УДК 004.04 DOI: 10.18698/2541-8009-2022-10-829

ГЕНЕРАТОР ПСЕДВОСЛУЧАЙНОЙ ПОСЛЕДОВАТЕЛЬНОСТИ КАСАМИ

Н.А. Аскерова nargizaskerova2013@yandex.ru
Т.Д. Соколов nomorepanica@gmail.com
А.А. Аскерова iselaskerova@yandex.ru

МГТУ им. Н.Э. Баумана, Москва, Российская Федерация

Аннотация

Рассмотрен синтез функциональной схемы генератора псевдослучайной последовательности Касами с описанием каждого блока. Выполнен подбор микросхем для построения генератора и подсчет временной задержки и мощности устройства. Разработан генератор псевдослучайной последовательности Касами по входным двоичным наборам. Приведены временные диаграммы работы генератора Касами, полученные при моделировании работы в Multisim. В результате моделирования устройства задержек не было обнаружено, однако в реальном устройстве появление задержек неизбежно. Поэтому в статье представлены вычисления теоретических задержек. Найден период последовательности Касами и доказана псевдослучайность сгенерированной последовательности, что подтверждает корректность работы устройства.

Ключевые слова

Псевдослучайная последовательность, Касами, генератор, микросхемы, диаграммы, регистр сдвига, псевдослучайность, Multisim, М-последовательность, автокорреляция

Поступила в редакцию 23.09.2022

Введение. Современное развитие систем цифровой передачи сообщений все в большей степени ориентируется на применение широкополосных методов передачи, основанных, в частности, на расширении спектра прямой последовательностью [1]. В таком случае каждый передаваемый бит информации представляется в виде последовательности, состоящей из определенного числа кодовых символов. Это реализуется сложением по модулю 2 исходной последовательности битов с кодовой расширяющей последовательностью. Каналы передачи имеют общую полосу частот, но разные кодирующие последовательности. Применение широкополосных сигналов обеспечивает увеличение показателя помехоустойчивости, снижение энергии передаваемых сигналов, повышение уровня скрытности самого процесса передачи информации по каналу с помехами. Наиболее часто для расширения спектра прямой последовательностью выбирают псевдослучайные последовательности Касами.

Примером простейшего алгоритма получения псевдослучайных последовательностей является М-последовательность. Однако она имеет не лучшие автокорреляционные свойства. Дальнейшее увеличение автокорреляционной функции

и достижение хороших взаимокорреляционных свойств между кодовыми последовательностями возможно путем комбинации нескольких М-последовательностей. На этом принципе и основаны схемы генерации кодов Касами.

В статье рассмотрен синтез функциональной схемы генератора псевдослучайной последовательности Касами (далее — ГПП Касами), выбор микросхем для построения ГПП Касами. Приведены временные диаграммы работы ГПП Касами, полученные при моделировании работы в Multisim.

Алгоритм получения последовательности Касами. Псевдослучайная последовательность Касами является примером линейных рекуррентных последовательностей (ЛРП) [2]. Ансамбль малого множества последовательностей Касами содержит все последовательности периода $2^n - 1$ с порождающим полиномом $K_S = h_1(x) \cdot h_2(x)$.

Последовательность Касами реализуется с помощью двух регистров сдвига (u, v) с различными обратными связями, каждый из которых формирует свою М-последовательность. Существует множество вариаций последовательности Касами. Для реализации был выбран алгоритм, изображенный на рис. 1. U и V — это две М-последовательности: одна длиной 8 бит (U), другая в 2 раза меньше — 4 бита (V).

