УДК 621.319.53; 681.3

В.Н. Максымовыч, М.Н. Мандрона, Ю.М. Костив, О.И. Гарасимчук

ИССЛЕДОВАНИЕ СТАТИСТИЧЕСКИХ ХАРАКТЕРИСТИК ГЕНЕРАТОРОВ ПУАССОНОВСКИХ ИМПУЛЬСНЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ, ПОСТРОЕННЫХ РАЗЛИЧНЫМИ СПОСОБАМИ

Введение

Генераторы пуассоновских импульсных последовательностей (ГПИП) используются при имитационном моделировании, в измерительной технике, средствах связи, радиолокации, системах защиты информации и др. [1–4]. В зависимости от цели и области применения ГПИП они могут быть реализованы как аппаратными, так и программными средствами.

В работах [5–7] предложена новая структура ГПИП (рис. 1) и усовершенствованная методика оценки качества импульсной последовательности на соответствие пуассоновским законом распределения.

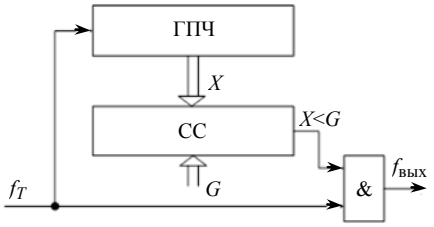


Рис. 1

В состав генератора входят: генератор псевдослучайных чисел (ГПЧ), схема сравнения (СС) и логический элемент И. Входные тактовые импульсы проходят на выход устройства при условии, что число на выходе ГПЧ (X) меньше управляющего кода G. Средняя частота выходных импульсов определяется уравнением

$$f_{\text{out}} = \frac{G}{2^m} f_T ,$$

где f_T — частота повторения тактовых импульсов, m — количество двоичных разрядов ГПЧ и СС.

В предложенной методике оценки качества ГПИП [8, 9] поток входных импульсов разделяется на n одинаковых групп, каждая из которых состоит из $i_{\max}$ импульсов. Максимальное количество групп — $n_{\max}$. Группам входных импульсов соответствуют группы выходных импульсов с числом импульсов k_1, k_2, …, $k_{n_{\max}}$.

Методика основана на классической методике проверки гипотезы о распределении генеральной совокупности по закону Пуассона с использованием критерия Пирсона (критерия χ^2) [10]. При этом с учетом специфики построения ГПИП предложены следующие дополнения:

- фиксируется номинальное (теоретическое) среднее значение чисел k_1, k_2, …, $k_{n_{\max}}$ (k_c) независимо от значения управляющего кода G;
- значение $i_{\max}$ переменное, зависит от значения G и определяется уравнением

$$i_{\max} = \frac{2^m}{G} k_c .$$

В результате использования предложенной методики для каждого значения G определяется значение χ_c^2. Далее по таблицам критических точек рас-

пределения χ^2 [10] и избранными уровнем значимости α (обычно α предоставляют одно из трех значений: 0,1; 0,05; 0,01) и числом степеней свободы r находят критическое значение $\chi^2_{сч}$. Если $\chi^2_c < \chi^2_{сч}$, нет оснований не принимать гипотезу о соответствии импульсного потока пуассоновскому закону распределения.

Разработанная улучшенная методика использовалась для оценки ГПИП различных типов, что дало возможность в определенной степени оптимизировать их структуру и алгоритмы работы. Однако большое количество возможных вариантов реализации ГПЧ, которые являются основой ГПИП, позволяет продолжать поиск лучших решений с учетом основных параметров генераторов: статистических характеристик импульсной последовательности, диапазона ее средних частот, быстродействия, сложности (технологичности) построения при аппаратной реализации.

Анализ статистических характеристик импульсных последовательностей

Статистические характеристики импульсных последовательностей анализируются при трех вариантах реализации ГПЧ: на основе функции random программной среды Delphi (при программной реализации ГПИП), на основе *R*-блока [11–13]; на основе модифицированного аддитивного генератора Фибоначчи (МАГФ) [12–14].

