бинарный информационный сигнал на выходе приемника выделяется без ошибок. По устойчивости к затуханию сигнала в канале связи исследуемая экспериментальная схема в разы превосходит другие экспериментальные системы связи на основе синхронизации хаотических систем [9].

На рис. 7 построена зависимость BER от величины l для случая SNR = 8 dB и $d = 0$. Значения l указаны в единицах шага выборки точек Δt. Полученные значения BER оказываются близкими к значениям, полученным в численном эксперименте (рис. 3). Для рассмотренной экспериментальной системы, построенной на базе микроконтроллеров семейства Atmel megaAVR, значение $l = 100$ ms, по-видимому, является оптимальным. При меньших l схема менее устойчива к шуму, а при больших l требуется больше памяти микроконтроллера и уменьшается скорость передачи информации.

Известно, что многие системы передачи информации, использующие хаотические сигналы, характеризуются в действительности ограниченной конфиденциальностью [13–17]. Показано, что скрытый информационный сигнал может быть выделен сторонним наблюдателем с помощью построения отображений последования [13,14], а также с помощью методов реконструкции динамической системы по временному ряду [15,16] и некоторых других методов [17]. Для проверки скрытности предложенной системы связи мы сначала применили метод выделения передаваемого сообщения, основанный на построении отображений последования.

Пусть $n = i_{\max}$ — время, при котором сигнал $\hat{X}_n$ имеет i-й локальный максимум S_i, а $n = i_{\min}$ — время, при котором $\hat{X}_n$ имеет i-й локальный минимум T_i. Построим отображения последования S_{i+1} от S_i, T_{i+1} от T_i и V_i от U_i, где $U_i = (S_i + T_i)/2$, $V_i = S_i - T_i$. На рис. 8, *a* показано отображение последования V_i от U_i, построенное по максимумам и минимумам временного ряда сигнала $\hat{X}_n$ для случая, когда мы не добавляли шум к сигналу в канале связи. В отличие от отображений последования, представленных в [13], рис. 8, *a* не демонстрирует никаких одномерных кривых, которые соответствуют различным переключаемым хаотическим режимам и могут быть использованы для выделения информационного сигнала. Отображения S_{i+1} от S_i и T_{i+1} от T_i также не имеют одномерных кривых. Кроме того, рассмотренные отображения последования оказываются визуально одинаковыми для случаев фиксированного и переключаемого времени задержки в передатчике. То есть метод построения отображений последования, позволяющий неавторизованному пользователю выделить скрытое сообщение во многих системах связи на основе хаотических сигналов низкой размерности, оказывается неработоспособным для нашей системы связи, построенной на генераторе с запаздыванием, демонстрирующем хаотическую динамику высокой размерности.

Другой подход, часто используемый для проверки скрытности системы передачи информации, основан на применении методов реконструкции модельного уравнения передатчика по временному ряду сигнала в канале связи [15]. Если передатчик построен на основе хаотической системы с запаздыванием, то для восстановления его параметров необходимо применять методы, разработанные специально для систем с задержкой [18,19,23,24]. Одним из таких методов является метод, основанный на статистическом анализе интервалов между экстремумами временного ряда. Установлено, что во временных рядах систем первого порядка с запаздыванием практически отсутствуют экстремумы, удаленные друг от друга на время запаздывания [24]. Определив для различных значений q количество N ситуаций, при которых точки хаотического временного ряда, разделенные интервалом времени q, одновременно являются экстремальными и построив зависимость $N(q)$, можно восстановить время запаздывания по положению абсолютного минимума $N(q)$ [24]. Для систем с двумя временами задержки зависимость $N(q)$ имеет отчетливо выраженные минимумы при значениях q, соответствующих этим задержкам.

Применим этот метод к хаотическому временному ряду сигнала $\hat{X}_n$. Подсчитав число N одновременных

обращений в нуль производных сигналов $\hat{X}_n$ и $\hat{X}_{n-q}$ для различных значений q, перебираемых с шагом, равным 1, построим зависимость $N(q)$, рис. 8, *b*. Для оценки производных по временному ряду мы использовали локальную параболическую аппроксимацию. График $N(q)$ построен по временному ряду длиной 30 000 точек для случая, когда мы не добавляли шум к сигналу в канале связи. Представленная на рис. 8, *b* зависимость $N(q)$ не позволяет восстановить переключаемые времена запаздывания $k = 100$ и $p = 110$.

Следует отметить, что для выделения скрытого информационного сигнала стороннему наблюдателю недостаточно знать о существовании нескольких задержек в системе. Необходимо знать значение времени запаздывания в текущий момент. А для этого нужно восстанавливать время запаздывания по короткому временному ряду, сопоставимому с длиной l интервала времени, в течение которого передается один бит. В нашей схеме значения l сопоставимы со значениями самих задержек. По таким коротким временным рядам очень сложно восстановить время запаздывания с помощью любых методов реконструкции динамических систем.

