УДК 004.04 DOI: 10.18698/2541-8009-2022-02-771

МОДЕЛИРОВАНИЕ ПСЕВДОСЛУЧАЙНЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ

Т.Д. Соколов nomorepanica@gmail.com
SPIN-код: 2356-3320

Н.А. Аскерова nargizaskerova2013@yandex.ru
SPIN-код: 2284-2227

А.А. Аскерова nargizaskerova2013@yandex.ru
SPIN-код: 2284-2227

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

Аннотация

Выполнен обзор различных псевдослучайных последовательностей, таких как М-последовательность, коды Голда и коды Касами. Для каждого вида псевдослучайной последовательности представлены способы формирования, которые также описаны на примерах с помощью схем и математических вычислений. Выбраны предпочтительные пары для формирования последовательностей Голда и Касами. Рассмотрены свойства псевдослучайных последовательностей. Исследована автокорреляционная функция и дано ее математическое обоснование. На примере соотношения взаимной корреляции и длин последовательностей кодов исследованы автокорреляционные свойства последовательностей. Сформированы рекомендации по применению кодов с учетом их свойств.

Ключевые слова

Псевдослучайная последовательность М-последовательность, коды Касами, коды Голда, сигналы, взаимная корреляция кодов, автокорреляционная функция, сравнительный анализ, эффективность

Поступила в редакцию 28.01.2022

Введение. Для передачи данных применяют различные сигналы, представленные набором нулей и единиц. В некоторых случаях возникает необходимость в использовании сигналов, которые бы выглядели случайными, хотя на самом деле такими бы не являлись. Сигнал, состоящий из случайной последовательности нулей и единиц, является непредсказуемым, поэтому если информация будет передана таким сигналом, её попросту будет невозможно расшифровать. Для этого используются псевдослучайные сигналы, которые выглядят случайными и имеют статистические свойства белого шума, однако однозначно определяются передатчиком и приемником [1–3].

Системы, в которых используются такие последовательности, применяют уже более 50 лет. Известные их достоинства, такие как высокая помехозащищенность по отношению к узкополосным помехам большой мощности, возможность разделения абонентов по кодовому признаку, скрытность передачи, высокая устойчивость к многолучевому распространению и даже высокая разрешающая способность при радиолокационных и навигационных измерениях предопределили их использование в различных системах связи и определения местоположения.

Выбор псевдослучайной кодовой последовательности в радиотехнической системе передачи информации очень важен, поскольку от ее параметров зависит усиление обработки системы, ее помехоустойчивость и чувствительность. При одной и той же длине кодовой последовательности параметры системы могут быть различны.

Существует несколько типов псевдослучайных кодовых последовательностей: М-последовательности, коды Голда и Касами. В данной работе рассмотрен каждый вид псевдослучайных последовательностей с последующим сравнением корреляционных свойств.

М-последовательности. М-последовательность, или последовательность максимальной длины — это псевдослучайная двоичная последовательность, формируемая регистром сдвига с линейной обратной связью. М-последовательности широко применяют в радиотехнических системах [4–7].

М-последовательности являются периодическими с периодом $N = 2^n - 1$, где n — число регистров сдвига. М-последовательность также используется для формирования других видов псевдослучайных последовательностей.

Рассмотрим М-последовательности на следующем примере (рис. 1).

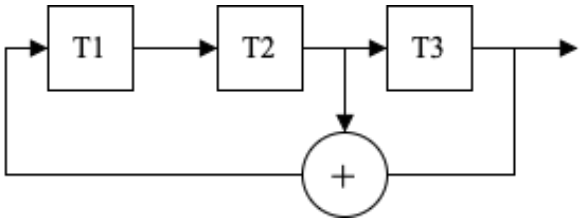

Рис. 1. Формирование М-последовательности

Допустим, что сдвигающий регистр на рис. 1 состоит из трех триггерных ячеек Т1, Т2 и Т3, которые играют роль дискретных элементов задержек. На триггеры поступают сдвигающие импульсы. Каждый тактовый импульс вызывает изменение состояния всех триггеров. При этом напряжение на выходе каждого триггера становится равным напряжению на его входе для предыдущего такта. Сигналы могут принимать два значения, которые условно обозначим 0 и 1. При суммировании любых комбинаций входных сигналов на выходе сумматора получаются только значения 0 и 1.