При этом особое внимание уделялось исследованию диапазона значений управляющего кода *G*, при котором обеспечивается соответствие выходного импульсного потока пуассоновскому закону распределения, и оптимизации структуры МАГФ, включая начальные состояния регистров генератора.

Результаты анализа статистических характеристик ГПИП на основе функции random, полученные с помощью имитационного моделирования, приведены на рис. 2.

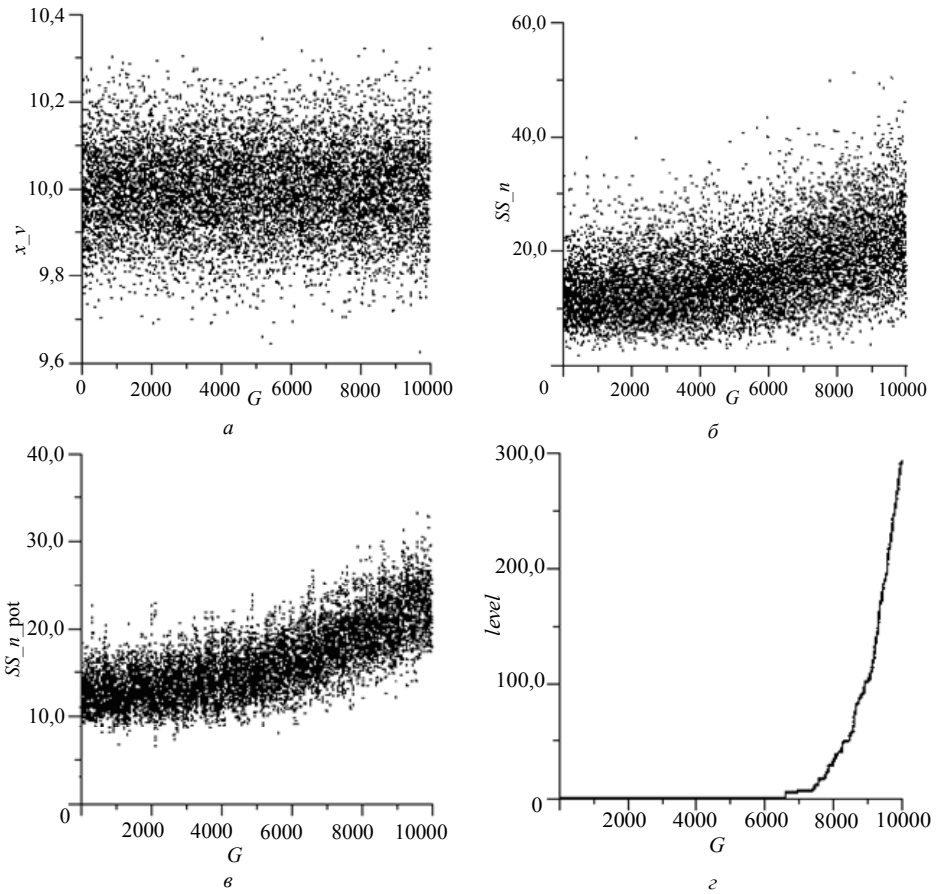


Рис. 2

Здесь представлены зависимости следующих величин от значения управляющего кода G:

а) средней величины значений k_1, k_2, …, $k_{n_{\max}}$ — $k_в$ (x_v);

б) значения χ_c^2 (SS_n);

в) усреднения величины пяти последних значений χ_c^2 — $\chi_{ссер}^2$ (SS_n_pot);

г) количества значений $\chi_{ссер}^2$, что превысили $\chi_{сч}^2$ — k_{level}.

Результаты получены при таких параметрах ГПИП:

$$m = 16,\ n_{\max} = 1000,\ k_c = 10,\ \chi_{сч}^2 = 25. \qquad (1)$$

Из зависимости k_{level} от G (рис. 2, *г*) следует, что в диапазоне значений $0 \div 6500$ управляющего кода G выходная импульсная последовательность ГПИП соответствует пуассоновскому закону распределения. Здесь и далее диапазоны значений G определяются примерно и при необходимости могут уточняться.

