УДК 004

А.А. Колесников, А.С. Капустина
(Технологический институт Южного федерального университета;
e-mail: anatoly.kolesnikov@gmail.com)

СИНЕРГЕТИЧЕСКИЙ МЕТОД СИНТЕЗА СИСТЕМ ХАОСОДИНАМИЧЕСКОЙ ОБРАБОТКИ И ЗАЩИТЫ ИНФОРМАЦИИ

Предложен способ скрытой передачи информации, основанный на применении широкополосных излучений в качестве несущего сигнала.

Ключевые слова: динамическая система, хаос, аттрактор, синергетический наблюдатель, хаотический генератор, защита информации.

A.A. Kolesnikov, A.S. Kapustina

SYNERGETICS METHOD OF SYSTEM SYNTHESIS FOR DATA CHAOTIC-DYNAMICS PROCESSING AND SECURING

We propose the method of hidden data transmission that is based on using the broadband radiations as carrying signal.

Key words: dynamics system, chaos, attractor, synergetics observer, chaotic generator, data securing.

Статья поступила в редакцию 24 сентября 2010 г.

Введение

В последние годы бурно развивается принципиально новое научное направление, основанное на явлении самоорганизации в нелинейных системах с динамическим хаосом. Эти системы характеризуются так называемыми "странными" аттракторами, которые могут применяться в качестве гибких информационных процессоров, эффективно обрабатывающих информацию. Суть нового подхода состоит в том, что информация порождается как каскадом бифуркаций, приводящих к нарушению симметрии в системе, так и её хаотической диссипативной динамикой, приводящей к всё более тонкому разрешению процессов.

К генераторам информации – аттракторам предъявляются следующие основные требования: во-первых, большая емкость памяти и, во-вторых, способность к значительному сжатию информации. Известно, что регулярные аттракторы типа Ван дер Поля, Релея, Пуанкаре и др., имеющие размерность 1, малоэффективны как модули для хранения информации, но практически идеальны как устройства для сжатия информации [1]. Однако в нелинейной динамике были обнаружены хаотические ("странные") аттракторы, обладающие, с информационной точки зрения, универсальными свойствами: с одной стороны, они имеют значительную информационную размерность, а с другой – они являются "компрессорами" информации.

Указанные свойства оказались весьма неожиданными для науки. Дело в том, что хаотические аттракторы, например, типа Лоренца, осуществляют про-

цессы обработки информации путем уменьшения числа степеней свободы в фазовом пространстве, когда динамическая система, стартуя из определенного множества начальных условий размерности n_0, через некоторое время неизбежно попадет на некоторый регулярный аттрактор – притягивающее множество, имеющий значительно меньшую размерность ($n_1 << n_0$). Это – процесс сжатия фазового пространства, который называют самоорганизацией системы. Таким образом, методы нелинейной динамики дают возможность создания принципиально новых методов обработки информации.

1. Метод динамической обработки и защиты информации с использованием синергетического наблюдателя

В последнее время в литературе был предложен ряд способов скрытой передачи информации, основанных на применении в качестве несущих сигналов широкополосных излучений генераторов хаоса, называемых далее "хаотическими генераторами" (ХГ) [2-7]. При этом с целью выделения сигнала из хаотического обычно используется явление хаотической синхронизации.

Но такие способы имеют ряд недостатков, наиболее существенным из которых является требование идентичности генераторов хаотических колебаний в приёмнике и передатчике. Так, если параметры этих генераторов отличаются всего лишь на 2 %, то указанный способ становится неэффективным [5]. Другой, более перспективный подход к реконструкции передаваемой информационных сигналов с использованием параметрически модулированных хаотических генераторов был предложен в работах [6, 7]. Суть этого подхода заключается в следующем. Исходная динамическая система, генерирующая обрабатываемый сигнал, описывается нелинейными дифференциальными уравнениями:

$$\frac{\mathrm{d}x}{\mathrm{d}t} = F(x, \mu^0), \qquad x \in R^n, \ \mu^0 \in R^m, \tag{1}$$

где x – вектор переменных состояния ХГ;

F – вектор правых частей модели ХГ;

μ^0 – вектор постоянных номинальных параметров ХГ.

