

Фазовые диаграммы для открытого текста существенно отличаются от диаграмм, построенных для выходных последовательностей шифров DES (des_ofb, des_cbc), СТБ (стб_ofb, стб_cbc) и алгоритмов на основе динамического хаоса по структурам OFB и CBC для пар собственных векторов с номерами: 1000 и 999, 1000 и 998 (см. рис. 2).

Для фазовых диаграмм шифров DES (des_ofb, des_cbc) (рис. 2 в, з, д, е), а также СТБ (рис. 2 ж, з, и, к) характерным, в отличие от диаграмм открытого текста (рис. 2 а, б), является наличие «зашумленности» фигур.

Фазовым диаграммам выходных последовательностей алгоритмов на основе динамического хаоса по структуре OFB присуща четкость линий, правильность фигур, повторяемость визуальной информации для 4-й и 128-й итераций, 8-й и 256-й итераций (например, рис. 2 л, м и н, р). Отмечается структурированность в построенных диаграммах, что свидетельствует о наличии детерминированности в исследуемых последовательностях. Фазовые диаграммы, построенные по выходным последовательностям алгоритмов шифрования на основе динамического хаоса по структуре CBC, отличаются «зашумленностью» фигур для диаграмм с числом итераций от 1-й до 1024-й (например, рис. 2 с–ц).

Таким образом, использование метода сингулярного спектрального анализа применительно к открытому тексту, а также к выходным последовательностям алгоритма шифрования на основе динамического хаоса по структурам OFB и CBC позволяет установить качественные критерии в виде фазовых диаграмм, а также количественные критерии по уровню главных компонент, дисперсии отклонений собственных значений матрицы главных компонент от среднего и медианы абсолютного отклонения.

В результате проведенных исследований установлено:

1) при анализе выходных последовательностей алгоритмов шифрования на основе динамического хаоса метод сингулярного спектрального анализа позволяет установить качественные (фазовые диаграммы) и количественные (уровень главных компонент, дисперсия отклонений собственных значений матрицы от среднего значения и медианы абсолютного отклонения) показатели как критерии возможности их использования для шифрования;

2) сравнительный анализ приведенных показателей выходных последовательностей алгоритмов на основе динамического хаоса по структуре OFB и CBC, шифров DES, СТБ показал, что алгоритм хаоса по структуре CBC позволяет получить методом сингулярного спектрального анализа для зашифрованной информации параметры, сопоставимые с шифром DES и Белорусского стандарта шифрования СТБ 34.101.31-2011.

1. Li S. When chaos meets computers // <http://arxiv.org/abs/nlin/0405038v3>.
2. Dachsel F., Schwarz W. // IEEE Trans Circuits Syst. I. 2001. Vol. 48. № 12. P. 1498.
3. Андреев В. В., Сапожникова Ю. В., Фомичев А. И. // Прикл. информатика. 2009. № 6. С. 80.
4. Сидоренко А. В., Мулярчик К. С. // Информатика. 2011. № 1. С. 95.
5. Alvarez G., Montoya F., Romera M., Pastor G. // Phys. Let. A. 2003. Vol. 319. P. 334.
6. Алферов А. П., Зубов А. Ю., Кузьмин А. С., Черемушкин А. В. Основы криптографии. М., 2005.
7. Главные компоненты временных рядов: метод «Гусеница» / Под ред. Д. Л. Данилова и А. А. Жиглявского. СПб., 1997.

Поступила в редакцию 20.01.12.

Алевтина Васильевна Сидоренко – доктор технических наук, профессор кафедры физики и аэрокосмических технологий.

Иван Владимирович Шакинко – студент 5-го курса факультета радиофизики и компьютерных технологий.

Константин Сергеевич Мулярчик – аспирант факультета радиофизики и компьютерных технологий. Научный руководитель – А. В. Сидоренко.

УДК 621.391.7

С. И. ПОЛОВЕНЯ, В. В. ДУБРОВСКИЙ

ОБЕСПЕЧЕНИЕ СКРЫТНОСТИ ИНФОРМАЦИИ ХАОТИЧЕСКИМИ СИГНАЛАМИ НА ОСНОВЕ ОТОБРАЖЕНИЙ, РАСПРЕДЕЛЕННЫХ ВО ВРЕМЕНИ

We propose method to ensure secrecy of information using chaotic signals based on maps distributed in time. This method can improve the structural stealth signals while maintaining dynamic range and noise immunity to get higher than that of the known communication systems based on dynamic chaos.