На рис. 3 приведена схема ГПЧ, реализованная с использованием *R*-блока [11–13]. В его состав входят регистры Рг 1–Рг3 и *R*-блок.

ГПЧ работает в соответствии с алгоритмом:

$$Q_1(t+1) = R_H[Q_2(t), Q_3(t), H],$$

$$Q_2(t+1) = Q_1(t),$$

$$Q_3(t+1) = Q_2(t),$$

где $Q_1(t)$, $Q_2(t)$, $Q_3(t)$ и $Q_1(t+1)$, $Q_2(t+1)$, $Q_3(t+1)$ — значения чисел в регистрах Рг1–Рг3 в текущем и следующем тактах работы устройства соответственно; R_H — функция преобразования, что реализуется *R*-блоком с помощью его внутренней таблицы *H*.

Некоторые результаты анализа статистических характеристик ГПИП при таком построении ГПЧ представлены на рис. 4. Они получены при тех же параметрах ГПИП, что и в предыдущем случае (1).

Зависимость k_{level} от G (рис. 4, *б*) позволяет сделать вывод, что в диапазоне значений $0 \div 6500$ управляющего кода G выходная импульсная последовательность ГПИП соответствует пуассоновскому закону распределения.

Статистические характеристики ГПИП получены при использовании методики заполнения таблиц *R*-блока, предложенной в [11, 12], и следующих начальных состояниях регистров: Рг1–0, Рг2–0, Рг3–1. Предварительные исследования показали, что в данном случае характеристики выходной импульсной последовательности незначительно зависят от этих начальных условий. Однако это требует дополнительных исследований.

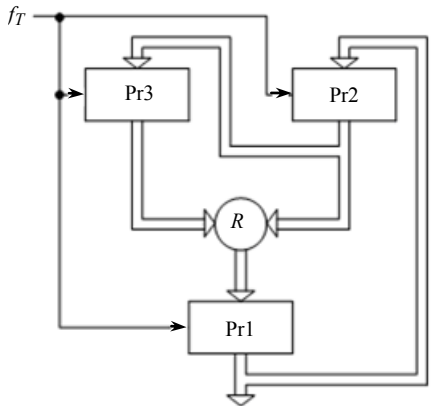


Рис. 3

ГПИП на основе функции random предназначен исключительно для программной реализации. ГПИП на основе *R*-блока может быть реализован как программно, так и аппаратно. Однако при

аппаратной реализации возникают сложности с построением *R*-блока и формированием его внутренних массивов [11–13]. Это приводит к усложнению и потере быстродействия. В связи с этим целесообразно построение ГПИП на основе других ГПЧ, допускающих простую аппаратную реализацию. Один из таких вариантов — ГПЧ на основе МАГФ [12, 14], схема которого приведена на рис. 5. В его состав входят регистры Рг1–Рг3, комбинационный сумматор (КС) и логическая схема (ЛС).

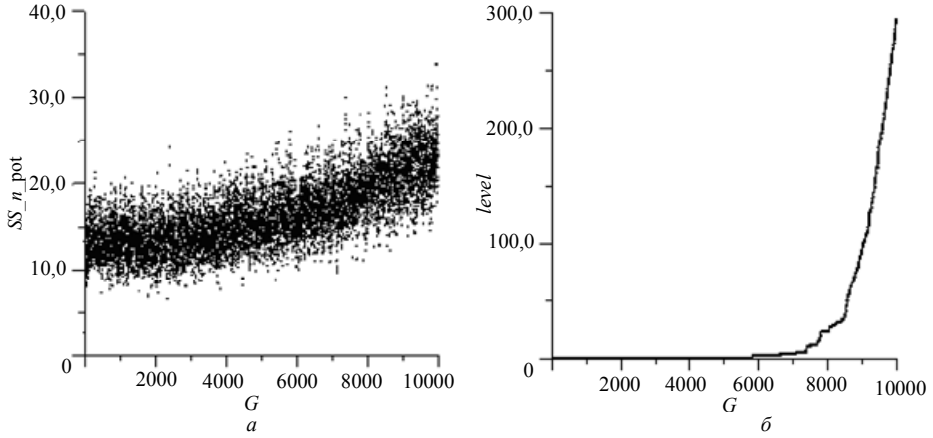


Рис. 4

МАГФ работает в соответствии с алгоритмом:

