УДК 004.056.5

Е. В. Ананасов, И. В. Георгица

МЕТОД ОБРАБОТКИ НЕЛИНЕЙНЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ ДЛЯ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ИНФОКОММУНИКАЦИОННЫХ СЕТЯХ

Повышение требований к телекоммуникационным системам по своевременности, достоверности и безопасности передачи, хранения и обработки информации связано с усложнением функциональных задач, возложенных на системы управления. Задача обеспечения помехоустойчивости и безопасности при использовании информационных технологий в настоящее время решается на этапе передачи основной информации, в то время как на этапе обработки служебно-технологических команд из-за воздействия преднамеренных помех возможна потеря надежности. Предлагается метод обработки информации, цель которого – обеспечение помехоустойчивости и информационной безопасности инфокоммуникационных сетей в условиях «информационной войны» за счет увеличения линейной сложности применяемых последовательностей при формировании служебно-технологической информации. Метод основан на применении нелинейных рекуррентных последовательностей для формирования служебно-технологической информации. Приведено описание процесса формирования нелинейных рекуррентных последовательностей, позволяющих повысить скрытность и безопасность передачи информации в сложной помеховой обстановке. Сформулирована задача оптимального приема служебной технологической информации, заключающаяся в обнаружении факта наличия приема этой информации по дискретизированным отсчетам и получении текущей оценки вектора состояния последовательности. С помощью полученных уравнений дискретизированных отсчетов возможен переход от представления логических операций с дискретными значениями к соответствующим им арифметическим с аналоговыми значениями. На основании приведенных правил квантования аналоговых величин и правил фиксации корректного приема служебно-технологической информации сделан вывод о ее соответствии переданной информации, если наблюдается совпадение состояний значений начальных условий и оценочных значений на протяжении n тактов обработки. Суть предлагаемого способа заключается в том, что оценка очередного элемента информации производится в аналоговом виде с учётом предсказанного значения, сформированного на основе рекуррентных свойств псевдослучайной последовательности. Отличительные особенности данного метода: отказ от предварительного квантования сигнала, учет рекуррентных свойств последовательностей по предсказанию очередных элементов сигнала, обработка в аналоговом виде с последующим квантованием.

Ключевые слова: «информационная война», служебно-технологическая информация, нелинейные последовательности, оптимальный приём, дискретно-аналоговая обработка.

Введение

Непрерывное повышение сложности и важности задач, которые решаются с использованием инфокоммуникационных сетей, предполагает совершенствование системы управления, которая, в свою очередь, предъявляет повышенные требования к телекоммуникационным системам по своевременности, достоверности и безопасности передачи, хранения и обработки информации.

Задача обеспечения помехоустойчивости и безопасности при использовании информационных технологий в настоящее время решается на этапе передачи основной информации, в то время как на этапе обработки служебно-технологической информации (СТИ) инфокоммуникационные сети подвержены воздействию преднамеренных помех и потере надёжности.

Целью наших исследований являлась разработка метода, позволяющего обеспечивать помехоустойчивость и информационную безопасность инфокоммуникационных сетей в условиях «информационной войны».

При передаче СТИ (сигналы синхронизации, маркировки, маршрутизации и др.) в инфокоммуникационных сетях для обеспечения конфиденциальности используются известные режимы формирования последовательностей с низкой структурной стойкостью, что дает возможность информационному противнику определить их структуру, разведать тип используемой аппаратуры и осуществить постановку помех или ввод ложной информации [1–4].

Метод, предложенный в работе, позволяет обеспечить необходимый уровень информационной безопасности в сетях благодаря увеличению структурной сложности последовательностей, формирующих СТИ.

Нелинейные рекуррентные последовательности (НЛРП) находят все большее применение в радиоэлектронной технике для обеспечения защиты от преднамеренных помех, для устранения демаскирующих признаков работы соответствующих типов аппаратуры передачи дискретных сообщений, в радиолокационной технике и др.

Постановка задачи

Нелинейные рекуррентные последовательности формируются путем усложнения структуры линейных рекуррентных регистров (ЛРР) нелинейным узлом усложнения (НУУ) [1, 3]. Возможны различные варианты построения таких генераторов, например с внешней нелинейной логикой (рис. 1) с использованием генератора хаотических импульсов (ГХИ) по алгоритму Ристенбатта.