К нелинейным формирующим функциям (НФФ) генераторов хаотических процессов (ХП) предъявляются два противоречивых требования: 1) в области определения НФФ должна быть нелинейной

с максимально большим количеством интервалов аргумента различной монотонности; 2) малые изменения аргумента НФФ не должны вызывать значительных приращений функции.

Увеличивающиеся требования к защищенности информации от перехвата при ее передаче по открытым каналам технически удовлетворяются двумя способами: путем усовершенствования алгоритмов криптографической защиты информации; с помощью создания и адаптации новых сигнально-кодowych конструкций и методов информационной модуляции. Второе направление связано с системами, в которых имеется существенно нелинейная обратная связь.

В работе [1] предложен один из возможных подходов к построению эффективных генераторов ХП. В настоящей работе предлагается формировать распределенные во времени НФФ в виде отрезков наклонных прямых с малыми углами наклона. Хаотический сигнал (ХС), сформированный на основе распределенных во времени отображений, дает возможность синтезировать более устойчивый к воздействию помех алгоритм обработки. При этом передаваемое по каналу связи сообщение по своим статистическим и спектрально-временным характеристикам схоже с шумом.

Алгоритм генерации

Элементарным фрагментом НФФ является отрезок прямой, описываемой уравнением $f(x) = ax + b$, где a и b – параметры базовой функции.

Полагаем, что ХП формируется в пределах динамического диапазона (ДД) $[-1; 1]$, следовательно, необходимо наложить ограничения на функцию $f(x)$, чтобы ее область допустимых значений (ОДЗ) также не превышала отрезка $[-1; 1]$. Обозначим указанные ограничения как некоторое дополнительное функциональное преобразование $F(\cdot)$. Для удобства практической реализации функции $F(\cdot)$ можно предложить два варианта: 1) ограничение функции $f(x)$ по уровням ± 1 (рис. 1 а); 2) «излом» функции у границ ДД (рис. 1 б).

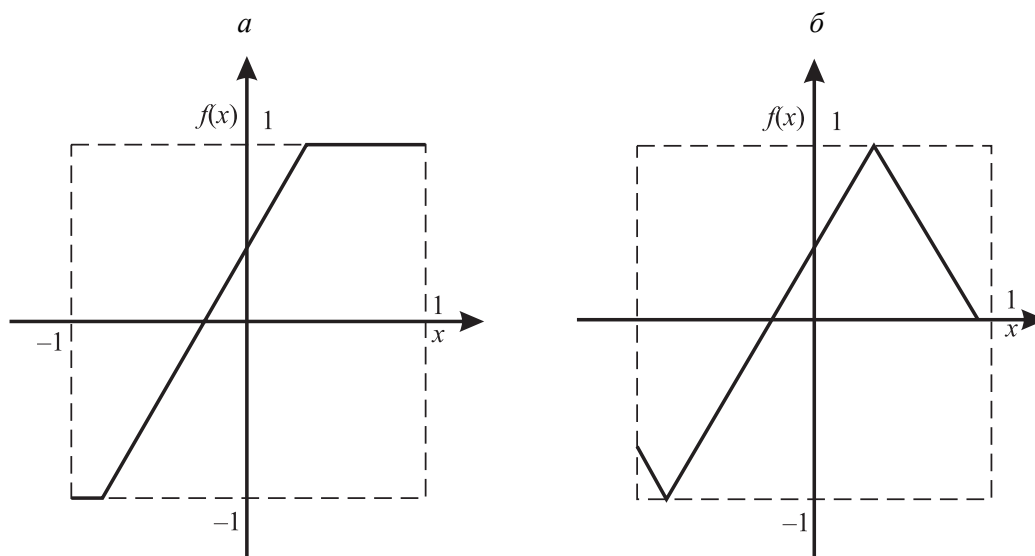


Рис. 1. Варианты ограничения ДД

ХП генерируется согласно выражению

$$\begin{cases} h_{k+1} = F[a_k h_k + b_k]; \\ a_{k+1} = \alpha f_a\left(\frac{1}{\alpha} a_k\right); \\ b_{k+1} = f_b(b_k). \end{cases} \quad (1)$$

Здесь a_k и b_k – значения параметров функции $f(x)$ на k -м такте формирования ХС; $\alpha \in [0; \infty)$ – предельный параметр наклона НФФ $f(x)$; f_a и f_b – НФФ, определяющие случайно подобные изменения параметров a_k и b_k . ОДЗ функций $f_a(\cdot)$ и $f_b(\cdot)$ при аргументах, принадлежащих $[-1; 1]$, не должна выходить за пределы отрезка $[-1; 1]$.