$$Q_1(\mathrm{t}+1) = [Q_2(t) + Q_3(t) + a] \bmod 2^m,$$

$$Q_2(t+1) = Q_1(t),$$

$$Q_3(t+1) = Q_2(t),$$

$$a = a_0 \oplus a_1 \oplus a_2 \oplus \cdots \oplus a_z, \quad (2)$$

где $Q_1(t) - Q_3(t)$ и $Q_1(t+1) - Q_3(t+1)$ — числа в регистрах Рг1–Рг3 в текущем и следующем тактах работы; a_i ($i = 0, 1, \ldots, z$; $z \le m - 1$) — значения двоичных разрядов числа Q_1 в регистре Рг1.

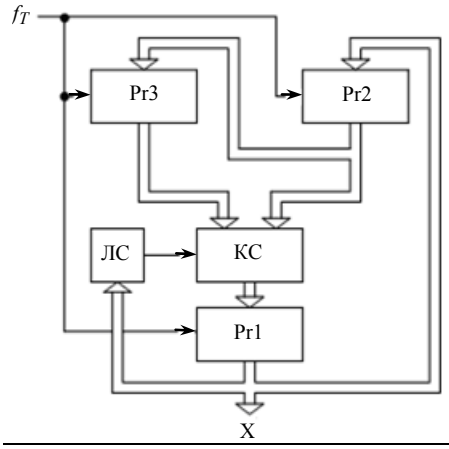
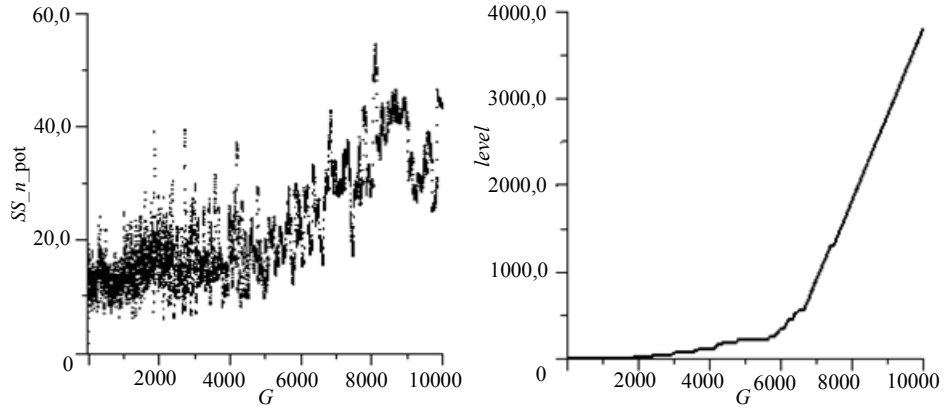


Рис. 5

В процессе работы выяснилось, что статистические характеристики ГПИП на основе МАГФ существенно зависят от начальных установок регистров Рг1–Рг3 и от количества членов уравнения (2), т.е. от количества двоичных разрядов Рг1, подключенных к ЛС.