Заключение

Предложена система скрытой передачи информации, основанная на переключении хаотических режимов в генераторе с запаздывающей обратной связью, которая демонстрирует высокую устойчивость к шумам и затуханию сигнала в канале связи. Предложенная система связи исследована численно и реализована экспериментально. В экспериментальной схеме передатчик и приемник реализованы в цифровом виде на базе программируемых микроконтроллеров. Использование цифровых элементов обеспечивает идентичность параметров приемника и передатчика и повышает качество выделения передаваемого информационного сигнала на выходе приемника.

Мы проиллюстрировали эффективность исследованной системы связи при передаче бинарного информационного сигнала. Построены модельные и экспериментальные зависимости вероятности ошибки на бит от отношения сигнал/шум, затухания сигнала в канале связи и длины интервала времени, в течение которого передается один бит. Показано, что по устойчивости к шуму и к затуханию сигнала предложенная экспериментальная схема в несколько раз превосходит остальные экспериментальные системы передачи информации, использующие хаотическую синхронизацию для передачи скрытого сообщения через аналоговый канал связи. Высокое качество передачи скрытого информационного сигнала через аналоговый канал, в котором передаваемый сигнал неизбежно подвергается шумам и искажениям, расширяет сферу применения предложенной схемы связи, открывая, в частности, возможность построения подобных систем передачи данных в СВЧ-диапазоне с использованием радиоканала.

С помощью построения отображений последования и метода восстановления времени задержки, основанного на статистическом анализе экстремумов временного ряда, исследована скрытность предложенной экспериментальной системы связи.

Работа выполнена при поддержке Российского научного фонда, грант № 14-12-00324.

Список литературы

[1] *Pecora L.M., Carroll T.L.* // Phys. Rev. Lett. 1990. Vol. 64. P. 821–824.
[2] *Parlitz U., Chua L.O., Kocarev L.* et al. // Int. J. Bifurcation and Chaos. 1992. Vol. 2. P. 973–977.
[3] *Cuomo K.M., Oppenheim A.V.* // Phys. Rev. Lett. 1993. Vol. 71. P. 65–68.
[4] *Halle K.S., Wu C.W., Itoh M., Chua L.O.* // Int. J. Bifurcation and Chaos. 1993. Vol. 3. P. 469–477.
[5] *Волковский А.Р., Рульков Н.Ф.* // Письма в ЖТФ. 1993. Т. 19. Вып. 3. С. 71–75.
[6] *Van Wiggeren G.D., Roy R.* // Science. 1998. Vol. 279. P. 1198–1200.
[7] *Дмитриев А.С., Панас А.И.* Динамический хаос: новые носители информации для систем связи. М.: Физматлит, 2002. 252 с.
[8] *Argyris A., Syvridis D., Larger L.* et al. // Nature. 2005. Vol. 437. P. 343–346.
[9] *Короновский А.А., Москаленко О.И., Храмов А.Е.* // УФН. 2009. Т. 179. Вып. 12. С. 1281–1310.
[10] *Короновский А.А., Москаленко О.И., Храмов А.Е.* // ЖТФ. 2010. Т. 80. Вып. 4. С. 1–8.
[11] *Wang M.-J., Wang X.-Y., Pei B.-N.* // Nonlinear Dyn. 2012. Vol. 67. P. 1097–1104.
[12] *Abderrahim N.W., Benmansour F.Z., Seddiki O.* // Nonlinear Dyn. 2014. Vol. 78. P. 197–207.
[13] *Pérez G., Cerdeira H.A.* // Phys. Rev. Lett. 1995. Vol. 74. P. 1970–1973.
[14] *Zhou C.-S., Chen T.-L.* // Phys. Lett. A. 1997. Vol. 234. P. 429–435.
[15] *Short K.M.* // Int. J. Bifurcation and Chaos. 1997. Vol. 7. P. 1579–1597.
[16] *Ponomarenko V.I., Prokhorov M.D.* // Phys. Rev. E. 2002. Vol. 66. 026215.
[17] *Alvarez G., Li S.* // Int. J. Bifurcation and Chaos. 2006. Vol. 16. P. 2129–2151.
[18] *Udaltsov V.S., Goedgebuer J.-P., Larger L., Rhodes W.T.* // Phys. Rev. Lett. 2001. Vol. 86. P. 1892–1895.
[19] *Пономаренко В.И., Прохоров М.Д.* // РиЭ. 2004. Т. 49. С. 1098–1104.
[20] *Kye W.-H.* // Phys. Lett. A. 2012. Vol. 376. P. 2663–2667.
[21] *Ponomarenko V.I., Prokhorov M.D., Karavaev A.S., Kulminskiy D.D.* // Nonlinear Dyn. 2013. Vol. 74. P. 1013–1020.
[22] *Караваев А.С., Кульминский Д.Д., Пономаренко В.И., Прохоров М.Д.* // Письма в ЖТФ. 2015. Т. 41. Вып. 1. С. 3–11.
[23] *Zhou C., Lai C.-H.* // Phys. Rev. E. 1999. Vol. 60. P. 320–323.
[24] *Пономаренко В.И., Прохоров М.Д., Караваев А.С., Безручко Б.П.* // ЖЭТФ. 2005. Т. 127. Вып. 3. С. 515–527.