УДК 621.391 DOI: 10.15222/TKEA2014.2-3.28

К. ф.-м. н. Р. Л. ПОЛИТАНСКИЙ, к. т. н. П. М. ШПАТАРЬ, А. В. ГРЕСЬ, к. т. н. А. Д. ВЕРИГА

Украина, Черновицкий национальный университет имени Юрия Федьковича
E-mail: alexgs85@ukr.net

СИСТЕМА ПЕРЕДАЧИ ДАННЫХ С ШИФРОВАНИЕМ ХАОТИЧЕСКИМИ ПОСЛЕДОВАТЕЛЬНОСТЯМИ

Предложена система передачи данных, зашифрованных последовательностями, которые сформированы на основе одномерных дискретных хаотических отображений. Рассмотрен принцип работы системы на примере передачи данных между двумя компьютерами.

Ключевые слова: динамическая система, хаотическая последовательность, начальные условия, логистическое отображение.

Перспективным направлением развития информационных и телекоммуникационных систем является использование широкополосных систем связи, базирующихся на явлении синхронизации генераторов хаоса. В системах данного класса могут использоваться сигналы, сформированные с использованием псевдослучайных последовательностей. Сигналы, генерируемые нелинейными динамическими системами, являются новым классом сигналов, возможность использования которых в системах связи определяется их свойствами [1, 2]. Одной из основных проблем, возникающих при построении таких систем, является обеспечение синхронизации между принимающей и передающей сторонами систем связи. Большинство способов скрытой передачи информации с синхронизацией хаосом основано на режиме полной хаотической синхронизации, что влечет за собой требование к высокой степени идентичности генераторов, располагающихся на передающей и приемной сторонах системы передачи информации. Совершенствование методов скрытой передачи данных на основе систем с хаотической синхронизацией стало в последнее время одной из важных задач в области создания информационно-телекоммуникационных систем на основе хаоса [3].

Цель настоящей работы заключается в экспериментальной реализации системы передачи данных, зашифрованных псевдослучайными последовательностями, которые генерируются на основе одномерных дискретных хаотических отображений с обеспечением синхронизации передающей и принимающей сторон системы.

Современные телекоммуникационные системы требуют обеспечения высокой скрытности и конфиденциальности связи. Защита передаваемой информации от несанкционированного доступа в телекоммуникационных системах возможна путем ее шифрования, заключающегося в наложении гаммирующей последовательности на открытый текст. В качестве таких последовательностей могут быть использованы псевдохаотические последовательности, алгоритмы генерирования которых реализуются на основании динамического хаоса, чувствительного к изменению начальных условий. Для генерирования цифровых хаотических последовательностей используется определенная функция, значения которой при определенных начальных условиях равномерно распределены на ограниченном отрезке. Этим свойством обладают решения логистического уравнения [4, 5]

$$x_{n+1} = \lambda x_n(1-x_n), \qquad (1)$$

где λ, x_n — начальные условия для генерирования последовательностей. Генерирование хаотической последовательности в соответствии с этим уравнением имеет место при $\lambda = 3{,}65 - 3{,}95$.

Структурные схемы предложенной системы передачи информации, а также схемы кодера и декодера системы приведены на **рис. 1** и **2** соответственно.

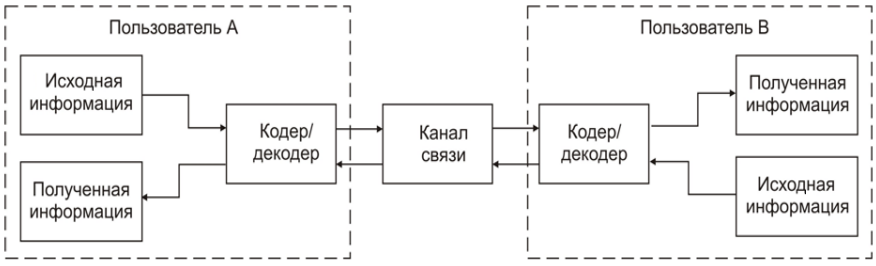


Рис. 1. Структурная схема системы передачи текстовой информации, шифрованой хаотическими последовательностями