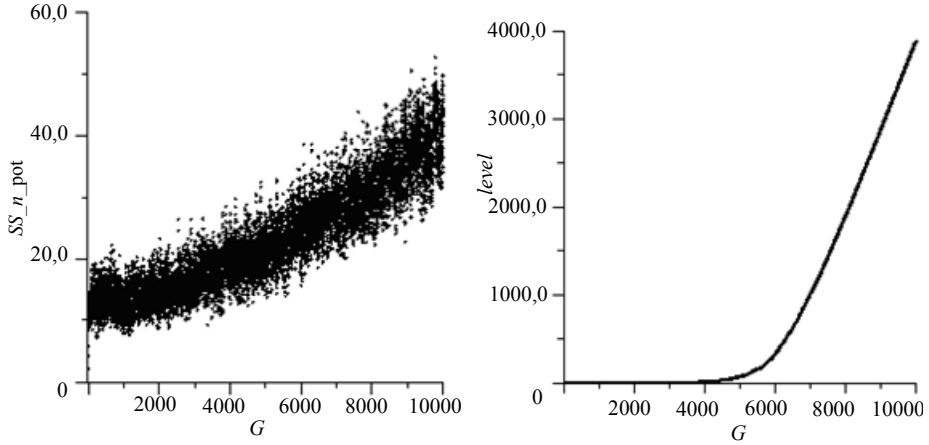
На рис. 6 и 7 приведены отдельные результаты при различных начальных состояниях регистров Рг1–Рг3 при соблюдении условия (1) и одинаковом способе подключения ЛС — $Q_1(0) = 0$, $Q_2(0) = 0$, $Q_3(0) = 1$, $a = a_0 \oplus a_1 \oplus \cdots a_{15}$.

Сравнив графики рис. 6, *б* и рис. 7, *б*, можно сделать вывод, что запись в регистр Рг1 в начальном состоянии числа $Q_1(0) = G$ вместо $Q_1(0) = 0$ позволяет существенно расширить диапазон значений управляющего кода, при котором выходная импульсная последовательность соответствует пуассоновскому закону распределения. Диапазон приблизительно увеличивается в два раза — от значения $0 \div 2000$ (см. рис. 6, *б*) до — $0 \div 4000$ (см. рис. 7, *б*).



а *б*

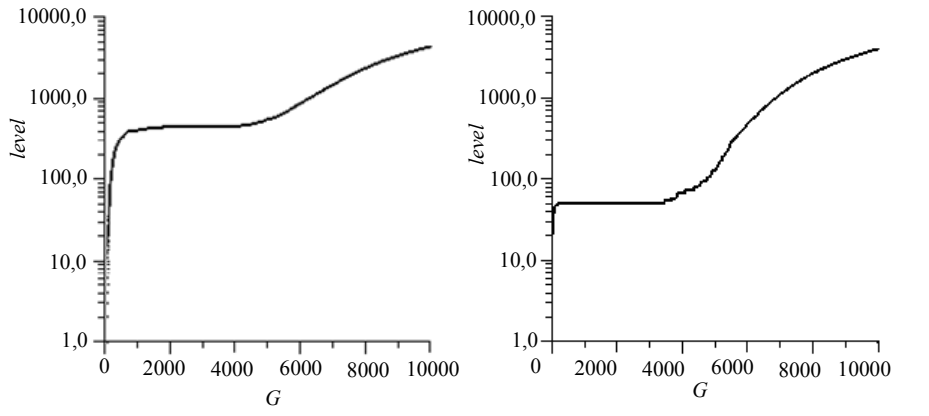
Рис. 6



а *б*

Рис. 7

На рис. 8 представлены зависимости величины k_{level} от G при разных способах подключения ЛС к КС и при одинаковых начальных условиях: $Q_1(0) = G$, $Q_2(0) = 0$, $Q_3(0) = 1$. Для лучшего восприятия отличий графики приведены в логарифмическом масштабе.