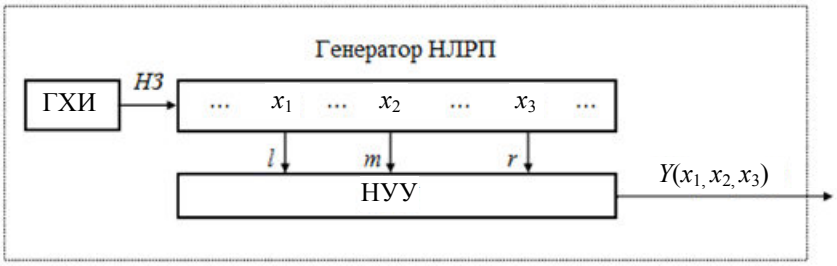

Рис. 1. Структурная схема генератора Ристенбатта

Выходной элемент псевдослучайной последовательности (ПСП) в данном примере формируется согласно функции Ристенбатта $Y(x_1, x_2, x_3) = \bar{x}_3 x_1 + x_2 \bar{x}_1$, где x_1, x_2, x_3 – значения элементов ПСП.

Сигнал, наблюдаемый на входе приёмного устройства, представляет собой смесь $\xi_{ij} = S(F(\bar{X}_{(lmr)ij}) + n_{ij})$, где S – функция, определяемая законом модуляции; $F(\bar{X}_{(lmr)ij})$ – функция нелинейного преобразования; n_{ij} – отсчеты гауссовской помехи; l, m, r – отводы регистра в соответствии с выходными элементами x_1, x_2, x_3.

Для приёма последовательностей Ристенбатта получим уравнения дискретизированных отсчётов (ДО), лежащих внутри тактовых интервалов (ТИ):

$$x'_{lij} = K_1 x'_{li(j-1)} + K_2 \frac{\partial F(x'_{li(j-1)}, x'_{mi(j-1)}, x'_{ri(j-1)})}{\partial x'_{li(j-1)}} (\xi_{ij} - F(x'_{ni(j-1)}, x'_{mi(j-1)}, x'_{ri(j-1)})); \quad (1)$$

$$x'_{mij} = K_1 x'_{mi(j-1)} + K_2 \frac{\partial F(x'_{li(j-1)}, x'_{mi(j-1)}, x'_{ri(j-1)})}{\partial x'_{mi(j-1)}} (\xi_{ij} - F(x'_{li(j-1)}, x'_{mi(j-1)}, x'_{ri(j-1)})); \quad (2)$$

$$x'_{rij} = K_1 x'_{ri(j-1)} + K_2 \frac{\partial F(x'_{li(j-1)}, x'_{mi(j-1)}, x'_{ri(j-1)})}{\partial x'_{ri(j-1)}} (\xi_{ij} - F(x'_{li(j-1)}, x'_{mi(j-1)}, x'_{ri(j-1)})), \quad (3)$$

где $x'_{lmri(j-1)}$ – начальные условия для оценки внутри ДО заданных элементов с выхода отводов l, m, r последовательности на предыдущем (j – 1)-м ДО; K_1 и K_2 – нормировочные коэффициенты; K_1 – оценка степени доверия к откорректированным начальным условиям ДО, K_2 – оценка степени доверия к оценочному значению, принятому из сети, величина коэффициентов выбирается в дискретно-аналоговом виде от 0 до1; ξ_{ji} – наблюдаемая смесь; $F(x'_{li(j-1)}, x'_{mi(j-1)}, x'_{ri(j-1)})$ – аналоговое значение нелинейной функции преобразования от заданных элементов последовательности на (j – 1)-м ДО; $\frac{\partial F(x'_{li(j-1)}, x'_{mi(j-1)}, x'_{ri(j-1)})}{\partial x'_{lmri(j-1)}}$ – значения частных производных функции F по элементам l, m, r.

Для приёма последовательностей Ристенбатта имеем уравнения, полученные на границах ТИ:

$$x'_{lij} = x'_{l(i-1)j} + K\frac{\partial F(x'_{l(i-1)j},\, x'_{m(i-1)j},\, x'_{r(i-1)j})}{\partial x'_{l(i-1)j}} \times (\xi_{ij} - F(x'_{l(i-1)j},\, x'_{m(i-1)j},\, x'_{r(i-1)j})); \quad (4)$$

где $x'_{lmr(i-1)j}$ – начальные условия для оценки на границах ТИ l, *m*, *r* заданных элементов последовательностей, использованные в предыдущем ТИ; $F(x'_{l(i-1)j},\, x'_{m(i-1)j},\, x'_{r(i-1)j})$ – значение нелинейной функции от заданных элементов последовательности на каждом предыдущем ТИ; $\frac{\partial F(x'_{l(i-1)j},\, x'_{m(i-1)j},\, x'_{r(i-1)j})}{\partial x'_{lmr(i-1)j}}$ – значения частных производных функции *G* по соответствующим компонентам l, *m*, *r* на (*i* – 1)-м ТИ.