Функциональная схема устройства, реализующего алгоритм, приведена на рис. 2.

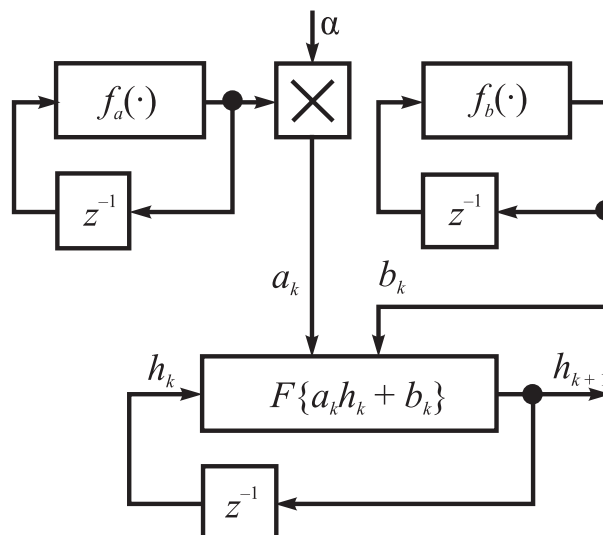


Рис. 2. Генератор ХП

На рис. 3 представлено отображение ХП, сформированного согласно алгоритму [1] для случая, когда функции $f_a(\cdot)$ и $f_b(\cdot)$ являются гармоническими.

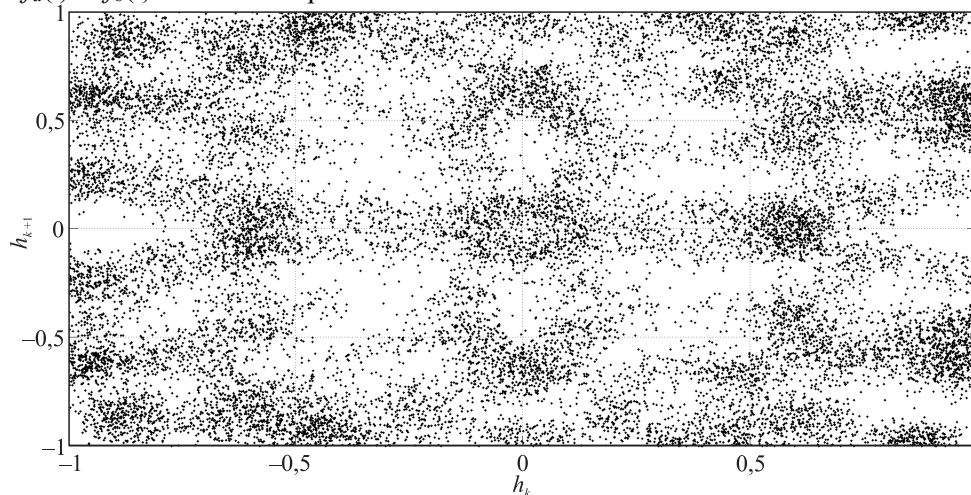


Рис. 3. Отображение хаотического процесса, сформированного согласно (1)

Информационная модуляция

Возможны два базовых метода модуляции хаотического процесса информационным сигналом: 1) метод манипуляции хаотических режимов; 2) метод нелинейного подмешивания (МНП).

Рассмотрим метод нелинейного подмешивания, алгоритм которого определяется соотношениями

$$\begin{cases} h_{k+1} = (1 - \gamma)F[a_k h_k + b_k] + \gamma; \\ a_{k+1} = \alpha f_a\left(\frac{1}{\alpha} a_k\right); \\ b_{k+1} = f_b(b_k). \end{cases} \quad (2)$$

Здесь a_k и b_k – значения параметров функции $f(x)$ на k -м такте формирования ХС; $\gamma \in [0; 1]$ – параметр, определяющий степень подмешивания полезного сообщения λ_k в ХС; $\alpha \in [0; \infty)$ – предельный параметр наклона нелинейной формирующей функции $f(x)$; $f_a(\cdot)$ и $f_b(\cdot)$ – нелинейные функции, определяющие характер изменения параметров НФФ.