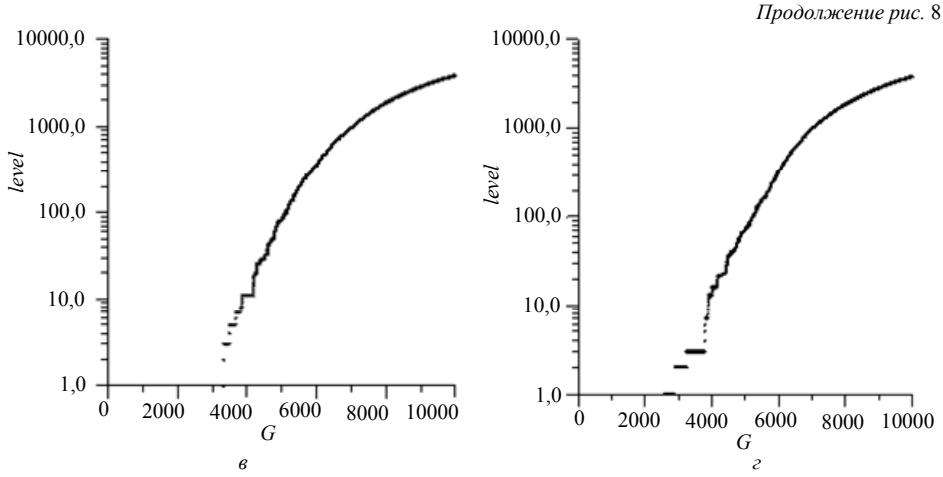


а *б*

Рис. 8

ISSN 0572-2691

Продолжение рис. 8



Таким образом, с увеличением задействованных членов уравнения (2) выходные импульсные последовательности ГПИП на основе МАГФ соответствуют пуассоновскому закону распределения в более широком диапазоне значений управляющего кода. Однако варианты построения ГПИП с небольшим (или даже нулевым) количеством разрядов регистра Рг1, подключенных к ЛС (рис. 8, *а*, *б* , где $a = 0$, $a = a_0 \oplus a_1 \oplus \cdots a_3$ соответственно), могут использоваться в более узких диапазонах значений управляющего кода. При этом не могут использоваться режимы работы генератора при малых значениях G, начиная с $G = 1$ (рис 8 *в*, *г* $a = a_0 \oplus a_1 \oplus \cdots a_7$ и $a = a_0 \oplus a_1 \oplus \cdots a_{15}$ соответственно).

Заключение

В настоящей работе показано, что ГПИП на основе функции random программной среды Delphi и на основе *R*-блока обеспечивают статистические характеристики выходной импульсной последовательности, соответствующие пуассоновскому закону распределения, в широком диапазоне значений управляющего кода по сравнению с ГПИП на основе МАГФ. Например, при количестве двоичных разрядов $m = 16$ диапазон допустимых значений управляющего кода для первых двух способов оставляет $0 \div 6500$, а для устройства на основе МАГФ — $0 \div 2000$ или $0 \div 4000$ в зависимости от начальных установок структурных элементов. Однако ГПИП на основе функции random предназначены только для программной реализации, а генераторы на основе *R*-блока чрезмерно сложные и имеют низкое быстродействие.

ГПИП на основе МАГФ существенно проще при аппаратной реализации и могут обеспечить гораздо большее быстродействие. Параметры их выходной последовательности существенно зависят от начальных установок его регистров Рг1–Рг3 и способа подключения логической схемы ЛС. Показано, что при увеличении количества двоичных разрядов Рг1, подключенных к ЛС, диапазон допустимых значений управляющего кода существенно расширяется. Кроме того, найдены начальные установки регистров, которые зависят от управляющего кода и позволяют расширить этот диапазон примерно в два раза.

В.М. Максимович, М.М. Мандрона, Ю.М. Костів, О.І. Гарасимчук

ДОСЛІДЖЕННЯ СТАТИСТИЧНИХ ХАРАКТЕРИСТИК ГЕНЕРАТОРІВ ПУАССОНІВСЬКИХ ІМПУЛЬСНИХ ПОСЛІДОВНОСТЕЙ, ПОБУДОВАНИХ РІЗНИМИ СПОСОБАМИ

Досліджено способи побудови генераторів пуассонівських імпульсних послідовностей на основі функції random програмного середовища Delphi,

R-блока та модифікованого адитивного генератора Фібоначчі. Досліджено їх статистичні характеристики та діапазони значень керуючого коду, при якому забезпечується відповідність вихідного імпульсного потоку пуассонівському закону розподілу.