Отдельные параметры вектора μ^0 достаточно медленно модулируются передаваемыми информационными сигналами $\mu_i(t)$. В результате образуются новые параметры ХГ:

$$\mu_i^*(t) = \mu_i^0 + \mu_i(t), \qquad i = 1, ..., m, \tag{2}$$

где μ_i^0 – постоянные значения параметров системы (1);

$\mu_i(t)$ – информационные сигналы.

Условия медленной модуляции можно представить в форме следующего неравенства:

$$\left|\overline{\frac{\mathrm{d}\mu_i}{\mathrm{d}t}}\right| << \left|\overline{\frac{\mathrm{d}x_j}{\mathrm{d}t}}\right| \tag{3}$$

для любых i и j. Тогда система уравнений (1) с учетом (2) принимает вид:

$$\frac{\mathrm{d}x}{\mathrm{d}t} = F\left(x, \mu^0 + \mu(t)\right), \tag{4}$$

где $\mu^0 = \left(\mu_1^0, \mu_2^0, ..., \mu_m^0\right)$, $\mu(t) = (\mu_1(t), \mu_2(t), ..., \mu_m(t))$.

Как показано в [6, 7], путём соответствующей замены переменных модели многих ХГ вида (4) можно преобразовать к виду:

$$\dot{x}_1(t) = x_2;\ \ \dot{x}_2 = x_3;\ ...\ \dot{x}_{n-1} = x_n;\ \dot{x}_n = f(x, \mu^*) \tag{5}$$

Далее генерируемый сигнал, например $x_n(t)$, передается в канал связи, а на принимающей стороне значения сигналов $x_1(t), ..., x_{n-1}(t)$ получаются последовательно путем интегрирования системы уравнений (5). При этом на принимающей стороне по известным значениям сигналов $x_i(t), i = 1,...,n$ вычисляются параметры μ^* посредством метода наименьших квадратов на основе уравнения

$$f(x, \mu^*) = 0. \tag{6}$$

В конечном итоге реконструированные информационные сигналы находятся из выражения (2):

$$\hat{\mu}_i(t) = \hat{\mu}_i^*(t) - \mu_i^0,$$

где $\hat{\mu}_i(t)$ – реконструированный информационный сигнал;

$\hat{\mu}_i^*(t)$ – реконструированный модулированный параметр.

Это означает, что, согласно (3), предложенный в [6, 7] подход к реконструкции сигналов по своей сути является статическим со всеми вытекающими отсюда последствиями. Дело в том, что условие (3) требует выбора такого временного окна t^*, что в его пределах значения параметров $\mu_i^* \approx \text{const}$ допустимо еще считать практически постоянными.

Иначе говоря, в течение времени t^* неавтономность системы (4) в расчёт не принимается. Тогда, скользя временным окном вдоль несущего сигнала, например, $x_n(t)$, можно на основе математической модели ХГ (5) осуществить выделение сигналов модуляции $\mu_i(t)$ в реальном времени [6, 7]. Однако в нелинейной динамике хорошо известно свойство повышенной чувствительности ХГ типа Лоренца, Релея и др. к малым изменениям их "управляющих параметров" и начальных условий. Эти особенности ХГ могут привести к практическим затруднениям при реализации описанного способа обработки и защиты информации. В этой связи, находясь в рамках идеологии глобальной реконструкции [5-7], предлагается динамический метод обработки информации, основанный на текущем вычислении параметров $\mu_i^*(t)$ с помощью синергетического наблюдателя [8-10].

Методику и синтез динамического наблюдателя проиллюстрируем на конкретном примере ХГ, представленного моделью Лоренца [5-7]:

$$\dot{x}(t) = \sigma(y - x); \quad \dot{y}(t) = rx - y - xz; \quad \dot{z}(t) = -bz + xy, \tag{7}$$

где x, y, z – переменные состояния;

σ, r, b – постоянные (номинальные) параметры.

