«Математика»

Научная статья
УДК 519.6: 532.5
DOI: 10.17072/1993-0550-2023-3-5-12

Применение формул прогонки для шифрования текстовых данных

Н.К. Волосова[1], К.А. Волосов[2], А.К. Волосова[2], М.И. Карлов[3], Д.Ф. Пастухов[4], Ю.Ф. Пастухов[4]

[1]Московский государственный технический университет (МГТУ) им. Н.Э. Баумана, Москва, Россия
[2] Российский университет транспорта (МИИТ), Москва, Россия
[3]Московский физико-технический университет (МФТИ), Москва, Россия
[4]Полоцкий государственный университет, Новополоцк, Республика Беларусь

Автор, ответственный за переписку: Дмитрий Феликсович Пастухов, dmitrij.pastuhov@mail.ru

Аннотация. В работе впервые рассматривается возможность применения формул трехдиагональной прогонки для шифрования текстовых данных. Алгоритм шифрования заключается в вычислении правой части системы линейных алгебраических уравнений с трехдиагональной матрицей. В задаче все коэффициенты уравнений, правая часть и решение принимают значения остатков по модулю простого числа *p*. Алгоритм дешифрования заключается в решении СЛАУ на классе вычетов простого модуля *p*. Алгоритм дешифрования использует метод трехдиагональной прогонки. Доказаны две теоремы для корректности алгоритма. Теорема 2 – достаточные условия корректности. Теорема 3 – необходимые условия корректности. Приведены три примера шифрования текста из 65, 67 символов, хорошо иллюстрирующие условия применимости теорем. Оценена мощность пространства ключей.

Ключевые слова: *численные методы; метод прогонки; системы линейных алгебраических уравнений; шифрование; теория чисел*

Для цитирования: *Волосова Н.К., Волосов К.А., Волосова А.К., Карлов М.И., Пастухов Д.Ф., Пастухов Ю.Ф.* Применение формул прогонки для шифрования текстовых данных // Вестник Пермского университета. Математика. Механика. Информатика. 2023. Вып. 3(62). С. 5–12. DOI: 10.17072/1993-0550-2023-3-5-12.

Статья поступила в редакцию 02.08.2023; одобрена после рецензирования 16.08.2023; принята к публикации 15.09.2023.

«Mathematics»

Research article

Sweep Formulas Applying to Encrypt Text Data

N.K. Volosova[1], K.A. Volosov[2], A.K. Volosova[2], M.I. Karlov[3], D.F. Pastuhov[4], Yu.F. Pastuhov[4]

[1]Bauman Moscow State Technical University (BMSTU), Moscow, Russia
[2]Russian University of Transport (RUT MIIT), Moscow, Russia
[3]Moscow University of Physics and Technology (MIPT), Moscow, Russia
[4]Polotsk State University, Novopolotsk, Republic of Belarus

Corresponding author: Dmitriy F. Pastukhov, dmitrij.pastuhov@mail.ru

Эта работа © 2023 Волосова Н.К., Волосов К.А., Волосова А.К., Карлов М.И., Пастухов Д.Ф., Пастухов Ю.Ф. под лицензией CC BY 4.0. Чтобы просмотреть копию этой лицензии, посетите http://creativecommons.org/licenses/by/4.0/

Abstract. In this paper we consider for the first time the possibility of applying the tridiagonal run-through formulas for text data encryption. The encryption algorithm consists in computing the right part of a linear algebraic equations system with a tridiagonal matrix. In the problem, all the equations coefficients, the right-hand side and the solution take the values of the residues modulo a prime number *p*. The decryption algorithm consists in solving the SLAE on the class of prime modulo *p* deductions. The decryption algorithm uses the tridiagonal run method. Two theorems are proved for the algorithm correctness. Theorem 2 is a sufficient condition for correctness. Theorem 3 is the necessary conditions for correctness. Three encryptions of the text of 65, 67 symbols examples are given for illustrate the theorems applicability conditions. The keys spatial power is estimated.

Keywords: *numerical methods; sweep method; system of linear algebraic properties; encryption; number theory*

For citation: *Volosova N.K., Volosov K.A., Volosova A.K., Karlov M.I., Pastuhov D.F., Pastuhov Yu.F.* Sweep Formulas Applying to Encrypt Text Data. Bulletin of Perm University. Mathematics. Mechanics. Computer Science. 2023;3(62):5-12. (In Russ.). DOI: 10.17072/1993-0550-2023-3-5-12.

The article was submitted 02.08.2023; approved after reviewing 16.08.2023; accepted for publication 15.09.2023.

Введение

Формулы прогонки с трехдиагональной матрицей в разностных уравнениях наиболее известны в Численных методах [1], [2]. Метод прогонки (трехдиагональный матричный алгоритм) используется в задаче аппроксимации достаточно гладких функций кубическими сплайнами; для решения краевой задачи с обыкновенным дифференциальным уравнением второго порядка и выше; в краевой задаче Дирихле с уравнением в частных производных эллиптического типа (уравнение Пуассона [1]).