Если на передаче выходной элемент ПСП, например, формируется как

$$Y(x_1, x_2, x_3) = \overline{x}_3 x_1 + x_2 \overline{x}_1,$$

то на приеме соответствующий элемент опорной последовательности (ОП) будет формироваться в аналоговом виде в соответствии с функцией

$$G(x'_1,\, x'_2,\, x'_3) = x'_1 + x'_2 - x'_1 x'_2 - x'_1 x'_3.$$

Нетрудно убедиться в совпадении таблиц истинности значений как для дискретных, так и для аналоговых величин (табл.).

Таблица истинности значений узла выборки с инверсией с первым управляющим входом для дискретных/аналоговых значений

x_1 / x'_1	x_2 / x'_2	x_3 / x'_3	$Y(x_1, x_2, x_3) / G(x'_1, x'_2, x'_3)$
$0 / x'_1 \le 0,5$	$0 / x'_2 \le 0,5$	$0 / x'_3 \le 0,5$	$Y = 0 / G \le 0,5$
$0 / x'_1 \le 0,5$	$1 / x'_2 > 0,5$	$0 / x'_3 \le 0,5$	$Y = 1 / G > 0,5$
$1 / x'_1 > 0,5$	$0 / x'_2 \le 0,5$	$0 / x'_3 \le 0,5$	$Y = 1 / G > 0,5$
$1 / x'_1 > 0,5$	$1 / x'_2 > 0,5$	$0 / x'_3 \le 0,5$	$Y = 1 / G > 0,5$
$0 / x'_1 \le 0,5$	$0 / x'_2 \le 0,5$	$1 / x'_3 > 0,5$	$Y = 0 / G \le 0,5$
$0 / x'_1 \le 0,5$	$1 / x'_2 > 0,5$	$1 / x'_3 > 0,5$	$Y = 1 / G > 0,5$
$1 / x'_1 > 0,5$	$0 / x'_2 \le 0,5$	$1 / x'_3 > 0,5$	$Y = 0 / G \le 0,5$
$1 / x'_1 > 0,5$	$1 / x'_2 > 0,5$	$1 / x'_3 > 0,5$	$Y = 0 / G \le 0,5$

Аналоговые величины имеют значение, соответствующее области определения, $x'_1, x'_2, x'_3 \in [0,1]$, правило квантования в рассматриваемом примере имеет следующий вид:

$$F(x'_1, x'_2, x'_3) = \begin{cases} 1, \text{ если } F(x'_1, x'_2, x'_3) > 0,5, \\ 0, \text{ если } F(x'_1, x'_2, x'_3) \le 0,5. \end{cases} \quad (5)$$

Признаком фиксации верного приема является выполнение правила

$$\sum_{i=1}^{n} (x'_{lmr} + x_{lmr}) \bmod 2 \ge 0 \begin{cases} 0, \text{ приём СТИ}, \\ > 0, \text{ нет приёма СТИ}, \end{cases}$$

т. е. СТИ можно считать принятой корректно в соответствии с переданной, если присутствует совпадение и начальных условий, и оценочных значений на протяжении определенного количества тактов обработки.

В основе предлагаемого способа лежит оценка очередного элемента передаваемой информации с учетом предсказанного значения в аналоговом виде с использованием рекуррентных свойств последовательностей.

Для этого необходимо преобразовать представление логических операций, работающих с дискретными значениями, к полностью соответствующим им арифметическим операциям, использующим аналоговые значения. Возможность такого преобразования освещена в [1, 2].

Графическая интерпретация предлагаемого метода обработки нелинейных последовательностей представлена на рис. 2. Выходные элементы ПСП формируются в соответствии с нелинейной функцией (рис. 2, *а*). Из принимаемой смеси, изображенной на рис. 2, *б*, выделяют импульсы тактовой частоты F_t (рис. 2, *в*), затем, для получения ДО, импульсы тактовой частоты дискретизируют с частотой, значение которой в k раз превышает тактовую (рис. 2, *г*). После дискретизации производится корректировка каждого ДО.