Сначала преобразуем модель (7) к виду (5), для чего используем замену переменных [5]:

$$X = x;\ \ Y = \sigma(y - x);\ \ Z = \sigma\left((r + \sigma)x - (\sigma + 1)y - xz\right).$$

В результате получим новую систему

$$\dot{X}(t) = Y; \quad \dot{Y}(t) = Z; \quad \dot{Z}(t) = f(X, Y, Z, \mu^0), \tag{8}$$

где $$f\left(X, Y, Z, \boldsymbol{\mu}^{\mathbf{0}}\right) = b\sigma X r_1 - b(\sigma + 1)Y - (b + \sigma + 1)Z - X^2 Y - \sigma X^3 + \frac{Y\left((\sigma + 1)Y + Z\right)}{X}; \tag{9}$$

$r_1 = r - 1.$

Итак, рассмотрим новый управляющий параметр генератора Лоренца:

$$r^*(t) = r + \mu(t). \tag{10}$$

Для этого будем полагать, что в канал связи передается сигнал $Z(t)$, сгенерированный системой (8-10). Примем следующие допущения: модулирующий сигнал $\mu(t)$ является кусочно-постоянным, то есть осуществляется передача цифровой информации; параметры σ, b – известны, а параметр $r(t) > 0$ является модулируемым параметром. Как известно [5, 6], в зависимости от значения параметра r (при постоянстве σ, b), например, при $24{,}74 < r < 30{,}1$, в системе Лоренца (7) наблюдается хаотический режим функционирования, то есть осуществляется генерация хаотических колебаний.

Покажем процедуру построения наблюдателя за параметром $r_1 = r - 1$ на принимающей стороне для системы (8). Для этого, согласно [8, 9] неизвестный параметр необходимо заменить его динамической моделью, отражающей эволюцию этого параметра. В нашем случае это может быть модель вида $\dot{w}(t) = 0$, поскольку решением этого дифференциального уравнения является $w(t) \approx \text{const}$, что и отражает скачкообразное изменение во времени параметра $r_1(t)$. На этом основании сформируем следующую расширенную систему:

$$\dot{X}(t) = Y; \ \ \dot{Y}(t) = Z; \ \ \dot{Z}(t) = b\sigma X w + G_1; \ \ \dot{w}(t) = 0, \tag{11}$$

где $$G_1 = -b(\sigma + 1)Y - (b + \sigma + 1)Z - X^2 Y - \sigma X^3 + \frac{Y\left((\sigma + 1)Y + Z\right)}{X};$$

w – переменная состояния динамической модели параметра r_1.

Как видно, в системе (11), в отличие от (8), параметр r_1 заменен переменной состояния модели w. В системе (11) наблюдаемыми (известными) являются переменные X, Y, Z, а ненаблюдаемой (неизвестной) переменной – w. Пусть $\hat{w}$ – искомая оценка параметра r_1, то есть $\hat{w} = \hat{r}_1$. Для построения оценки этого параметра введем макропеременную

$$\psi = w - \hat{w} \tag{12}$$

и запишем уравнение редукции

$$\hat{w} = Q(X, Y, Z) + v_1, \tag{13}$$

где $Q(X, Y, Z)$ – неизвестная функция от наблюдаемых переменных состояния системы (11);

v_1 – переменная состояния динамического наблюдателя.

Согласно [8, 9], макропеременная (12) должна удовлетворять функциональному уравнению:

$$\dot{\psi}(t) + L(X,Y,Z)\psi = 0, \tag{14}$$

где $L(X,Y,Z)$ – неизвестная функция, обеспечивающая устойчивость уравнения (14).

Производная по времени макропеременной (12) имеет вид

$$\frac{d\psi}{dt} = \frac{dw}{dt} - \frac{d\hat{w}}{dt}.$$

Тогда, подставив в это уравнение соответствующие выражения (11)-(13), получим

$$\begin{aligned} &-\frac{\partial Q(X,Y,Z)}{\partial X}Y - \frac{\partial Q(X,Y,Z)}{\partial Y}Z - \frac{\partial Q(X,Y,Z)}{\partial Z}(b\sigma Xw + G_1) - \\ &-\frac{dv_1}{dt} + L(X,Y,Z)(w - \hat{w}) = 0. \end{aligned} \tag{15}$$

Поскольку уравнение наблюдателя не должно содержать в себе ненаблюдаемые переменные состояния, то необходимо выписать из уравнения (15) все слагаемые, содержащие ненаблюдаемую переменную w:

$$w\left(-\frac{\partial Q(X,Y,Z)}{\partial Z}b\sigma X + L(X,Y,Z)\right) = 0.$$

Это равенство выполняется при условии

$$-\frac{\partial Q(X,Y,Z)}{\partial Z}b\sigma X + L(X,Y,Z) = 0, \tag{16}$$

так как $w \neq 0$. Преобразовав и проинтегрировав (16), получим

$$Q(X,Y,Z) = \frac{L(X,Y,Z)}{b\sigma X}Z. \tag{17}$$

С учётом полученного соотношения примем

$$L(X,Y,Z) = \alpha X^2, \tag{18}$$

где $\alpha > 0$ – постоянный коэффициент, задающий динамику (скорость) оценивания неизвестного параметра r_1.