Алгоритм (2) получает развитие, если вместо кусочно-линейных в качестве нелинейных формирующих функций использовать некоторые поверхности в трехмерном пространстве.

Алгоритм формирования ХП можно записать так:

$$\begin{cases} h'_k = c(1 - h_{k-1} / a - h_{k-2} / b); \\ h_k = 2\text{sign}(h''_k) - h''_k, \text{ если } |h''_k| > 1; \text{ иначе } h_k = h''_k; \\ h_k = (1 - \alpha)h'_k + \alpha\lambda_k. \end{cases}$$

Структура формирователя хаос-сигнала представляет собой систему связанных кольцевых подсистем, в каждой из которых введена нелинейная обратная связь (рис. 4). Основной подсистемой, формирующей сигнал, является вычислитель функции $F(\cdot)$ вместе с двумя регистрами задержки z^{-1} . Функция $F(\cdot)$ реализует отображение в виде некоторой плоскости в трехмерном пространстве фазовых состояний. Нормаль к плоскости, проведенная из начала координат, близка к вертикальной. Это обеспечивает нечувствительность НФФ к возмущениям. НФФ, кроме двух аргументов, имеет три параметра: a , b и c , обуславливающие характер изменения фазовых состояний хаос-процесса. Каждый из параметров определяется собственным хаос-генератором, тактируемым генератором тактовых импульсов (ГТИ).

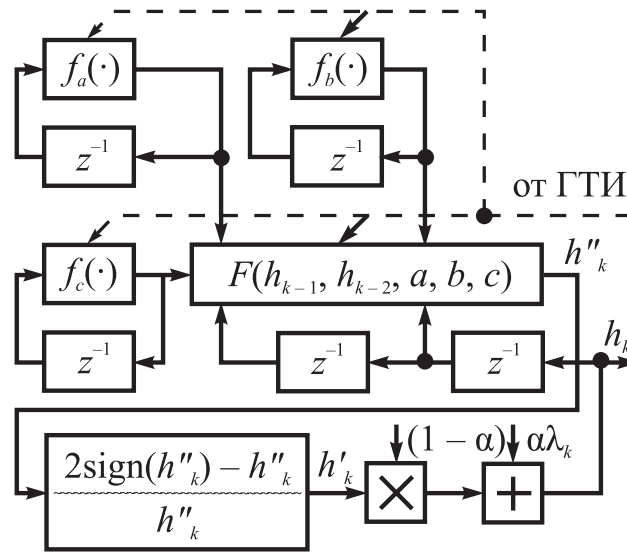


Рис. 4. Структура формирователя хаос-сигнала

По причине того, что достаточно сложно обеспечить ограниченность динамического диапазона хаос-процесса значениями ± 1 , в алгоритме предлагается использовать метод ограничения значений в виде «зеркального преобразования», описанного в [1], а на рис. 4 реализуемого блоком $2\text{sign}(h''_k) - h''_k$. Запись h''_k (см. рис. 4) означает, что если ХП не выходит за границы ДД, то на выход передается входное значение. Перемножитель и сумматор на схеме осуществляют нелинейное подмешивание информационного процесса λ_k к ХП h'_k . Последовательность отсчетов ХП h'_k подается на радиочастотный модулятор.

Алгоритм обработки сигнала

Алгоритм обработки ХС определяется выражением, которое следует из (1):

$$\begin{cases} \lambda_k = \frac{1}{\gamma} \{ h_{k+1} - (1 - \gamma) F[a_k h_k + b_k] \}; \\ a_{k+1} = \alpha f_a \left(\frac{1}{\alpha} a_k \right); \\ b_{k+1} = f_b(b_k). \end{cases}$$

МНП в нелинейных динамических системах является универсальным подходом с точки зрения возможности передачи как отсчетов аналогового сигнала, так и цифрового потока данных. В последнем случае структурную схему декодера ХС (рис. 5) необходимо дополнить решающим устройством (РУ).