Таким образом, с помощью обратной линейной связи и суммированию по модулю 2 с двух выходов триггерных ячеек на выходе будет получена М-последовательность. При начальной комбинации 100 будут получены значения триггерных ячеек, отображенные в табл. 1.

Таким образом, в итоге будет получена периодическая последовательность …0111001011100101110… Данная последовательность обладает периодом $N = 7.$

Каждую псевдослучайную последовательность можно математически описать формирующим ее полиномом. Последовательность, которая была описана в примере выше, можно представить как $h(x) = x^3 + x^2 + 1.$

Таблица 1

Значения триггерных ячеек

Номер такта	Вход T_1	Выход		
		T_1	T_2	T_3
1	0	1	0	0
2	1	0	1	0
3	1	1	0	1
4	1	1	1	0
5	0	1	1	1
6	0	0	1	1
7	1	0	0	1
8	0	1	0	0
9	1	0	1	0

Последовательности Голда. Псевдослучайная последовательность Голда — это вид псевдослучайных последовательностей, характерная особенность которого — фиксируемый и контролируемый уровень корреляции между кодами [5, 7].

Именно коды Голда позволяют получить большой набор кодов одинаковой длины с хорошими взаимокорреляционными свойствами. Такая последовательность формируется с помощью суммирования по модулю 2 двух М-последовательностей одинаковой длины. Вместе они формируют последовательность Голда, которая имеет такую же длину, как и исходные М-последовательности. Пара М-последовательностей, имеющих одинаковый период *N*, может быть связана соотношением $a' = a\lfloor q \rfloor$ для некоторого *q*. При этом М-последовательности *a* и a' называют предпочтительной парой при совместном выполнении следующих условий:

– *n* нечетное, или $n = 2(\mathrm{mod}\,4)$;

– наибольший общий делитель для *n* и *k* равен одному для нечетных *n* и равен двум для $n = 2(\mathrm{mod}\,4)$, где *n* —период последовательности, а *k* — какое-то *q* из a' [7].

Предпочтительные пары М-последовательностей для генерации кодов Голда, соответствующие перечисленным выше условиям, приведены в табл. 2.

Таблица 2

Предпочтительные пары для формирования последовательностей Голда

n	Длина кода	Пары М-последовательностей
5	31	[5,2][5,4,3,2]
6	63	[6,1][6,5,2,1]
7	127	[7,3,2,1][7,5,4,3,2,1]
8	255	[8,7,6,5,2,1][8,7,6,1]
9	511	[9,4][9,6,4,3][9,6,4,3][9,8,4,1]
10	1023	[10,9,8,7,6,5,4,3][10,9,7,6,4,1][10,8,7,6,5,4,3,1][10,9,7,6,4,1][10,8,5,1][10,7,6,4,2,1]
11	2047	[11,2][11,8,5,2][11,8,5,2][11,10,3,2]

Далее последовательности Голда будут рассмотрены на примере. Формирование последовательности Голда изображено на рис. 2.