Тогда из (17) и (18) имеем

$$Q(X,Y,Z) = \frac{\alpha}{b\sigma}XZ. \tag{19}$$

Теперь, зная $Q(X,Y,Z)$ (19) и $L(X,Y,Z)$ (18), мы можем из (15) выписать уравнение динамической составляющей наблюдателя возмущения:

$$\begin{aligned} \frac{dv_1}{dt} &= -\frac{\partial Q(X,Y,Z)}{\partial X}Y - \frac{\partial Q(X,Y,Z)}{\partial Z}G_1 - L(X,Y,Z)\hat{w} = \\ &= -\left(\frac{\alpha}{b\sigma}Z\right)Y - \left(\frac{\alpha}{b\sigma}X\right)G_1 - \alpha X^2\left(\frac{\alpha}{b\sigma}XZ + v_1\right), \end{aligned} \tag{20}.$$

Кроме того, имеем выражение для оценки параметра r_1:

$$\hat{w} = \hat{r}_1 = \frac{\alpha}{b\sigma}XZ + v_1. \tag{21}$$

Окончательно из (9) и (20) получаем:

$$\hat{r} = 1 + \hat{r}_1 = 1 + \frac{\alpha}{b\sigma} XZ + v_1 . \qquad (22)$$

Таким образом, синтезированный синергетический наблюдатель параметра r_1 состоит из двух составляющих: во-первых, динамической, заданной дифференциальным уравнением (15), и, во-вторых, статической, заданной выражением (17). Теперь из соотношения (10) найдем реконструированный на принимающей стороне информационный сигнал:

$$\mu_{\text{ðåêîíñòð.}}(t) = \hat{r} - r , \qquad (23)$$

который равен разности оцененного параметра и его номинального значения.

Смоделируем полученную систему реконструкции информации на основе ХГ Лоренца с синергетическим наблюдателем параметра. Неизменные параметры системы Лоренца (7): $b = 8/3$, $\sigma = 10$; номинальное значение модулируемого параметра $r = 24$. Информационный сигнал на передатчике $\mu(t)$ показан на рис. 1. На рис. 2 и 3 показаны результаты моделирования системы (8), то есть её поведение на передатчике. Реконструированный, согласно выражению (23), информационный сигнал на приёмнике $\mu_{\text{реконстр.}}(t)$ показан на рис. 4.