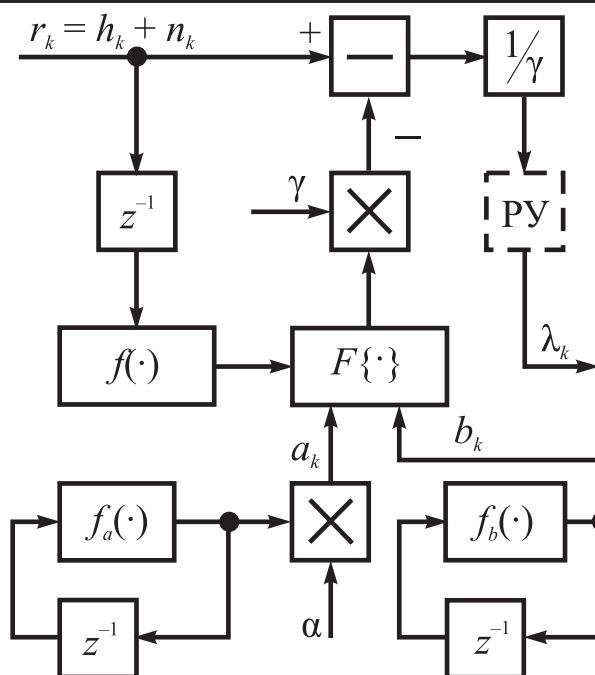


Рис. 5. Структурно-функциональная схема обработки и декодирования сигнала

На рис. 6 приведено семейство кривых помехоустойчивости для случая, когда параметры a_k и b_k определяются нелинейной функцией $\sin(\cdot)$, а $F\{\cdot\}$ – в виде «изломов» линейных функций. Кривые строились для различных уровней подмешивания бинарного потока к ХС.

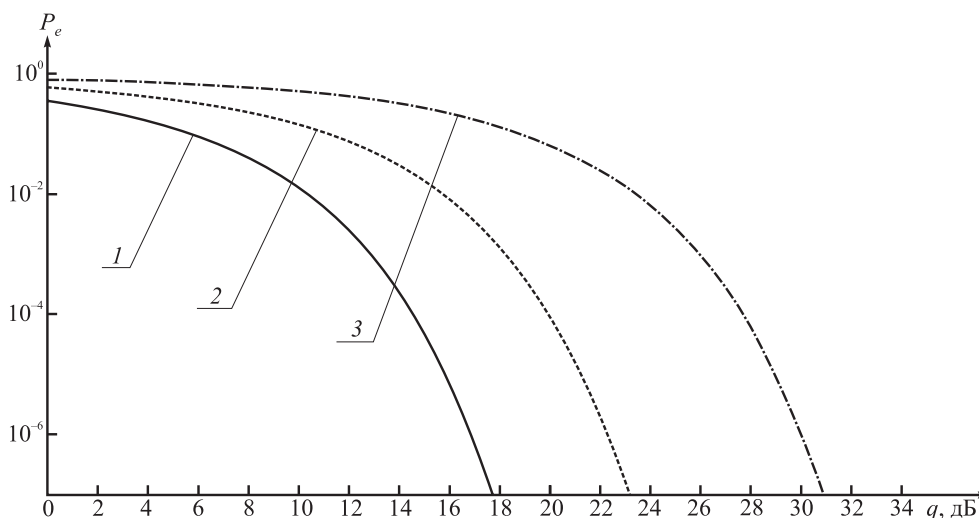


Рис. 6. Семейство кривых помехоустойчивости обработки ХС при различных уровнях подмешивания:
1 – для уровня 0,7; 2 – для уровня 0,4; 3 – для уровня 0,1

При кодировании информации в трехмерном пространстве состояний плоскость определяется следующим выражением: $Ax + By + Cz + D = 0$, где A, B, C задает проекции нормали к плоскости на оси координат; D – некоторый произвольный коэффициент. Для нечувствительности НФФ к возмущениям необходимо, чтобы $A \equiv 0, B \equiv 0$. Параметры D и C можно найти из второй формы уравнения для плоскости: $x/a + y/b + z/c = 1$. Плоскость пересекает оси координат в точках $(a; 0; 0)$, $(0; b; 0)$ и $(0; 0; c)$, где $c = -D/C$. Таким образом, параметры D и C могут быть произвольными, но значения $|C|$ и $|D|$ должны быть соразмерными. Такое требование следует из необходимости пересечения плоскостью оси Oz в точке, находящейся внутри или в непосредственной близости от интервала $(-1; 1)$.