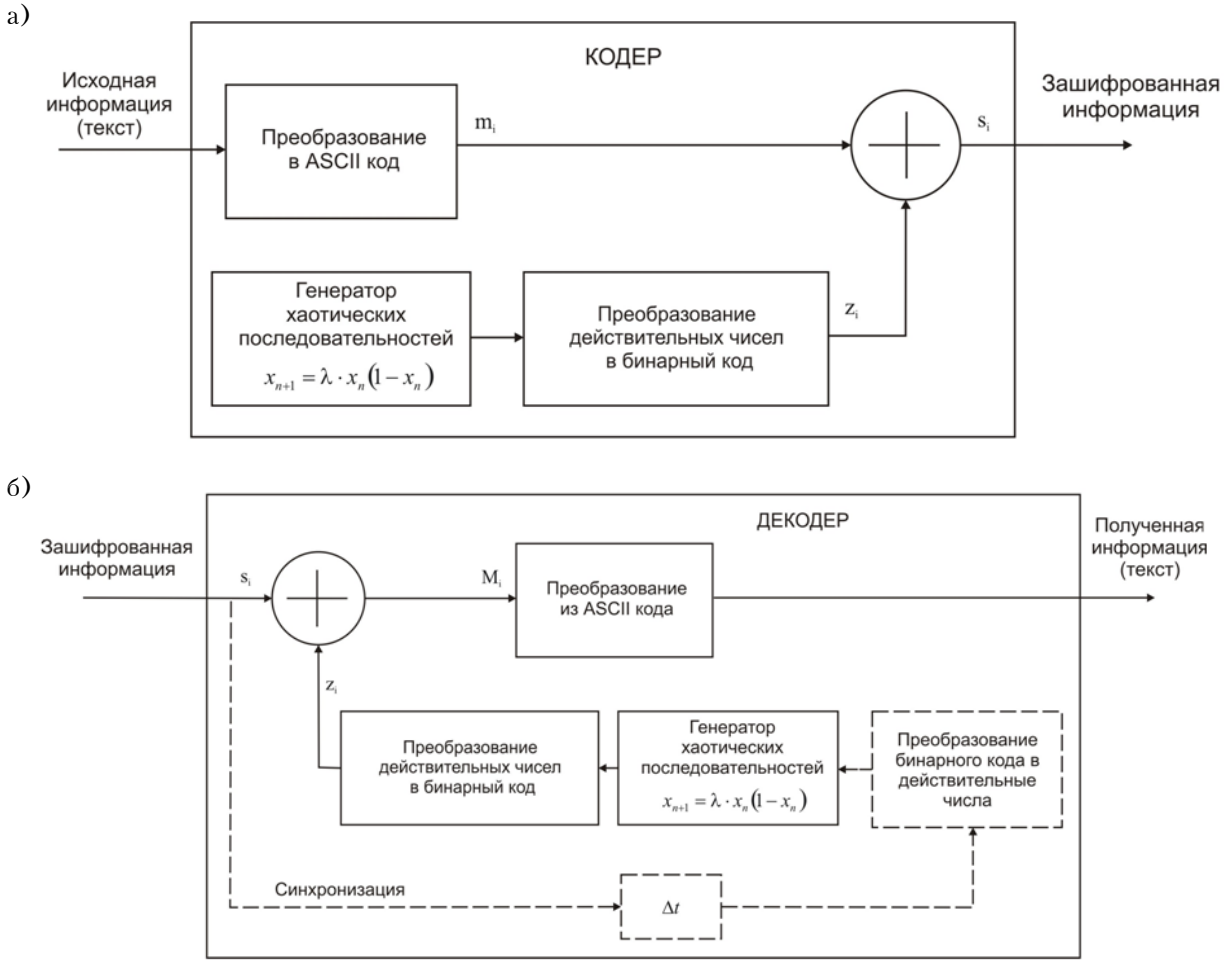


Рис. 2. Структурные схемы кодера (*а*) и декодера (*б*) системы передачи информации

Исходные данные (текст) из источника информации, поступая на вход кодера системы, преобразуются в 8-битовые символы в соответствии с таблицей кода ASCII. Для генерирования псевдослучайных последовательностей используется одномерное дискретное хаотическое отображение (логистическое отображение)

$$x_{n+1}=3{,}85x_n(1-x_n). \quad (2)$$

Генерируемая последовательность чисел преобразуется в двоичные 8-битовые символы в соответствии с формулой [5]

$$z_n = 2^{-1}\, b_{n1} + 2^{-2}\, b_{n2} + \ldots + 2^{-L}\, b_{nL}, \quad (3)$$

где L — разрядность двоичного представления.