В данной работе впервые используется метод трехдиагональной прогонки для шифрования и дешифрования текстовых данных в классах вычетов по простому модулю. В последнее время все более сложные математические методы используются для шифрования текстовой и графической информации. Например, в работах [6], [7], [8], [9], [10], [11], [12], [13], [14], [15].

Постановка задачи

Рассмотрим систему рекуррентных уравнений для решения СЛАУ с трехдиагональной матрицей. Запишем эту систему уравнений в виде [1, стр. 585], предложенном авторами известного учебника Численные методы Н.С. Бахвалов, Н.П. Жидков, Г.М. Кобельков для решения краевой задачи Дирихле для уравнения Пуассона [1]:

$$\begin{cases} -b_0 x_0 + c_0 x_1 = f_1, & k = 0 \\ a_k x_{k-1} - b_k x_k + c_k x_{k+1} = f_k, & k = \overline{1, n-1} \\ a_n x_{n-1} - b_n x_n = f_n, & k = n \end{cases} . \quad (1)$$

Если в задаче (1) коэффициенты, правые части и неизвестные $a_k, b_k, c_k, f_k, x_k \in R, k = \overline{0,n}$ являются действительными числами, то решение системы уравнений (1) известно: [1], [2]

$$x_k = \lambda_k x_{k+1} + \nu_k, \ \ k = \overline{0, n-1} \ . \quad (2)$$

Коэффициенты прогонки с индексом k=0 вычисляем по формуле (3) [1]:

$$x_0 = \frac{c_0 x_1 - f_1}{b_0} \Leftrightarrow \lambda_0 = \frac{c_0}{b_0}, \nu_0 = \frac{-f_1}{b_0} \ . \quad (3)$$

В формуле (2) коэффициенты прогонки вперед [1] имеют вид

$$\lambda_k = \frac{-c_k}{(a_k \lambda_{k-1} - b_k)}, \nu_k = \frac{f_k - a_k \nu_{k-1}}{(a_k \lambda_{k-1} - b_k)}, k = \overline{1, n-1} \ . \quad (4)$$

Наконец, значение переменной x_n на правом конце находим по формуле (5) [1]:

$$x_n = \frac{f_n - a_n \nu_{n-1}}{a_n \lambda_{n-1} - b_n} . \quad (5)$$

Зная x_n, коэффициенты $\lambda_k, \nu_k, k = \overline{0, n-1}$, вычисляем остальные неизвестные по обратному циклу с понижением индекса по формуле (6) [1]:

$$x_k = \lambda_k x_{k+1} + \nu_k, \ \ k = \overline{n-1, 0} . \quad (6)$$

В литературе [1], [2] формулы (3), (4) называют *формулами прогонки вперед*, а формулы (5), (6) *формулами прогонки назад.*

Рассмотрим решение задачи (1) на множестве целочисленных остатков

$$a_k, b_k, c_k, f_k, x_k \in \{1, 2, ..., p-1\} (\mathrm{mod}\ p), k = \overline{0, n}$$

по модулю простого числа *p*

$$\begin{cases} -b_0x_0 + c_0x_1 \equiv f_1 \pmod p, & k=0 \\ a_kx_{k-1} - b_kx_k + c_kx_{k+1} \equiv f_k \pmod p \\ a_nx_{n-1} - b_nx_n \equiv f_n \pmod p, & k=n \\ a_k, b_k, c_k, f_k, x_k \equiv \{0,1,2,..., p-1\} \end{cases}, \quad k = \overline{1, n-1}. \quad (7)$$

Необходимость выбора простого числа p в задаче (7) связано со свойствами делимости целых чисел [3], [4].

Пусть[3] числа $a, x, m \in Z$ целые, тогда справедлива

Теорема 1 [3, стр.19]. Для того чтобы сравнение $ax \equiv 1 (\mathrm{mod}\, m)$ имело решение, необходимо и достаточно, чтобы а было взаимно просто с m.

Следствие 1. Каждый примитивный класс вычетов а($НОД(a,m)=1$) по $(\mathrm{mod}\, m)$ имеет ровно один обратный класс х: $ax \equiv 1 (\mathrm{mod}\, m)$ [3, стр. 19].

Следствие 2. Пусть $m = p$ – простое число. Тогда для любого целого остатка числа р $a \equiv \{1,2,..., m-1\} (\mathrm{mod}\, p)$ существует единственный остаток – решение уравнения $ax \equiv 1 (\mathrm{mod}\, p)$.