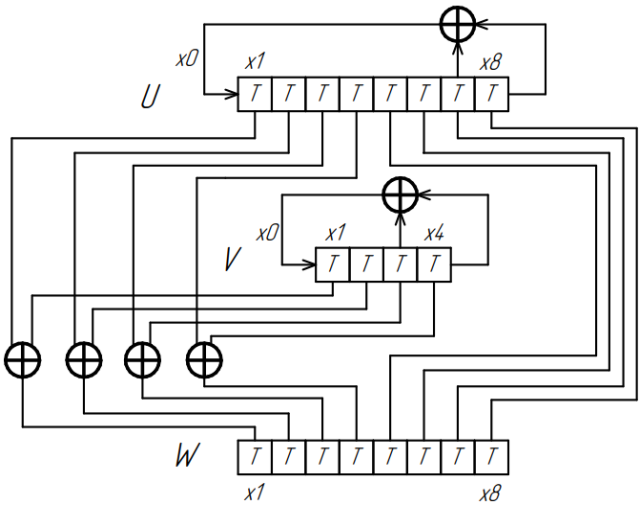

Рис. 1. Алгоритм генерации последовательности Касами
(T — значение (0 или 1) бита последовательности)

Полином первой М-последовательности $h_1(x) = x^8 + x^7 + 1$ имеет степень $n_1 = 8$, полином второй М-последовательности $h_2(x) = x^4 + x^3 + 1$ — степень $n_2 = n_1/2 = 4$. Тогда множество последовательностей Касами порождается полиномом $K_S = h_1(x) \cdot h_2(x) = x^{12} + x^{10} + x^8 + x^7 + x^4 + x^3 + 1$.

М-последовательности реализованы путем сдвига вправо, сложения по модулю двух младших бит и записи результата в старший бит. На каждом сдвиге четыре старших бита последовательности *U* складываются по модулю 2 с последовательностью *V* и результат заносится в последовательность Касами (*W*). Содержимое четырех младших битов последовательности *U* заносится в четыре младших бита *W* без изменений [1].

Фрагмент генерации последовательности Касами представлен в табл. 1. Знаком плюс обозначена сумма по модулю двух младший битов.

Таблица 1

Генерация последовательности Касами

U								+	*V*				+	*W*							
1	0	0	1	0	1	1	1	0	1	0	0	0	0	0	0	0	1	0	1	1	1
0	1	0	0	1	0	1	1	0	0	1	0	0	0	0	0	0	0	1	0	1	1
0	0	1	0	0	1	0	1	1	0	0	1	0	1	0	0	0	0	0	1	0	1
1	0	0	1	0	0	1	0	1	1	0	0	1	1	0	0	0	0	0	0	1	0
1	1	0	0	1	0	0	1	1	1	1	0	0	0	0	0	0	0	1	0	0	1
1	1	1	0	0	1	0	0	0	0	1	1	0	1	1	0	0	0	0	1	0	0
0	1	1	1	0	0	1	0	1	1	0	1	1	0	1	1	0	0	0	0	1	0

Стоит обратить внимание, что существует требование для первоначальной входной последовательности: в векторе, в котором перечислены коэффициенты многочлена в порядке убывания степеней, первая и последняя записи должны быть равны [3].

Для рассмотрения корреляционных свойств последовательности семейства Касами было решено разработать модуль вычисления автокорреляционной функции (АКФ), т. е. зависимость взаимосвязи между функцией (сигналом) и ее сдвинутой копией от величины временного сдвига.

Последовательность Касами является периодической. Ее период равен $2^m - 1$. Данная последовательность имеет дискретную структуру.

Автокорреляционная функция такого сигнала определяется по формуле

$$R(n) = \sum_{k=-\infty}^{\infty} a_k a_{k-n},$$

где n — целочисленный аргумент, указывающий, на сколько позиций сдвинута копия сигнала относительно оригинала.

Автокорреляционная функция, являясь в данном случае функцией целочисленного аргумента, обладает всеми свойствами обычной автокорреляционной функции. Это четная функция, поэтому $R(n) = R(-n)$. При нулевом сдвиге дискретная АКФ принимает максимальное значение.

Функциональная схема генератора последовательности Касами. Были определены функции устройства и реализующие их блоки — блок формирования начальных последовательностей (БФНП), блок реализации М-последовательностей (БРМП), блок формирования (БФПК) и вывода последовательности Касами (БВПК), блок формирования начальной последовательности Касами и её сдвинутых копий для вычисления АКФ (БФНПКиСК), блок подсчета (БП) и блок индикации (БИ).