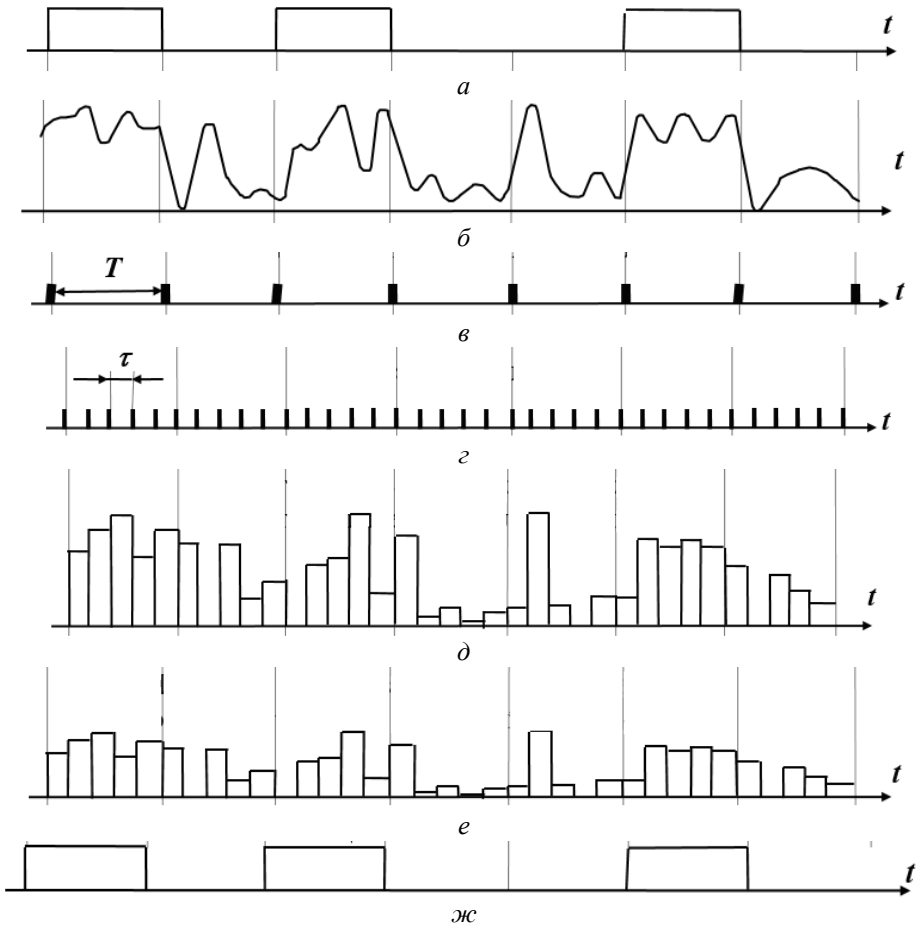

Рис. 2. Графическая интерпретация метода оптимального приёма СТИ:
а – сигналы на выходе передачи; *б* – принятый сигнал;
в – импульсы тактовой частоты; *г* – импульсы дискретизации;
д – аналоговые дискретизированные отсчеты принятых элементов последовательности;
е – предсказанные аналоговые дискретизированные отсчеты принятых элементов последовательности;
ж – квантовые оценочные значения элементов ПСП

Обработка сигнала осуществляется внутри и на границах ТИ. На границах ТИ на первом ДО ПСП формируют начальные условия – это откорректированные значения соответствующих элементов ОП. Корректируются одновременно три заданных значения, которые участвовали в формировании выходного элемента ПСП. Затем откорректированные значения соответствующих элементов ОП, которые были получены на первом ДО СТИ, задерживают на время τ, равное длительности ДО. После этого корректируются заданные значения элементов ОП на дальнейших ДО (см. формулы (1)–(3) . Значение, прошедшее корректировку на последнем ДО, принимается как откорректированное значение элемента в целом и используется как значение начальных условий для обработки следующего элемента, а на границах ТИ обработка производится по формуле (4).

Осуществляется также корректировка в последующих ветвях обработки (рис. 2, *е*). После корректировки производится квантование сигнала согласно формуле (5) (рис. 2, *ж*). В результате формируется СТИ, аналогичная передаваемой. Получение откорректированных значений сигнала, с учётом принимаемых предсказанных, не прекращается и производится непрерывно с целью получения предсказанных значений сигнала для сокращения времени при повторном приёме.