Доказательство. Так как каждый остаток $a \equiv \{1,2,..., p-1\} (\mathrm{mod}\, p)$ взаимно прост с простым числом p, то есть принадлежит примитивному классу вычетов, то по **Теореме 1** решение x сравнения $ax \equiv 1 (\mathrm{mod}\, p)$ существует, а по Следствию 1 класс, которому принадлежит число х, единственный (возможно и совпадение классов, например, для остатков $a \equiv x \equiv 1 (\mathrm{mod}\, p) : 1 \cdot 1 = 1 \equiv 1 (\mathrm{mod}\, p)$). Следствие 2 из **Теоремы 1** доказано.

Теперь формулы прогонки вперед аналогично (3), (4) перепишем в виде

$$\lambda_0 \equiv c_0 b_0^{-1} (\mathrm{mod}\, p), \nu_0 \equiv -f_1 b_0^{-1} (\mathrm{mod}\, p), \quad (8)$$

$$\begin{cases} \lambda_k \equiv -c_k (a_k \lambda_{k-1} - b_k)^{-1} (\mathrm{mod}\, p), \\ \nu_k \equiv (f_k - a_k \nu_{k-1})(a_k \lambda_{k-1} - b_k)^{-1} (\mathrm{mod}\, p), k = \overline{1, n-1} \end{cases}. \quad (9)$$

А формулы прогонки назад из формул (5), (6) примут вид

$$x_n \equiv (f_n - a_n \nu_{n-1})(a_n \lambda_{n-1} - b_n)^{-1} (\mathrm{mod}\, p), \quad (10)$$

$$x_{k-1} \equiv \lambda_{k-1} x_k + \nu_{k-1} (\mathrm{mod}\, p), k = \overline{n-1, 0}. \quad (11)$$

Сформулируем достаточные условия разрешимости задачи (7) и корректности алгоритма (8)–(11) в виде **Теоремы 2.**

Теорема 2 (достаточные условия корректности алгоритма (8)–(11)).

Пусть в задаче (7), алгоритме (8)–(11) выполнены условия на коэффициенты:

1) $b_0 \equiv c_0 (\mathrm{mod}\, p), c_0 \in \{1,2,..., p-1\}$;

2) $b_k \equiv a_k + c_k (\mathrm{mod}\, p), c_k \in \{1,2,..., p-1\}, k = \overline{1, n}$;

диагональный элемент матрицы коэффициентов системы (7) сравним с суммой недиагональных элементов строки по (mod p).

Тогда:

1. $\lambda_k \equiv 1 (\mathrm{mod}\, p), k = \overline{0, n-1}$.

2. Задача (7) имеет единственное решение в классах вычетов по простому модулю р, а алгоритм (8)–(11) корректен.

Доказательство Теоремы 2 проведем по индукции.

1. a) База индукции $k = 0$. Так как по условию 1) Теоремы 1 $c_0 \equiv b_0 (\mathrm{mod}\, p)$ число λ_0 в формуле (8)

$$\lambda_0 \equiv c_0 b_0^{-1} (\mathrm{mod}\, p) \equiv c_0 c_0^{-1} (\mathrm{mod}\, p) \equiv 1 (\mathrm{mod}\, p).$$

b) Индуктивный переход. Пусть $\lambda_k \equiv 1 (\mathrm{mod}\, p), k = \overline{1, s-1}$. Тогда в первой формуле (9) с учетом условия 2) Теоремы 2

$$b_k \equiv a_k + c_k (\mathrm{mod}\, p) \Leftrightarrow c_k \equiv b_k - a_k (\mathrm{mod}\, p), k = \overline{1, n}$$
$$\lambda_s \equiv -c_s (a_s \lambda_{s-1} - b_s)^{-1} (\mathrm{mod}\, p) \equiv c_s (b_s - a_s \lambda_{s-1})^{-1} (\mathrm{mod}\, p) \Leftrightarrow$$
$$\lambda_s \equiv c_s (b_s - a_s)^{-1} (\mathrm{mod}\, p) \equiv c_s (c_s)^{-1} (\mathrm{mod}\, p) \equiv 1 (\mathrm{mod}\, p).$$

Индуктивный переход и часть 1 Теоремы 2 доказана.

2. Используя доказанную первую часть, проверим корректность формул (8): $\nu_0 \equiv -f_1 b_0^{-1} (\mathrm{mod}\, p) \equiv -f_1 c_0^{-1} (\mathrm{mod}\, p)$ существует, так как по условию 1) Теоремы 2 $c_0 \in \{1,2,..., p-1\}$ и (по следствию 2 Теоремы 1) существуют числа c_0^{-1} и $\nu_0 \equiv -f_1 c_0^{-1} (\mathrm{mod}\, p)$. Поэтому формула (8) корректна. Аналогично в формуле (9):

$$\nu_k \equiv (f_k - a_k \nu_{k-1})(a_k \lambda_{k-1} - b_k)^{-1} (\mathrm{mod}\, p), k = \overline{1, n-1} \Leftrightarrow$$
$$\nu_k \equiv (a_k \nu_{k-1} - f_k)(b_k - a_k \lambda_{k-1})^{-1} (\mathrm{mod}\, p) \Leftrightarrow$$
$$\nu_k \equiv (a_k \nu_{k-1} - f_k)(b_k - a_k)^{-1} (\mathrm{mod}\, p) \Leftrightarrow$$
$$\nu_k \equiv (a_k \nu_{k-1} - f_k)(c_k)^{-1} (\mathrm{mod}\, p).$$