Представленное символами информационное сообщение m_i суммируется по модулю 2 с элементами псевдослучайной последовательности

$$s_i = m_i \oplus z_i. \quad (4)$$

Дешифрование информации осуществляется путем суммирования по модулю 2 полученного сообщения с псевдослучайной последовательностью, генерируемой на приемной стороне с использованием того же логистического уравнения при тех же начальных условиях [6—8].

Ключом шифрования системы является значение параметра логистического отображения λ и начальное значение x_n. Криптостойкость системы обуславливается количеством ключей шифрования. Количество ключей шифрования для двухпараметрической системы равно

$$N = (10^n)^2, \quad (5)$$

где n — точность введения параметров (количество знаков после запятой).

В нашем случае точность введения n для начальных условий λ и x_n задана программно и составляет 10. Соответственно, пространство ключей будет составлять 10^{20}, что является достаточно хорошим результатом для двухпараметрической системы. В таких системах возможность передачи информации с минимальным количеством ошибок в принятом тексте обеспечивается путем использования одного из способов синхронизации (полной, обобщенной, фазовой и др.). Авторами [9—11] синхронизация осуществлялась синхроимпульсами, не изменяющимися по форме

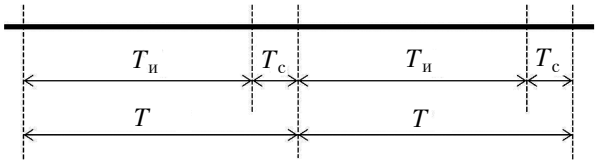


Рис. 3. Временная диаграмма передачи синхроимпульса и информационного сообщения

и длительности, при этом имела место периодическая передача синхроимпульса через интервал времени, состоящий из длительности информационной ($T_и$) и синхронизирующей ($T_с$) последовательностей.

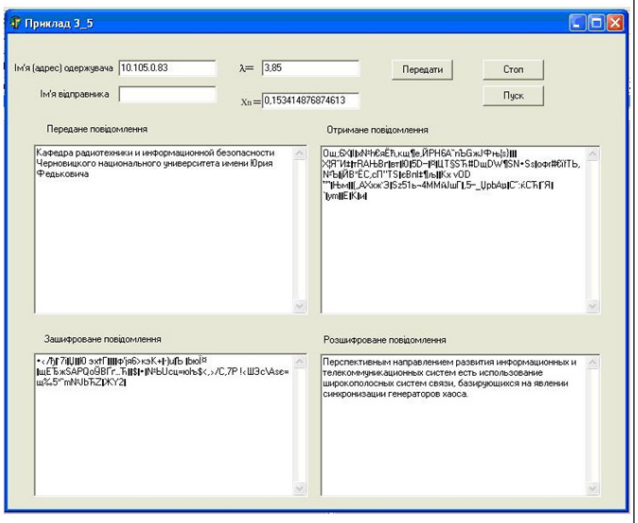
Временная диаграмма процесса передачи синхроимпульса и информационного сообщения приведена на **рис. 3** [9–11]. В данной системе предложено осуществление синхронизации путем передачи через определенные интервалы времени текущего значения x_n, генерируемого логистическим отображением. Период передачи x_n зависит от быстродействия компьютера и расстояния между абонентами системы, а его значение определяется путем передачи тестового сообщения перед началом сеанса связи. Безошибочный прием тестового сообщения свидетельствует об оптимальном подборе периода передачи текущего значения x_n. Подбор периода осуществляется на программном уровне. Максимальное значение периода передачи x_n исследуемой нами системы на компьютерах марки Intel P-IV 2,4 ГГц, находящихся на расстоянии 100 м, составило 27,8 мкс. При значениях периода меньше 27,8 мкс имеет место стабильная синхронизация. Предложенный метод синхронизации передающей и принимающей сторон обеспечивает безошибочную передачу и прием текста, состоящего из 10000 символов украинского, русского и английского алфавита.