Выводы

Отличительными особенностями предложенного метода являются: при передаче – использование нелинейных последовательностей, сформированных генератором Ристенбатта; на приёме – использование начальных условий для предсказания очередных элементов сигнала; на всех этапах обработки – корректировка элементов последовательности; на предварительном этапе – квантование сигнала; на завершающем – обработка принятого сигнала в дискретно-аналоговом виде. Работоспособность метода для решения задач по повышению помехозащищенности и обеспечению безопасности информации в инфокоммуникационных сетях подтверждена имитационными исследованиями.

Применение последовательностей Ристенбатта обеспечивает возрастание эквивалентной линейной сложности последовательности (под которой будем понимать длину ЛРР, генерирующего такую же последовательность, что и нелинейный) в соответствии с формулой [5]:

$$n_э = n\,(n-1), \qquad (6)$$

где $n_э$ – эквивалентная линейная сложность; n – длина ЛРР. Сравнительная оценка роста эквивалентной линейной сложности НЛРП (верхняя кривая) по сравнению с линейной рекуррентной последовательностью (ЛРП) при одинаковой длине регистра представлена на рис. 3.

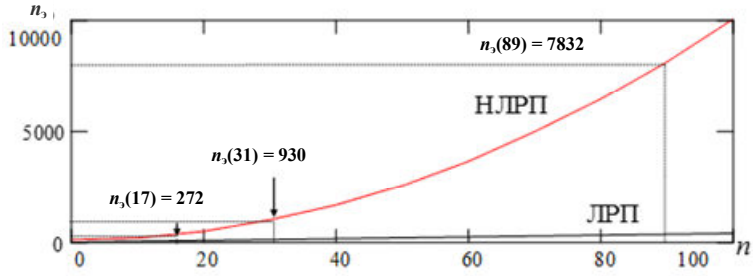

Рис. 3. График возрастания эквивалентной линейной сложности

Например, при использовании ЛРР с $n = 31$ эквивалентная линейная сложность последовательности возрастает с 31 до 930, в соответствии с формулой (6).

Это дает возможность значительно – в десятки раз – повысить скрытность передаваемой СТИ по каналу связи по сравнению с известными режимами формирования последовательностей с низкой структурной стойкостью, что не позволит информационному противнику своевременно осуществить постановку помех или ввод ложной информации.

СПИСОК ЛИТЕРАТУРЫ

1. *Апанасов Е. В.* Способ и устройство синхронизации псевдослучайных последовательностей для повышения безопасности связи / Е. В. Апанасов, А. Г. Прыгунов // Вопросы защиты информации. 2005. № 1 (68). С. 27–29.

2. *Апанасов Е. В.* Применение способа формирования и приёма служебной информации для повышения помехозащищённости систем радиосвязи в условиях «информационной войны» / Е. В. Апанасов, А. Г. Прыгунов, В. В. Слесарев // Изв. Южн. федер. ун-та. Технические науки. 2011. № 1 (114). С. 67–72.

3. *Введение* в криптографию / под общ. ред. В. В. Ященко. М.: МЦНМО, ЧеРо, 1998. 272 с.

4. *Диффи У.* Защищённость и имитостойкость. Введение в криптографию / У. Диффи, М. Э. Хеллман // Тр. Ин-та инженеров по электротехнике и радиоэлектронике. 1979. Т. 67, № 3. С. 71–109.

5. *Уорд Р.* Различение псевдослучайных сигналов методами последовательной оценки / Р. Уорд // Зарубежная радиоэлектроника. 1966. № 8. С. 20–37.

Статья поступила в редакцию 31.03.2015,
в окончательном варианте – 23.06.2015

ИНФОРМАЦИЯ ОБ АВТОРАХ

Апанасов Евгений Викторович – Россия, 346428, Новочеркасск; Южно-Российский государственный политехнический университет (НПИ) им. М. И. Платова; канд. техн. наук, доцент; доцент кафедры «Информационная безопасность, телекоммуникационные системы и информатика»; apanev@yandex.ru.

Георгица Ирина Викторовна – Россия, 346428, Новочеркасск; Южно-Российский государственный политехнический университет (НПИ) им. М. И. Платова; канд. экон. наук, доцент кафедры «Информационная безопасность, телекоммуникационные системы и информатика»; i-georgitsa@yandex.ru.