Последняя формула корректна, так как существует число $(c_k)^{-1}, k = \overline{1, n}$ по условию 2) Теоремы 2. Формула (10) эквивалентна формуле

$$x_n \equiv (f_n - a_n \nu_{n-1})(a_n \lambda_{n-1} - b_n)^{-1} (\mathrm{mod}\, p) \Leftrightarrow$$
$$x_n \equiv (a_n \nu_{n-1} - f_n)(b_n - a_n)^{-1} (\mathrm{mod}\, p) \Leftrightarrow$$
$$x_n \equiv (a_n \nu_{n-1} - f_n)(c_n)^{-1} (\mathrm{mod}\, p),$$

которая корректна по условию 2) Теоремы 2, так как число $(c_n)^{-1}$ существует. То есть, формулы (8)–(11) корректны. **Теорема 2** доказана.

Теорема 3 (Необходимые условия корректности алгоритма (8)–(11)).

Модуль шифрования – простое число *p*.

$$1)\quad b_k - a_k\lambda_{k-1} \neq 0(\mathrm{mod}\ p) \Leftrightarrow$$
$$\lambda_{k-1} \neq b_k a_k^{-1}(\mathrm{mod}\ p),\ k=\overline{1,n}$$
$$2)\quad b_0 \in \{1,2,...,\ p-1\}.$$

Доказательство Теоремы 3 разобьем на части.

1) Простота числа p необходима для взаимно-однозначного поиска обратного числа к любому остатку по $(\mathrm{mod}\ p)$. Это следует из Теоремы 1 и ее Следствий 1 и 2.

2) Запишем уравнение (9)

$$\lambda_k \equiv -c_k\left(a_k\lambda_{k-1} - b_k\right)^{-1}(\mathrm{mod}\ p).$$

Вторую часть теоремы докажем от противного. Пусть при некотором индексе k

$$\exists k: \lambda_{k-1} \equiv b_k a_k^{-1}(\mathrm{mod}\ p),\ k \in \overline{1,n} \Leftrightarrow$$
$$\left(b_k - a_k\lambda_{k-1}\right) \equiv 0(\mathrm{mod}\ p) \Rightarrow .$$

Не существует числа $\left(b_k - a_k\lambda_{k-1}\right)^{-1}(\mathrm{mod}\ p) \Rightarrow$ невозможно вычислить коэффициент $\lambda_k \equiv -c_k\left(a_k\lambda_{k-1} - b_k\right)^{-1}(\mathrm{mod}\ p)$ по предыдущему коэффициенту λ_{k-1}. Также невозможно правильно определить все последующие коэффициенты цепочки $\lambda_{k+1}, \lambda_{k+2}, ...$ формул прогонки вперед**.**

3) Условие $b_0 \in \{1,2,...,\ p-1\}$ следует из Формулы $\lambda_0 \equiv c_0 b_0^{-1}(\mathrm{mod}\ p)$ при вычислении коэффициента λ_0. **Теорема 3** доказана.

Применим алгоритм (8)–(11) для шифрования текстовых (символьных) данных. Например, восклицательный знак на клавиатуре в таблице ASCII имеет порядковый номер 33 [5]. Рассмотрим примеры.

Пример 1. Текст для шифрования: "Москва – город-герой в Великой Отечественной войне 1941–1945!!!" английским шрифтом (рис. 1.).

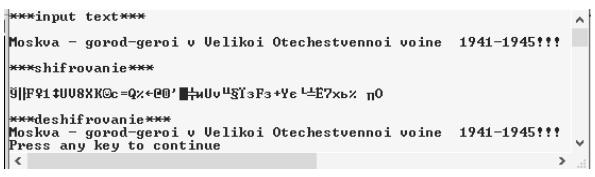

Рис. 1. *Шифруется текст (пример 1) с ключами*

$$c_0 = 1, b_0 = 1, n = 64, c_0 \equiv b_0(\mathrm{mod}\ 257)$$
$$c_k = 2k+1 < p = 257, c_k \in \{1,2,...,\ p-1\}, k = \overline{0,n}$$
$$a_k = 3k+1; b_k \equiv a_k + c_k(\mathrm{mod}\ 257), k = \overline{1,n}.$$

В примере 1 использованы условия 1), 2) Теоремы 2 (ограничения на коэффициенты). Как видно из рис. 1, исходный и дешифрованный тексты посимвольно совпадают.