Разработанная функциональная схема ГПП Касами представлена на рис. 2.

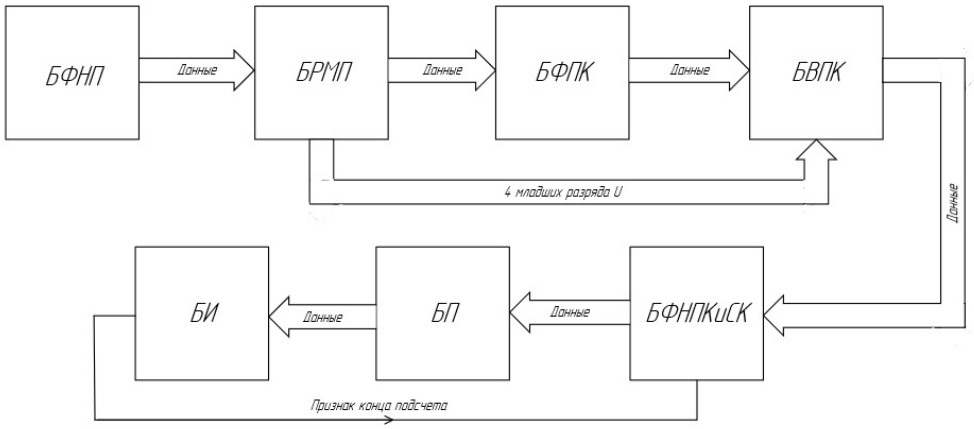

Рис. 2. Функциональная электрическая схема устройства

Блок формирования начальных последовательностей. Блок формирования начальных последовательностей обеспечивает ввод двоичных последовательностей. Их пользователь задает сам.

Блок содержит логические элементы «ИЛИ» 74ALS32M и генератор слов [4]. Он предназначен для генерации 32-разрядных двоичных слов и используется для отправки цифрового слова или битового шаблона в схему.

Блок реализации М-последовательностей. Блок реализации М-последовательностей состоит из двух сдвиговых регистров, хранящих последовательности длиной 8 бит и 4 бита.

Для реализации М-последовательности длиной 8 бит использовалось восемь D-триггеров 74ALS74N и один элемент XOR 74ALS86N для обеспечения принципа работы устройства (см. рис. 1). Для реализации М-последовательности длиной 4 бита использовалось четыре D-триггера и один элемент XOR [5].

Триггеры обеих последовательностей имеют входы синхронизации CLK. Все они подключены к одному генератору. Таким образом, сдвиги обеих последовательностей происходят одновременно по положительному фронту, что является необходимым для корректной работы устройства.

Блок формирования последовательности Касами. Блок формирования последовательности состоит из четырех элементов XOR 74ALS86N, которые и обеспечивают согласование последовательности Касами согласно принципу работы устройства (см. рис. 1) [4]. На вход каждого элемента поступает один бит из регистра последовательности и один бит из регистра последовательности *V*.

Блок вывода последовательности Касами. Для вывода последовательности Касами 4 измененных бита с выходов элементов XOR из блока формирования последовательности Касами и младшие четыре бита регистра последовательности *U* из блока реализации М-последовательностей поступают в блок вывода последовательности Касами. Данный блок состоит из двух логических анализаторов для вывода значений последовательностей *U* и *V*, а также для вывода результирующей последовательности Касами.

Блок формирования начальной последовательности Касами и ее сдвинутых копий. Блок формирования начальной последовательности Касами и ее сдвинутых копий состоит из двух четырехразрядных регистров сдвига 74LS194D. Они получают на вход двоичную последовательность из блока формирования и вывода последовательности Касами, и выводят ее сдвинутую копию. Сдвиг происходит синхронно с перепадом напряжения тактового по положительному фронту. После этого начальная последовательность Касами и ее сдвинутая копия поступают в следующий блок — блок подсчета.

Блок подсчета. На первом этапе блока подсчета начальная последовательность Касами побитово перемножается со сдвинутой последовательностью. Для этого использовано восемь элементов AND (логическое «И») 74ALS08M, по одному на каждый разряд [4].