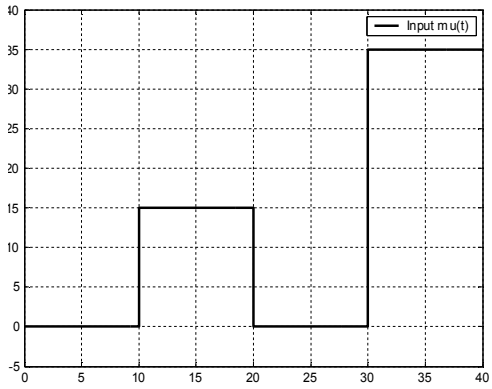

Рис. 1. Информационный сигнал на передатчике

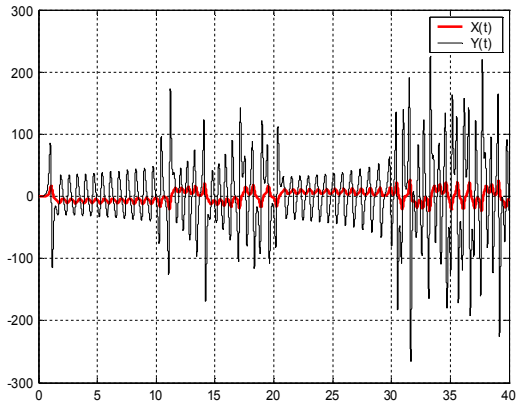

Рис. 2. Графики изменений переменных $X(t), Y(t)$ на передатчике

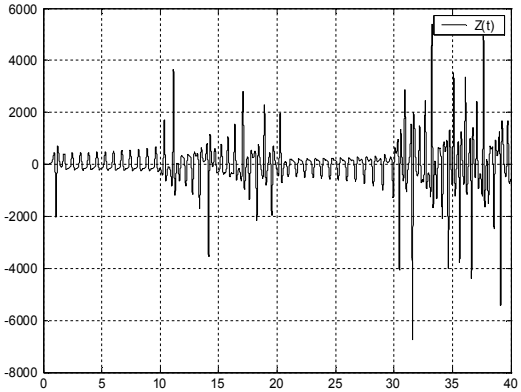

Рис. 3. График изменения передаваемого сигнала $Z(t)$ на выходе передатчика

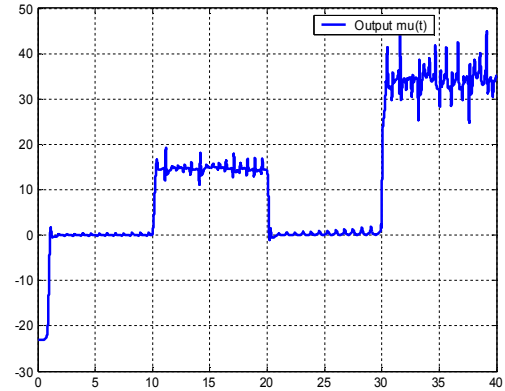

Рис. 4. Реконструированный информационный сигнал на выходе приёмника

Таким образом, предложен новый метод динамической обработки и защиты конфиденциальной информации, основанный на методе глобальной реконструкции динамки системы с использованием синергетического наблюдателя. Как следует из результатов моделирования, синтезированный наблюдатель обеспечивает достаточно точную оценку управляющего параметра $r(t)$ и реконструкцию информационного сигнала.

2. Метод синтеза генераторов "управляющих параметров" в системах с хаотической динамикой

Синтезируем теперь генератор "управляющего параметра" $r(t)$. Для этого, введя дополнительный параметр, расширим модель (7) следующим образом:

$$\begin{aligned} \dot{x}(t) &= y, \\ \dot{y}(t) &= -(1+\sigma)y - \sigma(1-r+z)x, \\ \dot{z}(t) &= -bz + \frac{1}{\sigma}xy + x^2, \\ \dot{r}(t) &= u(x,y,z) = F(t), \end{aligned} \tag{24}$$

где $u(x,y,z) = F(t)$ – генератор желаемых изменений "управляющего параметра" $r(t)$ с целью формирования соответствующих структур – аттракторов в модели Лоренца.

Итак, ставится задача: синтезировать обратную связь $u(x,y,z)$, обеспечивающую при произвольных начальных условиях x_0, y_0, z_0, r_0 формирование в структуре модели Лоренца желаемых аттракторов с соответствующими бифуркациями, например, типа "вилки". Для решения этой задачи введем, согласно методу АКАР [8-10], следующую макропеременную:

$$\psi = z - r + \mu - \alpha\cos x. \tag{25}$$

Подставляя данную макропеременную и её производную в функциональное уравнение

$$T\dot{\psi}(t) + \psi = 0,$$

получим

$$\dot{z}(t) - \dot{r}(t) + \alpha y \sin x + \frac{1}{T}\psi = 0.$$

Подставив в это уравнение соответствующие выражения для $\dot{z}(t)$ и $\dot{r}(t)$ из (24), получим

$$u = -bz + \frac{1}{\sigma}xy + x^2 + \alpha y \sin x + \frac{1}{T}\psi \tag{26}$$

На рис. 5-8 приведены результаты моделирования системы (24), (26) для параметров $\sigma = 10;\ b = 8/3;\ \mu = 0{,}5;\ \alpha = -2;\ T = 0{,}2$ при начальных условиях $r(0) = 28,\ x(0) = 1,\quad \dot{x}(0) = 0{,}2,\ z(0) = 0$. В этом случае, согласно структуре уравнения (27), система (24), (26) на финишном этапе своего движения выходит на аттрактор с бифуркацией типа "вилки", параметры которой зависят от знака начальных условий по координате $\pm x_0$, что наглядно видно из рис. 5. Из рисунков 5–8 следует, что в системе (24) не возникает каких-либо хаотических режи-

мов движения, хотя, как известно, в модели Лоренца (7) с параметрами $\sigma = 10;\ b = 8/3;\ r_0 = 28$ такие режимы всегда существуют, при этом в установившемся режиме параметр $r = 72$.