Пример 2. Текст для шифрования: "Москва – город-герой в Великой Отечественной войне 1941–1945!!!" с другими ключами (рис. 2).

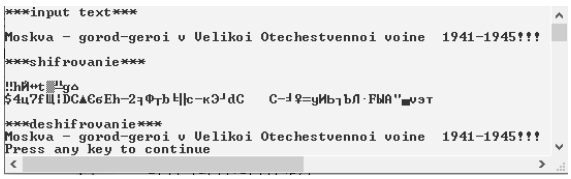

Рис. 2. *Шифруется текст (пример 2) с ключами*

$$c_0 = 3, b_0 = 3, n = 64, c_0 \equiv b_0(\mathrm{mod}\ 257)$$
$$c_k = k+3 < p = 257, c_k \in \{1,2,...,\ p-1\}, k = \overline{0,n}$$
$$a_k = 13k+2; b_k \equiv a_k + c_k(\mathrm{mod}\ 257), k = \overline{1,n}$$

В примере 2 также использованы условия 1), 2) Теоремы 2 – ограничения на коэффициенты. Как видно из рис. 2, исходный и дешифрованный тексты посимвольно совпадают. Разным наборам ключей соответствуют и разные шифры одного и того же текста (сравним шифры рис. 1 и рис. 2).

Пример 3 показывает, что условия Теоремы 2 являются достаточными для корректности алгоритма (8)–(11), но не являются необходимыми. Текст для шифрования: "Смоленск – город-герой в Великой Отечественной войне 1941–1945!!!" (рис. 3.).

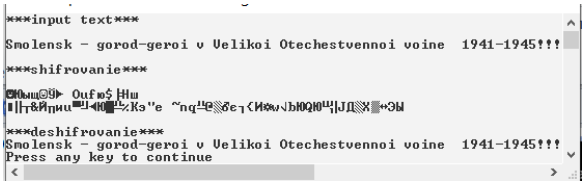

Рис. 3. *Шифруется текст (пример 3) с ключами*

$$c_0 = 3, b_0 = 3, n = 64, c_0 \equiv b_0(\mathrm{mod}\ 257)$$
$$c_k = 2k+3 < p = 257, c_k \in \{1,2,...,\ p-1\}, k = \overline{0,n}$$
$$a_k = k+2; b_k = c_k(\mathrm{mod}\ 257), k = \overline{1,n}$$

В примере 3 не выполнено достаточное условие Теоремы 2 $b_k \equiv a_k + c_k(\mathrm{mod}\ p), k = \overline{1,n}$. Тем не менее, исходный текст и дешифрованный совпадают.

Программа написана языке C++.

Все функции и переменные в программе принимают целые значения, в программе ключи шифрования и текст из примера 1.

```
#include "stdafx.h"
#include<stdio.h>#include<math.h>
int inverse(int x, int p){ int i,y;x=x%p;  if(x<0)
        {x=x+p;}for(i=1;i<=p-1;i++)
        {if(i*x%p==1){y=i;return y;}}}
int const p=257,n=65,n0=n-1;int main()
{int                                    j,
a[n+2],b[n+2],c[n+2],nu[n+2],lamda[n+2],f[n+2]
,mas1[n+2], mas2[n+2] ,d1,d2,d3,d4;
char mas[n+2]="Moskva - gorod-geroi v Velikoi
Otechestvennoi voine 1941–1945!!!\n";
                printf("***input text***\n");
                printf("\n");
for(j=0;j<=n;j++){printf("%c",mas[j]);}
        for(j=0;j<=n0;j++)
        { a[j]=(3*j+1)%p;      c[j]=(2*j+1)%p;
        b[j]=(a[j]+c[j])%p;}
                        b[0]=c[0];printf("\n");
        printf("***shifrovanie***\n");
                        printf("\n");f[0]=(-
b[0]*mas[0]+c[0]*mas[1])%p;
                if(f[0]<0)
        {f[0]=f[0]+p;}for(j=1;j<=n0-1;j++)
        {f[j]=(mas[j-1]*a[j]-
mas[j]*b[j]+mas[j+1]*c[j])%p;
        printf("%c",f[j]);}f[n0]=(mas[n0-
1]*a[n0]-mas[n0]*b[n0])%p;
        printf("\n");printf("\n");lamda[0]=(c[0]
*inverse(b[0],p))%p;
                nu[0]=(-
f[0]*inverse(b[0],p))%p;if(nu[0]<0){nu[0]=nu[0]
+p;}
        printf("***deshifrovanie***\n");for(j=1
;j<=n0;j++)
{d3=(b[j]-a[j]*lamda[j-
1])%p;lamda[j]=(c[j]*inverse(d3,p))%p;
                d4=(a[j]*nu[j-1]-
f[j])%p;if(d4<0){d4=d4+p;}
        nu[j]=(d4*inverse(d3,p))%p;}d1=(a[n0]
*lamda[n0-1]-b[n0])%p;
        d2=(f[n0]-a[n0]*nu[n0-
1])%p;if(d2<0){d2=d2+p;}mas1[n0]=(d2*invers
e(d1,p))%p;
for(j=n0-1;j>=0;j--
){mas1[j]=(mas1[j+1]*lamda[j]+nu[j])%p;}
for(j=0;j<=n0;j++){printf("%c",mas1[j]);}printf(
"\n");}
```