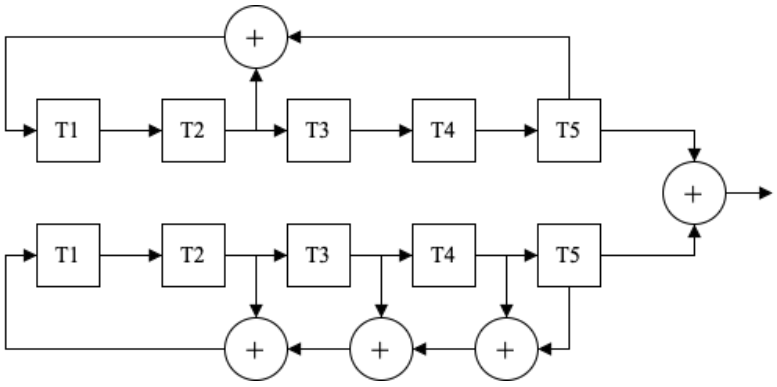

Рис. 2. Формирование последовательности Голда

Существуют две М-последовательности, которые являются предпочтительными парами и образуются следующими полиномами: $h_u(x) = x^5 + x^2 + 1$ и $h_v(x) = x^5 + x^4 + x^3 + x^2 + 1.$ Для того чтобы сформировать из них последовательность Голда, необходимо посимвольно суммировать эти последовательности по модулю 2. В данном случае на выходе будет получена последовательность Голда, имеющая период $N = 31,$ поскольку такой же период имели исходные М-последовательности.

Например, М-последовательности 11111000110111010100000100101100 и 11111001001100001011010100001110 после посимвольного суммирования образовывают следующую последовательность Голда: 10000100010001010001100011010 11. Данная последовательность определяется полиномом $G(u,v) = h_u(x) \cdot h_v(x) =$
$= (x^5 + x^2 + 1) \cdot (x^5 + x^4 + x^3 + x^2 + 1) = x^{10} + x^9 + x^8 + x^6 + x^5 + x^3 + 1.$

Последовательности Кассами. Последовательность Касами также формируется с помощью М-последовательности и представляет собой двоичную последовательность длиной $N = 2^n - 1,$ где *n* — четное целое число, которое отображает количество разрядов. Семейства последовательностей Касами известны благодаря их хорошим корреляционным свойствам. Различают малое множество последовательностей Касами и большое множество [5, 6].

Пусть *n* четно, $p = 2^{m/2} + 1,$ $h_1(x)$ — примитивный двоичный полином степени $n,$ порождающий М-последовательность, а $h_2(x)$ — примитивный двоичный полином степени *n*/2, корнями которого являются *p*-степени корней полинома $h_1(x).$ Ансамбль малого множества последовательностей Касами содержит все последовательности периода $2^n - 1$ с порождающим полиномом $h(x) = h_1(x) \cdot h_2(x).$

Пусть $t = 1 + 2^{(n+2)/2}$ — целое число, такое, что НОД $(t, 2_n - 1) = 3.$ Пусть $h_1(x)$ — примитивный двоичный полином степени *n*, $h_2(x)$ — примитивный

двоичный полином степени $n/2$, корнями которого являются p — степени корней полинома $h_1(x)$, $h_3(x)$ — полином степени n, корнями которого являются t — степени корней полинома $h_1(x)$. Ансамбль большого множества последовательностей Касами содержит все последовательности периода $2^n - 1$ с порождающим полиномом $h(x) = h_1(x) \cdot h_2(x) \cdot h_3(x)$.

Рассмотрим последовательности Касами на примере малого множества последовательностей Касами. Формирование последовательности изображено на рис. 3.