E. V. Apanasov, I. V. Georgitsa

METHOD OF PROCESSING OF NON-LINEAR SEQUENCES TO ENSURE INFORMATION SECURITY IN COMMUNICATION NETWORKS

Abstract. The increasing demands for telecommunication systems for timeliness, reliability and security of transmission, storage and processing of information are caused by the complexity of the functional tasks assigned to these systems. The issues of providing noise immunity and security in the transmission of information are currently solved at the stage of transmitting the basic information, but at the stage of processing service and technology commands the loss of reliability is possible due to the impact of intentional disturbances. The method of information processing is proposed; its purpose is to provide noise immunity and information security of informational and communicational networks in the conditions of "informational war" by increasing the linear complexity of the used sequences while collecting service and technological information. The method is based on the use of non-linear recurrent sequences to form the service and technological information. The paper describes the process of formation of non-linear recurrent sequences that improve the secrecy and security of information transfer in the complex interference environment. The problem of optimal acceptance of the service and technology information is stated. The problem consists in the detection of the information perception by discretized samples and obtaining a current assessment of the sequence state vector. On the base of the obtained equations of the discretized samples it is possible to convert the presentation of logic operations with discrete values to their corresponding arithmetic operations with analog values. Based on the rules of quantization of the analog data and the rules of fixation of the correct perception of the service-technological information, the conclusion on the information conformity to the sent information is made if there is a coincidence of the state of the initial condition data and evaluation data for n cycles of processing. The essence of the proposed method lies in the fact that the evaluation of the next item of information is made in the analog form, taking into account the predicted values generated on the basis of the recurrent properties of the pseudo-random sequence. The distinctive features of this method are refusal from pre-quantization of the signal, consideration of the recurrent properties of the sequences according to the prediction of the next elements of the signal and processing in the analog form with subsequent quantization.

Key words: "information war", service-technological information, non-linear sequences, optimal reception, discrete analog processing.

REFERENCES

1. Apanasov E. V., Prygunov A. G. Sposob i ustroistvo sinkhronizatsii psevdosluchainykh posledovatel'nostei dlia povysheniia bezopasnosti sviazi [Method and instrument of the synchronization of pseudo-random sequences for increase in communication security]. *Voprosy zashchity informatsii*, 2005, no. 1 (68), pp. 27–29.

2. Apanasov E. V., Prygunov A. G., Slesarev V. V. Primenenie sposoba formirovaniia i priema sluzhebnoi informatsii dlia povysheniia pomekhozashchishchennosti sistem radiosviazi v usloviiakh «informatsionnoi voiny» [Application of the way of formation and reception of the service information to increase noninterference of the radio systems in conditions of "informational war"]. *Izvestiia Iuzhnogo federal'nogo universiteta. Tekhnicheskie nauki*, 2011, no. 1 (114), pp. 67–72.

3. *Vvedenie v kriptografiiu* [Introduction to cryptography]. Pod obshchei redaktsiei V. V. Iashchenko. Moscow, MTsNMO, CheRo Publ., 1998. 272 p.

4. Diffi U., Khellman M. E. Zashchishchennost' i imitostoikost'. Vvedenie v kriptografiiu [Protection and spoofing resistance. Introduction to cryptography]. *Trudy Instituta inzhenerov po elektronike i radiotekhnike*, 1979, vol. 67, no. 3, pp. 71–109.

5. Uord R. Razlichenie psevdosluchainykh signalov metodami posledovatel'noi otsenki [Distinction of pseudo-random signals using the methods of sequent assessment]. *Zarubezhnaia radioelektronika*, 1966, no. 8, pp. 20–37.

The article submitted to the editors 31.03.2015,
in the final version – 23.06.2015

INFORMATION ABOUT THE AUTHORS

Apanasov Evgeniy Viktorovich – Russia, 346428, Novocherkassk; South-Russian State Polytechnic University (NPI) named after M. I. Platov; Candidate of Technical Sciences, Assistant Professor; Assistant Professor of the Department "Information Security, Telecommunication Networks and Information Science"; apanev@yandex.ru.

Georgitsa Irina Viktorovna – Russia, 346428, Novocherkassk; South-Russian State Polytechnic University (NPI) named after M. I. Platov; Candidate of Economics, Assistant Professor; Assistant Professor of the Department "Information Security, Telecommunication Networks and Information Science"; i-georgitsa@yandex.ru.