Основные полученные результаты:

1) Предложен алгоритм шифрования-дешифрования СЛАУ с трехдиагональной матрицей в классах вычетов по простому модулю-формулы (7)–(11).

2) В Теореме 2 доказаны достаточные условия корректности алгоритма (8)–(11).

3) В Теореме 3 доказаны необходимые условия корректности алгоритма (8)–(11).

4) Приведены 3 примера шифрования–дешифрования текстовых данных, поясняющие смысл и условия доказанных теорем.

Список источников

1. *Бахвалов Н.С.* Численные методы: учебное пособие для студентов физ.-мат. специальностей вузов / Н.С. Бахвалов, Н.П. Жидков, Г.М. Кобельков; Московский гос. ун-т им. М.В. Ломоносова. 7-е изд. М.: Бином. Лаб. знаний, 2011. 636 с. (Классический университетский учебник). ISBN 978-5-9963-0449-3. EDN QJXMXL.
2. *Бахвалов Н.С., Лапин А.В., Чижонков Е.В.* Численные методы в задачах и упражнениях. М.: БИНОМ, 2010, 240 с.
3. *Фаддеев Д.К.* Лекции по алгебре: учеб. пособие для вузов. М.: Наука. Гл. ред. физ.-мат. лит-ры. 1984. 416 с.
4. *Виноградов И.М.* Основы теории чисел: учеб. пособие. Изд. 11-е, стер. СПб [и др.]: Лань, 2006. 176 с. (Лучшие классические учебники. Математика). ISBN 5-8114-0535-9. EDN QJPTQT.
5. *Лидовский В.В.* Теория информации: Учебное пособие. М.: Компания Спутник, 2004. 111 с. ISSN 5-93406-661-7.
6. *Чернов П.К.* Создание интегрированной модели данных из разнородных источников, содержащих цифровые следы / П.К. Чернов, Е.А. Рабчевский // Вестник Пермского университета. Математика. Механика. Информатика. 2022. Вып. 2(57). С. 81–87. DOI 10.17072/1993-0550-2022-2-81-87. EDN UYUSGT.
7. *Пермский* международный форум "Наука и глобальные вызовы XXI века" / М.М. Бузмакова, Е.Ю. Никитина, А.В. Черников, Л.Н. Ясницкий // Вестник Пермского университета. Математика. Механика. Информатика. 2022. Вып. 4(59). С. 5–8. EDN WUMBNC.
8. *Нехорошева Э.А.* Построение модели протокола электронного голосования с возможностью проверки результата избирателями / Э.А. Нехорошева, А.П. Шкарапута

// Вестник Пермского университета. Математика. Механика. Информатика. 2022. Вып. 4(59). С. 61–67. DOI 10.17072/1993-0550-2022-4-61-67. EDN QAMNYK.

9. *Поторочина К.Л.* Безопасность применения IoT в сфере здравоохранения / К.Л. Поторочина, Е.Ю. Никитина // Вестник Пермского университета. Математика. Механика. Информатика. 2022. Вып. 4(59). С. 68–81. DOI 10.17072/1993-0550-2022-4-68-81. EDN FBHTIG.
10. *Пастухов Д.Ф., Волосова Н.К., Волосова А.К.* Некоторые методы передачи QR-кода в стеганографии / Д.Ф. Пастухов, Н.К. Волосова, А.К. Волосова // Мир транспорта. 2019. Т. 17, № 3(82). С. 16–39.
11. *Чернов П.К.* Модификация алгоритма на основе сети Фейстеля с добавлением элемента случайности в ключ шифрования / П. К. Чернов, А. П. Шкарапута // Вестник Пермского университета. Математика. Механика. Информатика. 2021. Вып. 1(52). С. 81–88. DOI 10.17072/1993-0550-2021-1-81-88. EDN MGBPSA.
12. *Разработка* элементов криптопроцессора с использованием отечественной САПР "Ковчег" / О.А. Зобнина, А.Н. Каменских, Г.К. Королев, С.Ф. Тюрин // Вестник Пермского университета. Математика. Механика. Информатика. 2019. Вып. 2(45). С. 60–66. DOI 10.17072/1993-0550-2019-2-60-66. EDN IYZAXK.
13. *Александрова Е.И.* Модификация алгоритмов на основе сети Фейстеля посредством внесения избыточности с помощью кодов Хэмминга / Е.И. Александрова, А.П. Шкарапута // Вестник Пермского университета. Математика. Механика. Информатика. 2018. Вып. 3(42). С. 95–103. DOI 10.17072/1993-0550-2018-3-95-103. EDN VKVNHZ.
14. *Евстафьев Е.О.* Алгоритм динамической обфускации информации с ограничением количества попыток расшифровки, исполнения и просмотра на web-клиенте / Е.О. Евстафьев, С.Ф. Тюрин // Вестник Пермского университета. Математика. Механика. Информатика. 2018. Вып. 4(43). С. 56–59. DOI 10.17072/1993-0550-2018-4-56-59. EDN YRJEDJ.
15. *Ронзин В.И.* Разработка программного модуля поиска нарушений для интегрированной системы безопасности / В.И. Ронзин, Е.Ю. Никитина // Вестник Пермского университета. Математика. Механика. Информатика. 2020. Вып. 1(48). С. 69–73. DOI 10.17072/1993-0550-2020-1-69-73. EDN MSQOTG.