Результаты работы

Для построения системы связи использовались современные программные средства, в частности язык Delphi 7.0 Система работает в реальном времени в полнодуплексном режиме при любой аппаратной реализации доступа к сети Интернет. Пользователям системы связи достаточно указать только IP-адреса. Результаты работы программы приведены на **рис. 4**.

На рис. 4, *а* изображено окно программы пользователя *A*, который передает пользователю *B* сообщение «Кафедра радиотехники и информационной безопасности Черновицкого национального университета имени Юрия Федьковича». В поле имени получателя введен IP-адрес пользователя *B* (10.105.0.83). При этом значение параметра ключа шифрования λ для передающей и принимающей сторон равнялось 3,85. Начальное значение x_n вводится только организатором шифрованного обмена сообщениями (например, пользователем *A*), а в дальнейшем в окне программы выводится текущее значение x_n. Аналогично пользователь *B* может передавать зашифрованные сообщения пользователю *A* (рис. 4, *б*).

а)



б)

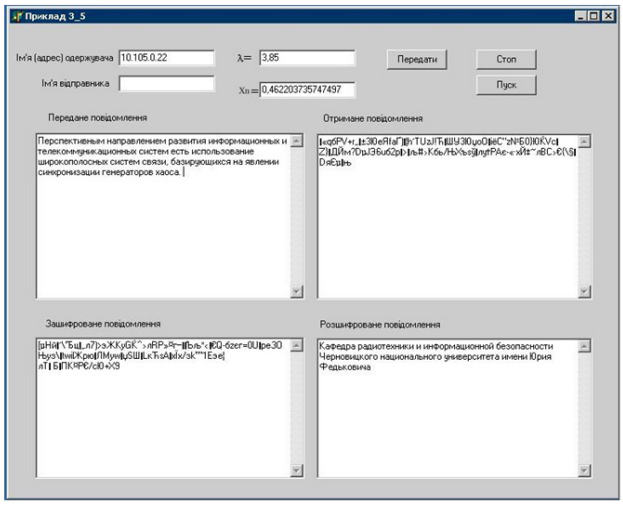


Рис. 4. Пример обмена сообщениями между пользователями *A* (*а*) и *B* (*б*) системы

Работа программы тестировалась на передаче текстов различной длины. При передаче текстовых сообщений длиной до 10000 символов в онлайн-режиме в условиях устойчивой синхронизации между передающей и принимающей сторонами наблюдалось точное воспроизведение переданной информации.

С целью установки условий шифрования, при которых зашифрованные информационные последовательности обладают свойствами псевдослучайных последовательностей, производилось их тестирование тестами NIST STS. Результаты приведены в **таблице**.

В результате тестирования было установлено, что при λ = 3,85 последовательности обладают

Результаты прохождения тестов NIST STS

Название теста	Значение p-value	Прохождение, %
Частотный побитовый тест	0,345	99
Частотный блочный тест	0,297	96
Тест на последовательность одинаковых битов	0,654	97,2
Тест на самую длинную последовательность единиц в блоке	0,612	99
Тест рангов бинарных матриц	0,732	98
Спектральный тест	0,512	98
Тест на совпадение неперекрывающихся шаблонов	0,432	98,5
Тест на совпадение перекрывающихся шаблонов	0,371	97,5
Универсальный статистический тест Маурера	0,052	98
Тест на основе сжатия Лемпеля – Зива	0,299	97
Тест на линейную сложность	0,377	97,3
Тест приблизительной энтропии	0,342	98,1
Тест кумулятивных сумм	0,099	96
Тест на произвольные отклонения	0,645	99
Другой тест на произвольные отклонения	0,034	99
Тест на периодичность	0,087	97

свойствами псевдослучайных последовательностей и, следовательно, являются криптостойкими.

Заключение

Таким образом, предложена система передачи информации с шифрованием хаотическими последовательностями, генерированными в соответствии с логистическим уравнением $x_{n+1} = \lambda x_n(1-x_n)$ при $\lambda = 3{,}65 - 3{,}95$. Синхронизация системы передачи информации обеспечивается путем передачи по каналу связи через определенные интервалы времени текущего значения x_n, генерируемого логистическим отображением. Период передачи x_n зависит от быстродействия компьютера и расстояния между абонентами системы. При этом имеет место безошибочное воспроизведение текстовой информации на приемной стороне. Криптостойкость системы обуславливается количеством ключей шифрования, которое в данном случае было равно 10^{20}, что является достаточно хорошим результатом для двухпараметрической системы. Криптостойкость системы подтверждена результатами статистических тестов.