Последовательность, полученная путем перемножения последовательности Касами и ее сдвинутой копии, поступает на следующий этап блока подсчета.

Для нахождения коэффициента корреляции необходимо подсчитать количество единиц в полученной на прошлом этапе последовательности. Данный этап содержит 15-разрядный регистр сдвига и счетчик 74LS192D. Младший бит этой последовательности поступает в счетчик. Регистр сдвига построен на 15 триггерах 74ALS74N. Такое число разрядов обусловлено необходимостью наличия перепада, поскольку счетчик последовательно увеличивается на единицу при положительном фронте на входе прямого счета тактовых импульсов Up. Каждый положительный фронт тактового импульса на входе обратного счета Down уменьшает показания счетчика. Чтобы избежать уменьшение числа в счетчике при положительном фронте на входе Down, решено использовать

элемент NOT 74ALS04BM (логическое отрицание). На каждой итерации последовательность сдвигается, и число, хранящееся в счетчике, суммируется с новым значением младшего бита последовательности произведений, а в освободившиеся разряды записываются нули [5].

Значения с выходов счетчика поступают в следующий блок — блок индикации.

Блок индикации. Для удобства решено выводить значения коэффициентов корреляции АКФ на 7-сегментный индикатор АЛС324Б [6]. На выходе предшествующего блока 4 двоичных сигнала в двоично-десятичном коде. С помощью преобразователя 74LS47D с четырьмя двоичными входами в двоично-десятичном коде и семью двоичными выходами в 7-сегментном коде осуществлен вывод на светодиодный индикатор [4].

После появления признака конца подсчета управление переходит на блок формирования начальной последовательности Касами и ее сдвинутых копий.

Моделирование работы устройства. Моделирование работы устройства проводилось в среде Multisim [7]. В результате были получены временные диаграммы работы ГПП Касами в начале и конце периода, представленные на рис. 3–8.