References

1. *Bakhvalov N.S., Zhidkov N.P., Kobelkov G.M.* Numerical methods: a textbook for students of physical and mathematical specialties of higher educational institutions; Moscow state. un-t im. M.V. Lomonosov. 7th ed. M.: Binom. Lab. Knowledge; 2011. 636 p. (Classic University textbook). ISBN 978-5-9963-0449-3. EDN QJXMXL. (In Russ.).
2. *Bakhvalov N.S., Lapin A.V., Chizhonkov E.V.* Numerical methods in problems and exercises. M.: BINOM; 2010. 240 p. (In Russ.).
3. *Faddeev D.K.* Lectures on Algebra: Textbook for High Schools. M.: Science. The main edition of physical and mathematical literature; 1984. 416 p. (In Russ.).
4. *Vinogradov I.M.* Fundamentals of number theory: textbook. Allowance. Ed. 11th, ster. St. Petersburg [and others]: Lan, 2006; 176 p. (The best classical textbooks. Mathematics). ISBN 5-8114-0535-9. EDN QJPTQT. (In Russ.).
5. *Lidovsky V.V.* Information Theory: Textbook. M.: Company Sputnik +; 2004. 111 p. ISSN 5-93406-661-7. (In Russ.).
6. *Chernov P.K., Rabchevsky E.A.* Creation of an integrated data model from heterogeneous sources containing digital traces. Bulletin of the Perm University. Mathematics. Mechanics. Computer science. 2022; 2(57):81–87. DOI 10.17072/1993-0550-2022-2-81-87. EDN UYUSGT. (In Russ.).
7. *Buzmakova M.M., Nikitina E.Yu., Chernikov A.V., Yasnitsky L.N.* Perm International Forum "Science and Global Challenges of the 21st Century". Bulletin of the Perm University. Mathematics. Mechanics. Computer science. 2022;(4(59)):5–8. EDN WUMBNC. (In Russ.).
8. *Nehorosheva E.A., Shkaraputa A.P.* Building a model of the protocol of electronic voting with the possibility of checking the result by voters. Bulletin of the Perm University. Mathematics. Mechanics. Computer science. 2022;(4(59)):61–67. DOI 10.17072/1993-0550-2022-4-61-67. EDN QAMNYK. (In Russ.).

9. *Potorochina K.L., Nikitina E.Yu.* Safety of IoT application in healthcare. Bulletin of the Perm University. Mathematics. Mechanics. Computer science. 2022;(4(59)):68–81. DOI 10.17072/1993-0550-2022-4-68-81. EDN FBHTIG. (In Russ.).
10. *Pastukhov D.F., Volosova N.K., Volosova A.K.* Some methods of transmitting a QR code in steganography. World of transport. 2019;(17, 3(82)):16–39. (In Russ.).
11. *Chernov P.K., Shkaraputa A.P.* Algorithm modification based on the Feistel network with the addition of an element of randomness to the encryption key. Bulletin of the Perm University. Mathematics. Mechanics. Computer science. 2021;(1(52)):81–88. DOI 10.17072/1993-0550-2021-1-81-88. EDN MGBPSA. (In Russ.).
12. *Zobnina O.A., Kamenskikh A.N., Korolev G.K., Tyurin S.F.* Development of cryptoprocessor elements using domestic CAD "Ark". Bulletin of the Perm University. Mathematics. Mechanics. Computer science. 2019;(2(45)):60–66. DOI 10.17072/1993-0550-2019-2-60-66. EDN IYZAXK. (In Russ.).
13. *Aleksandrova E.I., Shkaraputa A.P.* Modification of algorithms based on the Feistel network by introducing redundancy using Hamming codes. Bulletin of the Perm University. Mathematics. Mechanics. Computer science. 2018;(3(42)):95–103. DOI 10.17072/1993-0550-2018-3-95-103. EDN VKVNHZ. (In Russ.).
14. *Evstafiev E.O., Tyurin S.F.* Algorithm for dynamic information obfuscation with a limited number of attempts to decrypt, execute and view on a web client. Bulletin of the Perm University. Mathematics. Mechanics. Computer science. 2018;(4(43)):56–59. DOI 10. 17072/1993-0550-2018-4-56-59. EDN YRJEDJ. (In Russ.).
15. *Ronzin V.I., Nikitina E.Yu.* Development of a software module for detecting violations for an integrated security system. Bulletin of the Perm University. Mathematics. Mechanics. Computer Science. 2020;(1(48)):69–73. DOI 10.17072/1993-0550-2020-1-69-73. EDN MSQOTG. (In Russ.).