ИСПОЛЬЗОВАННЫЕ ИСТОЧНИКИ

1. Дмитриев А.С., Панас. А.И. Динамический хаос: новые носители информации для систем связи. – Москва: Издательство физико-математической литературы, 2002.

2. Кроновер Р. М. Фракталы и хаос в динамических системах. Основы теории. – Москва: Постмаркет, 2000.

3. 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.

4. Стасєв Ю. В., Васюта К. С., Женжера С. В. Інформаційні системи на основі динамічного хаосу // Системи озброєння і військова техніка. – 2009.– № 1 (17).– С. 134 – 138.

5. Савельев С. В. Счетное множество бинарных последовательностей для широкополосных систем связи на основе системы с динамическим хаосом // III Всероссийская конференция «Радиолокация и радиосвязь». – ИРЭ РАН, 2009. – С. 488 – 493.

6. Політанський Р. Л., Шпатар П. М., Гресь О. В., Ляшкевич В. Я. Шифрування інформації з використанням псевдовипадкових гаусових послідовностей // Восточно-европейский журнал передовых технологий. – 2012. – № 6/11 (60). – С. 8 – 10.

7. Andreyev Yu. V., Dmitriev A. S., Kuminov D. A., Starkov S. O. CDMA communications using maps with stored information // European Conference on Circuit Theory and Design. – Budapest. – 1997. – P. 324 – 329.

8. Політанський Р. Л., Політанський Л. Ф., Гресь О. В., Галюк С. Д. Система передавання даних з використанням генераторів хаосу // Всеукраинский межведомственный научно-технический сборник «Радиотехника». – 2011. – № 164. – С. 66 – 71.

9. Політанський Л.Ф., Кушнір М.Я., Політанський Р.Л., Еліяшів О.М., Невельський О.О., Величко С.В. Багатокористувальницька система зв'язку з використанням хаотичної частотної модуляції // Восточно-европейский журнал передових технологий. – 2010. – № 1/5 43). – С. 44 – 47.

10. Політанський Р. Л., Політанський Л. Ф., Шпатар П. М., Іванюк П. В. Кодування каналу передавання даних, шифрованих псевдовипадковими послідовностями // Восточно-европейский журнал передовых технологий. – 2013. – № 1/9(61). – С. 61 – 64.

11. Элияшив О. М., Галюк С. Д., Политанский Л. Ф., Кушнир Н. Я., Танасюк В. С. Непрерывная и импульсная синхронизация работы генераторов Чуа // Технология и конструирование в электронной аппаратуре. – 2012. – № 1. – С. 22 – 26.

Дата поступления рукописи в редакцию 05.08 2013 г.

Р. Л. ПОЛІТАНСЬКИЙ, П. М. ШПАТАР, О. В. ГРЕСЬ, А. Д. ВЕРИГА
Чернівецький національний університет імені Юрія Федьковича
E-mail: alexgs85@ukr.net

СИСТЕМА ПЕРЕДАВАННЯ ДАНИХ З ШИФРУВАННЯМ ХАОТИЧНИМИ ПОСЛІДОВНОСТЯМИ

У статті представлено реалізацію системи передавання даних з шифруванням послідовностями, генерування яких здійснюється на основі одновимірних дискретних хаотичних відображень із забезпеченням синхронізації передавальної і приймальної сторін системи. Роботу системи продемонстровано на прикладі передавання інформації між користувачами.

Ключові слова: хаотична послідовність, початкові умови, логістичне відображення, синхронізація.

DOI: 10.15222/TKEA2014.2-3.28
UDC 621.391

R. L. POLITANS'KYY, P. M. SHPATAR, A. V. HRES, A. D. VERIGHA
Yuriy Fedkovych Chernivtsi National University
E-mail: alexgs85@ukr.net

DATA TRANSMISSION SYSTEM WITH ENCRYPTION BY CHAOTIC SEQUENCES

Protection of transferable information in the telecommunication systems is possible by its imposition of coding sequence on a plaintext. Encryption of pseudorandom sequences can be performed by using generation algorithms which are implemented on the basis of the phenomenon of dynamical chaos, which is sensitive to changes in the initial conditions. One of the major problems encountered in the construction of secure communication systems is to provide synchronization between the receiving and transmitting parties of communication systems. Improvement of methods of hidden data transfer based on the systems with chaotic synchronization is the important task of research in the field of information and telecommunication systems based on chaos.