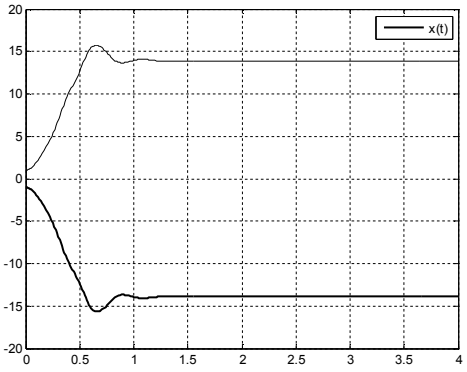

Рис. 5. Графики изменения $x(t)$

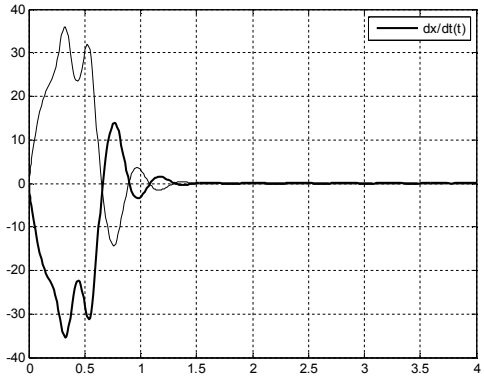

Рис. 6. Графики изменения $\dot{x}(t)$

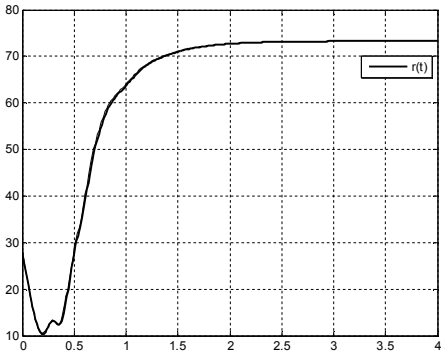

Рис. 7. График изменения $r(t)$

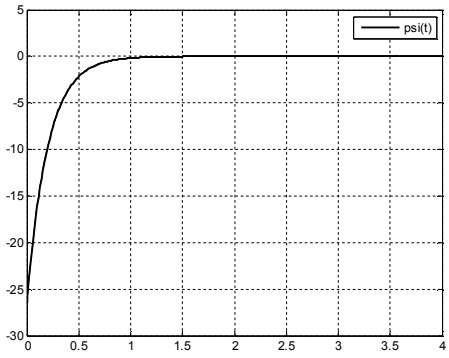

Рис. 8. График изменения $\psi(t)$

При большом значении параметра r получаются результаты моделирования системы (24), (26), приведенные на рис. 9-12. В данном случае были выбраны параметры $\sigma = 10;\ b = 8/3;\ \mu = 0{,}5;\ \alpha = 2;\ T = 0{,}2$ и начальные условия $r(0) = 150,\ x(0) = \pm 0{,}5,\ \dot{x}(0) = 0,\ z(0) = 0{,}5$. В этом случае, система (24), (26) на финишном этапе своего движения также выходит на аттрактор с бифуркацией типа "вилки", параметры которой зависят от знака начальных условий по координате $\pm x_0$, что наглядно видно из рис. 9.

Это показывает, что если синтезировать генератор "управляющего параметра" $r(t)$, например вида (28), то тогда модель Лоренца становится обычной системой дифференциальных уравнений, в которой отсутствует странный аттрактор, фрактальная размерность и хаос. Из чего следует, что таким образом мы можем управлять сложными системами.