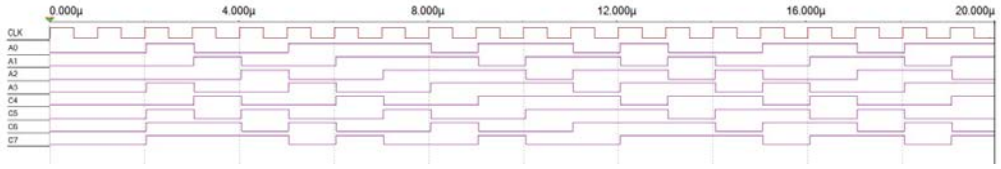

Рис. 3. Временная диаграмма М-последовательности *U* в начале периода

Рис. 4. Временная диаграмма М-последовательности *V* в начале периода

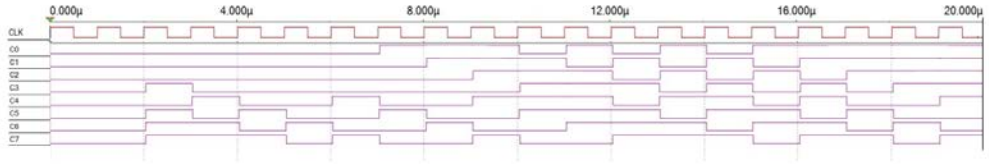

Рис. 5. Временная диаграмма последовательности Касами в начале периода

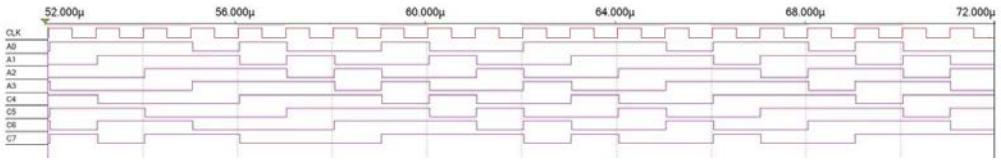

Рис.6. Временная диаграмма М-последовательности *U* в конце периода

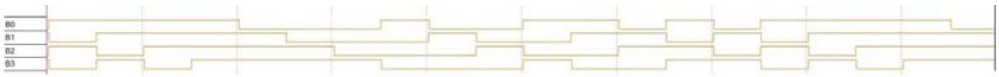

Рис.7. Временная диаграмма М-последовательности *V* в конце периода

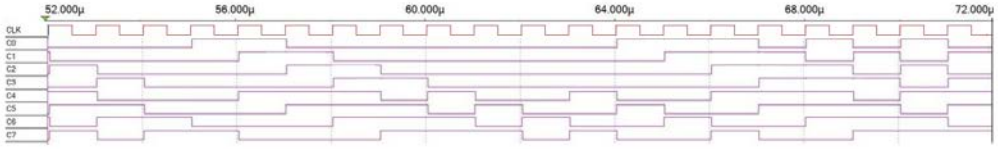

Рис. 8. Временная диаграмма последовательности Касами в конце периода

В результате моделирования устройства в среде Multisim задержек не было обнаружено. Однако в реальном устройстве появление задержек неизбежно. Далее для каждого элемента устройства подсчитаем теоретическую задержку согласно формуле $t_3 = rise\_delay + fall\_delay$ [8].

Рассчитаем мощность, потребляемую генератором последовательностей импульсов. На все МС подано напряжение 5 В. Суммарная мощность, потребляемая устройством, состоит из статической и динамической мощностей:

$$P_{\text{уст}} = \sum P_{\text{ст.микр}} + \sum P_{\text{дин.микр}}.$$

Статическую мощность каждой микросхемы находят по формуле

$$P_{\text{ст.микр}} = U_{CC} I_{CC}.$$

Таблица 2

Задержки и мощности элементов генератора последовательности Касами

Наименование микросхемы	Задержка, нс	Количество микросхем	Суммарная задержка, нс	Максимальная потребляемая статическая мощность, мВт	Суммарная потребляемая стат. мощность, мВт	Максимальная потребляемая динамическая мощность, мВт	Суммарная потребляемая дин. мощность, мВт
74ALS32M	2	3	6	0,15	0,45	4,25	12,75
74ALS74N	65	6	390	0,60	3,60	6,00	36,00
74ALS86N	2	2	4	0,15	0,30	5,00	10,00
∑	400 нс			4,35 мВт		58,75 мВт	

Для расчета потребляемой устройством мощности в динамическом режиме воспользуемся формулой

$$P_{\text{дин.микр}} = C_{\text{вн}} U_{\text{п}} f,$$

где $C_{\text{вн}}$ — внутренняя емкость ИМС (из документации); $U_{\text{п}}$ — напряжение питания; f — частота работы, f = 1 МГц [9].

Результаты вычислений представлены в табл. 2 и 3.

Таблица 3

Задержка и мощности элементов модуля подсчета АКФ

Наименование микросхемы	Задержка, нс	Количество микросхем	Суммарная задержка, нс	Максимальная потребляемая статическая мощность, мВт	Суммарная потребляемая стат. мощность, мВт	Максимальная потребляемая динамическая мощность, мВт	Суммарная потребляемая мощность, мВт
74ALS32M	2	2	4	0,15	0,30	4,25	8,50
74ALS74N	65	8	520	0,60	4,80	6,00	48,00
74LS194D	48	2	96	0,15	0,30	5,00	10,00
74ALS08M	2	2	4	0,50	1,00	0,50	1,00
74LS192D	50	1	50	0,15	0,15	0,50	0,50
74ALS04BM	2	1	2	0,50	0,50	0,50	0,50
74LS47D	200	1	200	0,15	0,15	0,50	0,50
АЛС324Б	0	1	0	0,90	0,90	125,00	10,00
∑	876 нс			8,10 мВт		79,00 мВт	

Проверка работы генератора последовательности Касами. Поскольку последовательность Касами является псевдослучайной с конечным числом внутренних состояний, то период последовательности заранее известен и составляет 2^n тактов, где n — длина последовательности.