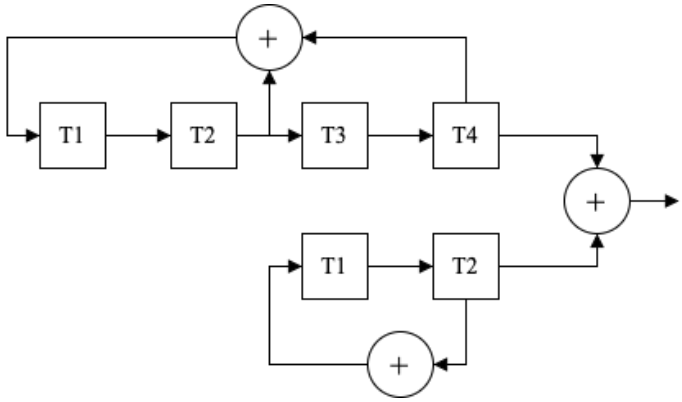

Рис. 3. Формирование последовательности Касами

Построим ансамбль Касами длиной $N = 2^4 - 1 (h = 2, K = \sqrt{N+1} = 4)$. Начнем с бинарной $\{0, 1\}$ m-последовательности $\{u_i^t\}$ длиной $N = 2^4 - 1 = 15$ на основе примитивного полинома $f(x) = x^4 + x + 1$ с начальным состоянием $u_0^t = 1, u_1^t = u_2^t = u_3^t = 0$. Имеем $\{u_i^t\} = \{1,0,0,0,1,0,0,1,1,0,1,0,1,1,1\}$. Децимация этой последовательности с индексом $d = 2^h + 1 = 5$ дает m-последовательность периода три $\{v_i\} = \{1,0,1,1,0,1,1,0,1,1,0,1,1,0,1\}$. Сумма по модулю 2 последовательности $\{u_i^t\}$ с тремя сдвинутыми копиями $\{v_i^t\}$ после перехода к алфавиту $\{\pm 1\}$ образует первые три сигнатуры Касами:

$$\{a_{1,i}\} = \{+ + - - - - - - + - - - + - +\};$$

$$\{a_{2,i}\} = \{+ - + - + + + - + - - + + + + -\};$$

$$\{a_{3,i}\} = \{- - - + + - + + + + + - - + +\}.$$

Данная последовательность определяется полиномом: $G(u,v) = h_u(x) \cdot h_v(x)$ $= (x^4 + x + 1) \cdot (x^2 + 1) = (x^6 + x^4 + x^3 + x^2 + x + 1)$.

Свойства псевдослучайных последовательностей. Псевдослучайные последовательности обладают следующими свойствами.

1. Выходные последовательности зависят от длины сдвиговых регистров, первоначального состояния и логики обратной связи.

2. Псевдослучайные последовательности проходят все состояния, кроме состояний всех нулей (также это не может быть первоначальным состоянием).

3. Свойство баланса: в каждом состоянии псевдослучайной последовательности количество единиц всегда больше, чем нулей.

4. Любая псевдослучайная последовательность содержит 2^{n-1} единиц, $2^{n-1}-1$ нулей.

5. В каждом состоянии псевдослучайной последовательности количество возможных групп находится по следующей формуле:

$$\text{groups} = \left[\frac{\text{length}+1}{2}\right].$$

где groups — количество возможных групп, а length —длина псевдослучайной последовательности. Отметим, что деление, в данном случае осуществляется с выделением целой части (без округления).

Данные свойства основываются на постулатах Голомба [4].

Автокорреляционные функции псевдослучайных последовательностей. Перед тем как изучить корреляционные свойства псевдослучайных последовательностей необходимо выяснить, что такое корреляционные свойства. Понять эти свойства и сравнить их позволяет автокорреляционная функция (АКФ), которая представляет собой зависимость взаимосвязи между сигналом и его сдвинутой копией во времени. Автокорреляционная функция псевдослучайной последовательности определяется по формуле

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

где n — количество позиций, на которое сдвинута копия сигнала относительно оригинала, а a_k и a_{k-n} — сигнал и его сдвинутая копия сигнала соответственно [5].

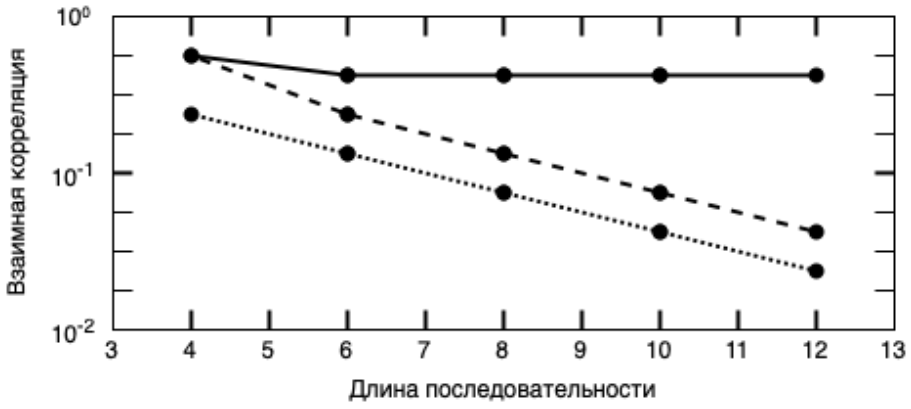

Рис. 4. Взаимная корреляция кодов различных псевдослучайных последовательностей:
М-последовательности; коды Голда; коды Касами