V.N. Maksymovych, M.N. Mandrona, Yu.M. Kostiv, O.I. Harasymchuk

INVESTIGATION OF THE STATISTICAL CHARACTERISTICS OF PULSE SEQUENCES POISSON GENERATORS, WHICH ARE CONSTRUCTED IN DIFFERENT WAYS

The ways of building pulse sequences Poisson generators based on random functions of programming environment Delphi, on the basis of *R*–block and based on the modified Fibonacci additive generator are investigated. There are analysed their statistical characteristics and control code ranges, at which output pulse flow corresponds to Poisson's law of distribution.

1. *Syroka Z.* Generator liczb losowych o rozkładzie Poissona w symulacji procesów losowych w kanałach radiowych, Krajowa Konferencja Systemy Łączności i Informatyki na potrzeby obronności i bezpieczeństwa RP, 04–06.10. — 1995. — **2**. — P. 109–116.
2. *Wawrzynek J.* Metody opisu i wnioskowania statystycznego. — Wrocław: Wydawnictwo Akademii Ekonomicznej im. — 2007. — P. 56–57.
3. *Kuhl M.E., H. Damerdji and J.R.* Wilson. Estimating and simulating Poisson processes with trends or asymmetric cyclic effects, Proc. 1997 // Winter Simulation Conference. — Atlanta, 1997. — P. 287–295.
4. *Grabowski J.* Abstract Jacobi and Poisson structures. quantization and star–products // J. Geom. Phys. — 1992. — **9**. — P. 45–73.
5. *Генератори* тестових імпульсних послідовностей для дозиметричних пристроїв / О.І. Гарасимчук , В.Б. Дудикевич, В.М. Максимович, Р.Т. Смук // Вісник НУ «Львівська політехніка». — 2004. — № 506. — С. 187–193.
6. *Гарасимчук О.І.* Алгоритм формування пуассонівського імпульсного потоку // Автоматика, вимірювання та керування. — 2003. — № 475. — С. 21–25.
7. *Формування* пуассонівської імпульсної послідовності на основі генератора Голлманна / Ю.М. Костів, В.М. Максимович, О.І. Гарасимчук, М.М. Мандрона // Комп'ютерні системи та мережі. — 2014. — № 806. — С. 105–110.
8. *Методика* оптимізації параметрів генераторів пуассонівських імпульсних послідовностей, побудованих на основі лінійних конгруентних генераторів / В.М. Максимович, Ю.М. Костів, О.І. Гарасимчук, М.М. Мандрона // Науковий вісник НЛТУ України . — 2013. — Вип. 23.14. — С. 322–328.
9. *Methodology* for research of Poisson pulse sequence generators using Pearson's Chi–squared test / Yu.M. Kostiv, V.M. Maksymovych, O.I. Harasymchuk, M.M. Mandrona // Sustainable Development. — 2013. — N 9. — P. 67–72.
10. *Критические* точки распределения χ^2 . — http://math.semestr.ru/group/xixi.php.
11. *Дослідження* генераторів псевдовипадкових послідовностей, побудованих з використанням *R*-блоків / М.М. Мандрона, В.М. Максимович, Ю.Ю. Рибак, Ю.М. Костів, О.І. Гарасимчук // Інформаційна безпека. — 2013. — № 4 (12). — С. 84–92.
12. *Мандрона М.М.* Апаратні генератори псевдовипадкових бітових послідовностей з покращеними характеристиками : Дис. канд. техн. наук : 05.13.21. — Львів, 2015. — 146 с.
13. *Иванов М.А.*, *Чугунков И.В.*Теория, применение и оценка качества генераторов псевдослучайных последовательностей. — М.: КУДИЦ–ОБРАЗ, 2003. — 240 с.
14. *Mandrona M.M.*, *Maksymovych V.M.* Investigation of the statistical characteristics of the modified Fibonacci generators // Journal of Automation and Information Sciences. — 2014. — **46, N** 12. — P. 48–53.

Получено 10.08.2016
После доработки 12.09.2016