Для генератора, рассматриваемого в данной статье, период последовательности Касами равен 256 тактам.

Чтобы оценить и проверить, соответствуют ли полученные при генерации последовательности свойству псевдослучайности, необходимо промоделировать его работу в конце периода, т. е. на 256-м такте.

Логический анализатор позволяет за один раз строить временную диаграмму лишь на 100 тактом, весь процесс симуляции был разделен на 3 этапа. Последовательности U и V, поэтому полученные на 100-м такте первых двух этапах симуляции, были внесены как начальные последовательности U и V. Работа устройства начинается со второго такта, таким образом устройство за один этап симуляции максимально проходит 99 тактов:

$$99 + 99 + (x - 1) = 256 \Rightarrow x = 59,$$

где x — число тактов на 3-м этапе.

Временные диаграммы М-последовательностей и последовательности Касами в конце периода представлены на рис. 4. Значения, полученные на 59-м такте, полностью соответствуют значениям на первом такте устройства. Таким образом, псевдослучайность последовательности Касами, полученной в результате работы устройства, доказана.

Литература

[1] Владимиров С.С., Когновицкий О.С. Малое множество последовательностей Касами и их декодирование на основе двойственного базиса. *Труды учебных заведений связи*, 2018, т. 4, № 1, с. 22–31.

[2] Султанов А.Я. Дополнительные вопросы алгебры. Рекуррентные последовательности. Пенза, ПГПУ им. В.Г. Белинского, 2011.

[3] Kasami Sequence Generator. URL: https://lost-contact.mit.edu/afs/inf.ed.ac.uk/group/teaching/matlab-help/R2015a/comm/ref/kasamisequencegenerator.html (дата обращения 2022-09-05).

[4] Нефедов А.П. Интегральные микросхемы и их зарубежные аналоги. Т. 11. Серии К1564 — К1814. М., РадиоСофт, 2001.

[5] Белоус А.И., Емельянов В.А., Турцевич А.С. Основы схемотехники микроэлектронных устройств. М., Техносфера, 2012.

[6] Индикаторы АЛС324А, АЛС324Б, АЛС324В. URL: https://radio-hobby.org/uploads/datasheets/als/als324.pdf (дата обращения: 11.09.2022).

[7] Марухина Т. Исследование логических схем с использованием программного комплекса Multisim. *pandia.ru: веб-сайт*. URL: https://pandia.ru/text/77/484/3439-3.php (дата обращения: 11.09.2022).

[8] Таблицы расчета времени задержек. *aspektcenter.ru: веб-сайт*. URL: https://aspektcenter.ru/tablitsy-rascheta-vremeni-zaderzhek/ (дата обращения: 11.09.2022).

[9] Сенегов П.Н. Электромеханические переходные процессы. Челябинск, ЧГТУ, 1996.

Аскерова Наргиз Агасафовна — бакалавр кафедры «Компьютерные системы и сети», МГТУ им. Н.Э. Баумана, Москва, Российская Федерация.

Соколов Тимофей Дмитриевич — бакалавр кафедры «Компьютерные системы и сети», МГТУ им. Н.Э. Баумана, Москва, Российская Федерация.

Аскерова Айсель Агасафовна — магистр кафедры «Высшая математика», МГТУ им. Н.Э. Баумана, Москва, Российская Федерация.

Научный руководитель — Ким Тамара Александровна, ассистент кафедры «Компьютерные системы и сети», МГТУ им. Н.Э. Баумана, Москва, Российская Федерация.