Взаимная корреляция кодов различных псевдослучайных последовательностей изображена на рис. 4. По графикам можно сделать вывод, что наилучшими корреляционными свойствами обладают именно псевдослучайные последовательности Касами, поскольку при увеличении длины псевдослучайной последовательности количество совпадений между сигналом и его сдвинутой копией во времени стабильно уменьшается. Несмотря на то что коды Голда демонстрируют такую же тенденцию, коды Касами все равно показывают лучший результат, когда как взаимная корреляция М-последовательностей просто в определенный момент начинает оставаться на одном уровне, то есть при увеличении длины последовательности уровень взаимной корреляции остается прежним [5, 8, 9].

Вывод. На основе рассмотренных видов псевдослучайных последовательностей можно сделать вывод, что при выборе наиболее оптимальной для использования псевдослучайной последовательности нужно обратить внимание на корреляционные свойства. Если стоит необходимость в наиболее лучших из возможных взаимокорреляционных свойств, то стоит остановить выбор на последовательностях Касами. В свою очередь, коды Голда подойдут в случае, если нужно контролировать уровень корреляции. М-последовательности подойдут только для формирования остальных псевдослучайных последовательностей с более хорошими корреляционными свойствами или в случаях, когда эти свойства не имеют значения.

Литература

[1] Псевдослучайные последовательности. *siblec.ru: веб-сайт*. URL: https://siblec.ru/telekommunikatsii/ teoreticheskie-osnovy-tsifrovoj-svyazi/12-metody-rasshirennogo-spektra/12-2-psevdosluchajnye-posledovatelnosti (дата обращения: 10.12.2021).

[2] Псевдослучайные последовательности и их свойства. *studfile.net: веб-сайт*. URL: https://studfile.net/preview/9478149/page:17/ (дата обращения: 10.12.2021).

[3] Sadiq K.G. Performance comparison of various short codes in direct sequence spread spectrum (DS/SS) system. *J. Techniques*, 2011, vol. 24, no. 8, pp. E154–E167.

[4] Варакин Л.Е. Системы связи с шумоподобными сигналами. М., Радио и связь, 1985.

[5] Прозоров Д.Е., Смирнов А.В., Баланов М.Ю. Алгоритм быстрой кодовой синхронизации шумоподобных сигналов, построенных на последовательностях повышенной структурной сложности. *Вестник РГРТУ*, 2015, № 51, с. 3–8. (in Russ.).

[6] Оптимальные и асимптотически оптимальные ансамбли дискретных сигнатур. *siblec.ru: веб-сайт*. URL: https://siblec.ru/telekommunikatsii/shirokopolosnye-signaly-i-sistemy/12-optimalnye-i-asimptoticheski-optimalnye-ansambli-diskretnykh-signatur#12.3 (дата обращения: 10.12.2021).

[7] Последовательности Голда. *crypto.pp.ua: веб-сайт*. URL: http://crypto.pp.ua/2011/12/posledovatelnosti-golda-chast-1/ (дата обращения: 10.12.2021).

[8] Autocorrelation and cross-correlation for two half-cycle Wischmeyer sweeps generated using Kasami sequences. *researchgate.net: веб-сайт*. URL: https://www.researchgate.net/figure/Autocorrelation-grey-only-the-peak-value-is-visible-and-cross-correlation-black-for_fig6_259544211 (дата обращения: 10.12.2021).

[9] Autocorrelation Function of PN sequence generated. *researchgate.net: веб-сайт*. URL: https://www.researchgate.net/figure/Autocorrelation-Function-of-PN-sequence-generated_fig2_ 263464034 (дата обращения: 10.12.2021).