This article shows an implementation of a data transmission system, encrypted by sequences, generated on the basis of one-dimensional discrete chaotic maps with ensuring synchronization of the transmitting and receiving sides of the system. In this system realization of synchronization is offered by a transmission through certain time domains of current value of x_n generated by a logistic reflection. X_n transmission period depends on computer speed and distance between subscribers of the system. Its value is determined by transmitting a test message before the session. Infallible reception of test message indicates the optimal choice of a transmission period of the current value of x_n. Selection period is done at the program level. For the construction of communication network modern software was used, in particular programming language Delphi 7.0. The work of the system is shown on the example of information transmission between the users of the system. The system operates in real time full duplex mode at any hardware implementation of Internet access. It is enough for the users of the system to specify IP address only.

Keywords: chaotic sequence, initial conditions, logistic map, synchronization.

REFERENCES

1. Dmitriev A.S., Panas. A.I. *Dinahmicheskii khaos: novye nositeli informatsii dlya sistem svyazi* [Dynamical chaos: new media for communication systems]. Moscow, Publishing physical and mathematical literature, 2002, 252 p.

2. Kronover P.M. *Fraktaly i khaos v dinamicheskikh sistemakh. Osnovy teorii.* [Fractals and chaos in dynamical systems. Fundamentals of the theory]. Moscow, Postmarket, 2000, 350 p.

3. Koronovskii A. A., Moskalenko O. I., Khramov A. E. [On the use of chaotic synchronization for secure communication]. *Uspekhi fizicheskikh nauk*, 2009, vol. 179, no 12, pp. 1281-1310. (in Russian)

4. Stasyev Yu. V., Vasyuta K. S., Zhenzhera S. V. [Information systems based on dynamic chaos]. *Sistemi ozbroyennya i viis`kova tekhnika*, 2009, no 1 (17), pp. 134-138. (in Ukrainian)

5. Saveliev S.V. Countable set of binary sequences for broadband communication systems based on a system with dynamic chaos. *Proc. of the III Russian Conference «Radar and radio» IRE–2009*, pp. 488-493. (in Russian)

6. Politans'kyy R.L., Shpatar P.M., Gres A.V., Liashkevych V.Ya. [Information encryption using pseudorandom gaussian sequences]. *Vostochno-evropeiskii zhurnal peredovikh tekhnologii*, 2012, no 6/11 (60), pp. 8–10. (in Ukrainian)

7. Andreyev Yu. V., Dmitriev A. S., Kuminov D. A., Starkov S. O. CDMA communications using maps with stored information. *European Conference on Circuit Theory and Design*, Budapest, 1997, pp. 324-329.

8. Politans`kii R.L., Politans`kii L.F., Gres` O.V., Galyuk S.D. [Data transmission system using chaos generators]. *Vseukrainskii mezhvedomstvennyi nauchno-tekhnicheskii sbornik «Radiotekhnika»*, 2011, no 164, pp. 66-71. (in Ukrainian)

9. Politans'kyy L.F., Kushnir M.Ya., Politans'kyy R.L., Eliyashiv O.M., Nevel'sky O.O., Velichko S.V. [The multiuser communication system with use of chaotic frequency modulation] *Vostochno-evropeiskii zhurnal peredovikh tekhnologii*, 2010, no 1/5 (43), pp. 44-47. (in Ukrainian)

10. Politans'kyy R.L., Politans'kyy L.F., Shpatar P.M., Ivaniuk P.V. [Coding of channel of data transmission encrypted by pseudo-random sequences]. *Vostochno-evropeiskii zhurnal peredovikh tekhnologii*, 2013, № 1/9 (61), pp. 61-64. (in Ukrainian)

11. Eliyashiv O.M., Galyuk S.D. , Politans`kii L.F., Kushnir N.Ya., Tanasyuk V.S. [Continuous and pulse synchronization of generators Chua] *Tekhnologiya i Konstruirovanie v Elektronnoi Apparature*, 2012, no 1, pp. 22-26. (in Russian)