Информация об авторах:

Наталья Константиновна Волосова – аспирант МГТУ им. Н. Э. Баумана (105005, Россия, г. Москва, 2-я Бауманская ул., д. 5, стр. 1), navalosova@yandex.ru, https://orcid.org/0000-0538-2445;

Константин Александрович Волосов – доктор физико-математических наук, профессор кафедры прикладной математики Российского университета транспорта (127994, ГСП-4, Россия, г. Москва, ул. Образцова, д. 9, стр. 9), konstantinvolosov@yandex.ru, https://orcid.org/0000-0002-7955-0587, AuthorID 128228;

Александра Константиновна Волосова – кандидат физико-математических наук, начальник аналитического отдела ООО "Трамплин" Российского университета транспорта (127994, ГСП-4, Россия, г. Москва, ул. Образцова, д. 9, стр. 9), alya01@yandex.ru, https://orcid.org/0000-0002-0538-2445, AuthorID 607500;

Михаил Иванович Карлов – кандидат физико-математических наук, доцент кафедры высшей математики Московского физико-технического университета (МФТИ) (141701, Россия, Московская область, г. Долгопрудный, Институтский пер., 9.), karlov@shade.msu.ru, AuthorID 14680;

Дмитрий Феликсович Пастухов – кандидат физико-математических наук, доцент кафедры технологий программирования Полоцкого государственного университета (211440, Республика Беларусь, Витебская обл., г. Новополоцк, ул. Блохина, 29), dmitrij.pastuhov@mail.ru, https://orcid.org/0000-0003-1398-6238, AuthorID 405101;

Юрий Феликсович Пастухов – кандидат физико-математических наук, доцент кафедры технологий программирования Полоцкого государственного университета (211440, Республика Беларусь, Витебская обл., г. Новополоцк, ул. Блохина, 29), pulsar1900@mail.ru, https://orcid.org/0000-0001-8548-6959, AuthorID 405109.

Information about the authors:

Natalya K. Volosova – Post-graduate Student of Bauman Moscow State Technical University (2nd Baumanskaya St. 5-1, Moscow, Russia, 105005), navalosova@yandex.ru, https://orcid.org/0000-0538-2445;

Konstantin A. Volosov – Doctor of Physical and Mathematical Sciences, Professor of the Department of Applied Mathematics of the Russian University of Transport (Obraztsova St. 9-9, Moscow, GSP-4, Russia, 127994), konstantinvolosov@yandex.ru, https://orcid.org/0000-0002-7955-0587, AuthorID 128228;

Aleksandra K. Volosova – Candidate of Physical and Mathematical Sciences, Chief Analytical Department "Tramplin" LLC, Russian University of Transport (Obraztsova St. 9-9, Moscow, GSP-4, Russia, 127994), alya01@yandex.ru, https://orcid.org/0000-0002-0538-2445, AuthorID 607500;

Mikhail I. Karlov – Candidate of Physical and Mathematical Sciences, Associate Professor of the Department of Higher Mathematics, Moscow University of Physics and Technology (9, Institutskiy per., Dolgoprudny, Moscow region, Russia, 141701), karlov@shade.msu.ru, AuthorID 14680;

Dmitriy F. Pastukhov – Candidate of Physical and Mathematical Sciences, Associate Professor of Polotsk State University (Blokhin St. 29, Novopolotsk, Vitebsk Region, Republic of Belarus, 211440), dmitrij.pastuhov@mail.ru, https://orcid.org/0000-0003-1398-6238; AuthorID 405101;

Yuriy F. Pastukhov – Candidate of Physical and Mathematical Sciences, Associate Professor of Polotsk State University (Blokhin St. 29, Novopolotsk, Vitebsk Region, Republic of Belarus, 211440), pulsar1900@mail.ru, https://orcid.org/0000-0001-8548-6959, AuthorID 405109.