Для случая нелинейного подмешивания алгоритм декодирования хаос-сигнала описывается следующим выражением:

$$\begin{cases} \lambda_k = [h_k - (1-\alpha)h'_k] / \alpha; \\ h''_k = c(1 - h_k / a - h_{k-1} / b); \\ h'_k = 2\text{sign}(h''_k) - h''_k, \text{ если } |h''_k| > 1; \text{ иначе } h'_k = h''_k. \end{cases}$$

На рис. 7 представлена схема, реализующая алгоритм (ХГ – хаотический генератор).

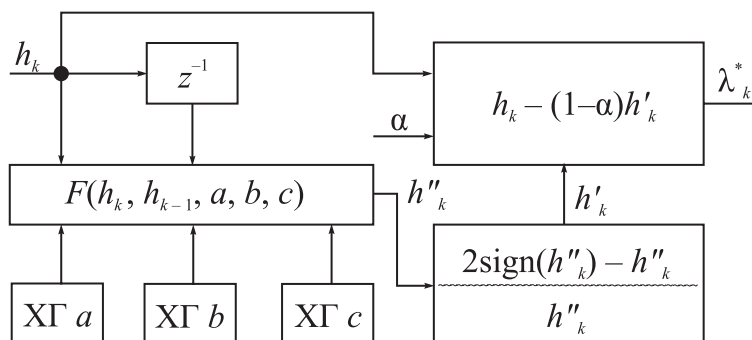


Рис. 7. Структурная схема обработки хаос-сигнала

Структурная схема обработки хаос-сигнала представляет собой нелинейный фильтр, реализуемый функцией $F(\cdot)$, аргументами которой являются два последовательных входных отсчета, а три параметра определяют характер изменения отображения, известный на приемной стороне.

Особенность предлагаемых алгоритмов генерации ХП заключается в том, что в нем не существует строго определенной НФФ. В рассматриваемом случае один или несколько параметров НФФ изменяются хаотическим образом на каждом такте генерации.

В работе [1] обоснована целесообразность «расщепления» НФФ во времени. При этом сохраняются все положительные свойства ХС и существенно повышается помехоустойчивость.

Численное моделирование показало необходимость тщательного выбора параметра γ и в особенности предельного углового коэффициента a элементарной НФФ. При сравнительно больших $\alpha > 0,5$ фазовые траектории хаотического колебания становятся сложными, но снижается помехоустойчивость. При малых значениях $\alpha \approx 0,02 \dots 0,1$ помехоустойчивость обработки высокая, но колебания могут иметь квазирегулярную структуру.

В реальных системах параметр c на каждом такте работы схемы на рис. 4 должен приобретать значительное приращение, составляющее не менее 0,5. При удовлетворении требования обеспечивается высокая степень стохастизации колебаний, а также эффективная информационная модуляция. При небольшой разрядности целочисленных регистров, предназначенных для хранения значений хаотического процесса, а также значений параметров НФФ, обеспечивается хорошее перемешивание траекторий модулированного колебания, а значит, высокая степень сокрытия информации. При формировании и обработке сигнала необходимо осуществление сравнительно простых операций с целыми числами: сложение (вычитание), умножение, задержка (перенос в регистр). Следовательно, даже при высоких скоростях передачи информации не требуется дорогостоящая программно-аппаратная часть, реализующая алгоритм.

Главная цель, достигаемая при реализации алгоритмов, – это относительно малое приращение формирующей функции при внесении значительного возмущения ее аргумента с сохранением высокой степени стохастизации колебательного процесса. Параметр α при этом должен быть близким к нулю. Таким образом, решаются две задачи: 1) достигается высокая структурная скрытность сигнала, фактически определяемая функциями $f_a(\cdot)$ и $f_b(\cdot)$; 2) обеспечивается робастность алгоритма обработки сигналов в канале с помехами.

1. Чердынцев В. А., Половения С. И., Дубровский В. В. // Докл. БГУИР. 2010. № 4(50). С. 11.
2. Дубровский В. В., Чердынцев В. А. // Докл. БГУИР. 2007. № 1(17). С. 34.

Поступила в редакцию 24.08.12.

Сергей Иванович Половения – ассистент кафедры радиотехнических устройств БГУИР.

Василий Викторович Дубровский – кандидат физико-математических наук, доцент кафедры радиотехнических устройств БГУИР.