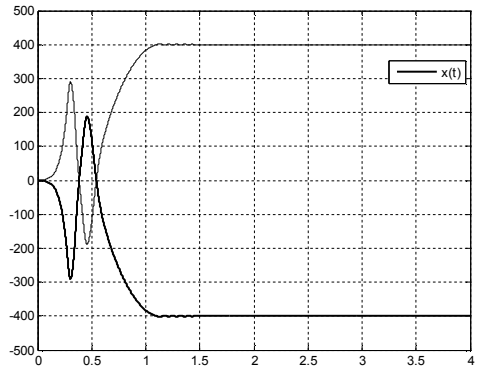

Рис. 9. Графики изменений $x(t)$

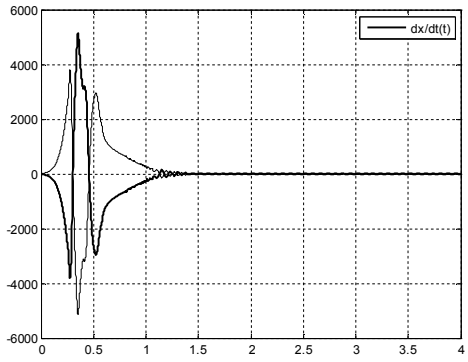

Рис. 10. Графики изменений $\dot{x}(t)$

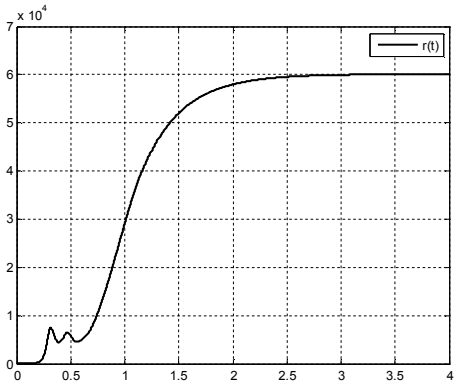

Рис. 11. График изменения $r(t)$

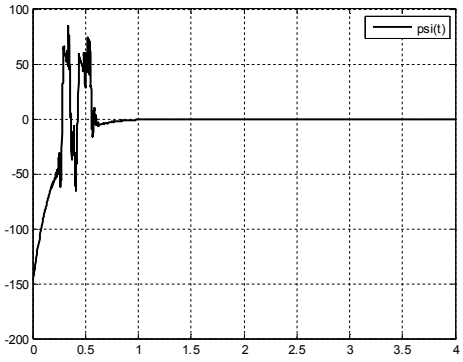

Рис. 12. График изменения $\psi(t)$

Заключение

Предложенный в данной статье новый метод динамической обработки и защиты информации основан на методе глобальной реконструкции динамки системы с использованием синергетического наблюдателя, который обеспечивает достаточно точную оценку управляющего параметра и соответственно реконструкцию информационного сигнала. Это позволяет применять данный метод к задаче скрытой передачи информации по каналам связи, используя в качестве несущего сигнала колебания хаотических генераторов, несмотря на их высокую чувствительность к малым изменениям "управляющих параметров" и начальных условий.

Предложен также метод синергетического синтеза генераторов "управляющих параметров", основанный на применении метода АКАР, который позволяет сформировать в структуре модели Лоренца желаемые аттракторы.

Литература

1. ***Николис Дж.*** Динамика иерархических систем. М.: Мир, 1989.

2. ***Experimental*** demonstration of secure communications via chaotic synchronization / Kocarev L., Halle K.S., Eckert K., Chua L., Parlitz U. // Int. J. Bifurcation and chaos. – 1992. – № 3. Pp. 709-713.

3. ***Бельский Ю.Л., Дмитриев А.С.*** Передача информации с использованием детерминированного хаоса // Радиоэлектроника и электроника. Журнал РАН. – 1993. – № 7. С. 1310-1315.

4. ***Радиосвязь*** с использованием хаотических сигналов / Дмитриев А.С., Кузьмин Л.В., Панас А.И., Стариков С.О. // Препринт ИРЭ РАН. М., 1997. № 1.

5. ***Нелинейные*** эффекты в хаотических и стохастических системах / Анищенко В.С., Астахов В.В., Вадивасова Т.Е., Нейман А.Б. Москва-Ижевск: Институт компьютерных исследований, 2003.

6. ***Анищенко В.С., Вадивасова Т.Е., Астахов В.В.*** Нелинейная динамика хаотических и стахостических систем. Саратов: Изд-во Саратовского университета, 1999.

7. ***Anishchenko V.S., Pavlov A.N., Yanson N.B.*** Reconstruction of dynamic systems as applied to secure communications // Technical Physics, 1998. –Vol. 43(12). Pp. 1401-1407.

8. ***Колесников А.А.*** Синергетические методы управления сложными системами: теория системного синтеза. М.: УРСС/Комкнига, 2006.

9. ***Современная*** прикладная теория управления. Ч. II: Синергетический подход в теории управления / Колесников А.А. и др. Москва-Таганрог: Изд-во ТРТУ, 2000.

10. ***Колесников А.А.*** Синергетическая теория управления. М.: Энергоатомиздат, 1994.