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

Аскерова Наргиз Агасафовна — 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:
Соколов Т.Д., Аскерова Н.А., Аскерова А.А. Моделирование псевдослучайных последовательностей. *Политехнический молодежный журнал*, 2022, № 02(67). http://dx.doi.org/10.18698/2541-8009-2022-02-771

MODELING PSEUDO-RANDOM SEQUENCES

T.D. Sokolov nomorepanica@gmail.com
SPIN-code: 2356-3320

N.A. Askerova nargizaskerova2013@yandex.ru
SPIN-code: 2284-2227

A.A. Askerova nargizaskerova2013@yandex.ru
SPIN-code: 2284-2227

Bauman Moscow State Technical University, Moscow, Russian Federation

Abstract

The paper presents a review of various pseudo-random sequences, such as the M-sequence, Gold codes and Kasami codes. For each type of pseudo-random sequence, methods of formation are presented, which are also described in examples using diagrams and mathematical calculations. Preferred pairs for the formation of Gold and Kasami sequences have been selected. The properties of pseudo-random sequences are considered. The autocorrelation function is investigated and its mathematical substantiation is given. The autocorrelation properties of the sequences have been studied using the example of the ratio of cross-correlation and lengths of code sequences. Recommendations on the use of codes are formed, taking into account their properties.

Keywords

Pseudo-random sequence M-sequence, Kasami codes, Gold codes, signals, cross-correlation of codes, autocorrelation function, comparative analysis, efficiency

Received 28.01.2022

References

[1] Psevdosluchaynye posledovatel'nosti [Pseudorandom sequences]. *siblec.ru: website* (in Russ.). URL: https://siblec.ru/telekommunikatsii/teoreticheskie-osnovy-tsifrovoj-svyazi/12-metody-rasshirennogo-spektra/12-2-psevdosluchajnye-posledovatelnosti (accessed: 10.12.2021).

[2] Psevdosluchaynye posledovatel'nosti i ikh svoystva [Pseudorandom sequences and their properties]. *studfile.net: website* (in Russ.). URL: https://studfile.net/preview/9478149/page:17/ (accessed: 10.12.2021).

[3] Sadiq K.G. Performance comparison of various short codes in direct sequence spread spectrum (DS/SS) system. *J. Techniques*, 2011, vol. 24, no. 8, pp. E154–E167.

[4] Varakin L.E. Sistemy svyazi s shumopodobnymi signalami [Communication system noise-type signal]. Moscow, Radio i svyaz' Publ., 1985 (in Russ.).

[5] Prozorov D.E., Smirnov A.V., Balanov M.Yu. Fast code synchronization algorithm of spread spectrum signals based on sequences with high structural complexity. *Vestnik RGRTU* [Vestnik of Ryazan State Radio Engineering University], 2015, no. 51, pp. 3–8 (in Russ.).

[6] Optimal'nye i asimptoticheski optimal'nye ansambli diskretnykh signatur [Optimum and asymptotically optimal signature ensemble]. *siblec.ru: website* (in Russ.). URL: https://siblec.ru/ telekommunikatsii/shirokopolosnye-signaly-i-sistemy/12-optimalnye-i-asimptoticheski-optimalnye-ansambli-diskretnykh-signatur#12.3 (accessed: 10.12.2021).

[7] Posledovatel'nosti Golda [Gold sequences]. *crypto.pp.ua: website* (in Russ.). URL: http://crypto.pp.ua/2011/12/posledovatelnosti-golda-chast-1/ (accessed: 10.12.2021).

[8] Autocorrelation and cross-correlation for two half-cycle Wischmeyer sweeps generated using Kasami sequences. *researchgate.net: website*. URL: https://www.researchgate.net/figure/ Auto-correlation-grey-only-the-peak-value-is-visible-and-cross-correlation-black-for_fig6_259544211 (accessed: 10.12.2021).

[9] Autocorrelation Function of PN sequence generated. *researchgate.net: website*. URL: https://www.researchgate.net/figure/Autocorrelation-Function-of-PN-sequence-generated_fig2_263464034 (accessed: 10.12.2021).

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

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

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

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

Please cite this article in English as:
Sokolov T.D., Askerova N.A., Askerova A.A. Modeling pseudo-random sequences. *Politekhnicheskiy molodezhnyy zhurnal* [Politechnical student journal], 2022, no. 02(38). http://dx.doi.org/ 10.18698/ 2541-8009-2022-02-522.html (in Russ.).