Ссылку на эту статью просим оформлять следующим образом:
Аскерова Н.А., Соколов Т.Д., Аскерова А.А. *Политехнический молодежный журнал*, 2022, № 10(75). http://dx.doi.org/10.18698/2541-8009-2022-10-829

KASAMI PSEUDORANDOM SEQUENCE GENERATOR

N.A. Askerova nargizaskerova2013@yandex.ru
T.D. Sokolov nomorepanica@gmail.com
A.A. Askerova iselaskerova@yandex.ru

Bauman Moscow State Technical University, Moscow, Russian Federation

Abstract

The synthesis of functional scheme of Kasami pseudorandom sequence generator with a description of each block is considered. Selection of microcircuits to build the generator and calculation of time delay and power of the device are performed. Kasami pseudorandom sequence generator is developed by input binary sets. The timing diagrams of the Kasami generator obtained by modeling the operation in Multisim are given. As a result of device simulation no delays have been detected, however, in a real device the appearance of delays is inevitable. Therefore, the paper presents the calculations of theoretical delays. The period of the Kasami sequence was found and the pseudorandomness of the generated sequence was proved, which confirms the device correctness.

Keywords

Pseudorandom sequence, Kasami, generator, microchips, diagrams, shift register, pseudorandomness, Multisim, M-sequence, autocorrelation

Received 23.09.2022

References

[1] Vladimirov S.S., Kognovitskiy O.S. The small set of Kasami sequences and their decoding based on the dual basis. *Trudy uchebnykh zavedeniy svyazi* [Proceedings of Telecommunication Universities], 2018, vol. 4, no. 1, pp. 22–31 (in Russ.).

[2] Sultanov A.Ya. Dopolnitelnye voprosy algebry. Rekurrentnye posledovatelnosti [Additional algebra questions. Recurring sequences]. Penza, PGPU im. V.G. Belinskogo Publ., 2011 (in Russ.).

[3] Kasami Sequence Generator. URL: https://lost-contact.mit.edu/afs/inf.ed.ac.uk/group/teaching/matlab-help/R2015a/comm/ref/kasamisequencegenerator.html (accessed: 2022-09-05).

[4] Nefedov A.P. Integralnye mikroskhemy i ikh zarubezhnye analogi. T. 11. Serii K1564 — K1814 [Integral microchips and their foreign analogs. Vol. 11. K1564 — K1814 series]. Moscow, RadioSoft Publ., 2001 (in Russ.).

[5] Belous A.I., Emelyanov V.A., Turtsevich A.S. Osnovy skhemotekhniki mikroelektronnykh ustroystv [Basics of microelectronic circuitry]. Moscow, Tekhnosfera Publ., 2012 (in Russ.).

[6] Indikatory ALS324A, ALS324B, ALS324V [ALS324A, ALS324B, ALS324V indicators] (in Russ.). URL: https://radio-hobby.org/uploads/datasheets/als/als324.pdf (accessed: 11.09.2022).

[7] Marukhina T. Issledovanie logicheskikh skhem s ispolzovaniem programmnogo kompleksa Multisim [Study on logic circuits using Multisim software]. *pandia.ru: website* (in Russ.). URL: https://pandia.ru/text/77/484/3439-3.php (accessed: 11.09.2022).

[8] Tablitsy rascheta vremeni zaderzhek. aspektcenter.ru: veb-sayt. URL: https://aspektcenter.ru/tablitsy-rascheta-vremeni-zaderzhek/ (accessed: 11.09.2022).
[9] Senegov P.N. Elektromekhanicheskie perekhodnye protsessy [Electromechanical transient processes]. Chelyabinsk, ChGTU Publ., 1996 (in Russ.).

Askerova N.A. — B.Sc. Student, Department of Computer Systems and Networks, Bauman Moscow State Technical University, Moscow, Russian Federation.

Sokolov T.D. — B.Sc. Student, Department of Computer Systems and Networks, Bauman Moscow State Technical University, Moscow, Russian Federation.

Askerova A.A. — M.Sc. Student, Department of Further Mathematics, Bauman Moscow State Technical University, Moscow, Russian Federation.

Scientific advisor — Kim T.A., Assis. Professor, Department of Computer Systems and Networks, Bauman Moscow State Technical University, Moscow, Russian Federation.

Please cite this article in English as:
Askerova N.A., Sokolov T.D., Askerova A.A. Kasami pseudorandom sequence generator. *Politekhnicheskiy molodezhnyy zhurnal* [Politechnical student journal], 2022, no. 10(75). http://dx.doi.org/10.18698/2541-8009-2022-10-829.html (in Russ.).