МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
федеральное государственное автономное образовательное учреждение высшего образования
“САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ АЭРОКОСМИЧЕСКОГО ПРИБОРОСТРОЕНИЯ”

КАФЕДРА № 14

ОТЧЕТ
ЗАЩИЩЕН С ОЦЕНКОЙ
ПРЕПОДАВАТЕЛЬ

доц., канд. техн. наук		Н.А. Шехунова
должность, уч. степень, звание	подпись, дата	инициалы, фамилия

ОТЧЁТ О ЛАБОРАТОРНОЙ РАБОТЕ № 2

«Конечные поля. Генерирование элементов полей $GF(p^m)$ в конечных полях»

по курсу: «Кодирование и декодирование сообщений»

РАБОТУ ВЫПОЛНИЛ
СТУДЕНТ ГР. № 1842 Я.А.Вишневский
подпись, дата инициалы, фамилия

Санкт-Петербург 2021

1. Цель работы

Изучить способы задания циклических кодов, формирование порождающей матрицы и получение кодовых слов на основе построенного полинома заданного циклического кода. Для заданного порождающего полинома конечного поля построить информационные последовательности, порождающую матрицу и кодовые слова.

2. Постановка задачи

Построить информационные векторы полинома, представленного в лексикографическом порядке 75G, GF(2^m) при m = 5;

Выполнить операции сложения и умножения полей

3. Результаты

Полином 75G раскладывается на 111101 и равен $x^5 = 1 + x^2 + x^3 + x^4$

Таблица 1 – конечные поля полинома 75G

0	0	0	0	0	0	0
1	0	0	0	0	1	1
0	1	0	0	0	v^1	x^1
0	0	1	0	0	v^2	x^2
0	0	0	1	0	v^3	x^3
0	0	0	0	1	v^4	x^4
1	0	1	1	1	v^5	1+x^2+x^3+x^4
1	1	1	0	0	v^6	1+x^1+x^2
0	1	1	1	0	v^7	x^1+x^2+x^3
0	0	1	1	1	v^8	x^2+x^3+x^4
1	0	1	0	0	v^9	1+x^2
0	1	0	1	0	v^10	x^1+x^3
0	0	1	0	1	v^11	x^2+x^4
1	0	1	0	1	v^12	1+x^2+x^4
1	1	1	0	1	v^13	1+x^1+x^2+x^4
1	1	0	0	1	v^14	1+x^1+x^4
1	1	0	1	1	v^15	1+x^1+x^3+x^4
1	1	0	1	0	v^16	1+x^1+x^3
0	1	1	0	1	v^17	x^1+x^2+x^4
1	0	0	0	1	v^18	1+x^4
1	1	1	1	1	v^19	1+x^1+x^2+x^3+x^4
1	1	0	0	0	v^20	1+x^1
0	1	1	0	0	v^21	x^1+x^2
0	0	1	1	0	v^22	x^2+x^3
0	0	0	1	1	v^23	x^3+x^4
1	0	1	1	0	v^24	1+x^2+x^3
0	1	0	1	1	v^25	x^1+x^3+x^4
1	0	0	1	0	v^26	1+x^3
0	1	0	0	1	v^27	x^1+x^4
1	0	0	1	1	v^28	1+x^3+x^4
1	1	1	1	0	v^29	1+x^1+x^2+x^3
0	1	1	1	1	v^30	x^1+x^2+x^3+x^4

```
Таблица хранения переменных, где крайний правый столбец это степень v:
     1     0     0     0     0     0
     0     1     0     0     0     1
     0     0     1     0     0     2
     0     0     0     1     0     3
     0     0     0     0     1     4
     1     0     1     1     1     5
     1     1     1     0     0     6
     0     1     1     1     0     7
     0     0     1     1     1     8
     1     0     1     0     0     9
     0     1     0     1     0    10
     0     0     1     0     1    11
     1     0     1     0     1    12
     1     1     1     0     1    13
     1     1     0     0     1    14
     1     1     0     1     1    15
     1     1     0     1     0    16
     0     1     1     0     1    17
     1     0     0     0     1    18
     1     1     1     1     1    19
     1     1     0     0     0    20
     0     1     1     0     0    21
     0     0     1     1     0    22
     0     0     0     1     1    23
     1     0     1     1     0    24
     0     1     0     1     1    25
     1     0     0     1     0    26
     0     1     0     0     1    27
     1     0     0     1     1    28
     1     1     1     1     0    29
     0     1     1     1     1    30
Операция сложения:
9 строка:
     0     0     1     1     1

22 строка:
     0     1     1     0     0

Результат операции сложения 9 и 22 строки:
     0     1     0     1     1

Операция умножения:
9 строка:
     0     0     1     1     1

22 строка:
     0     1     1     0     0

Результат операции умножения 9 и 22 строки - 30 строка:
     1     1     1     1     0
```

Рисунок 1 – Вывод результата работы в командную строку

4. Блок-схема алгоритма

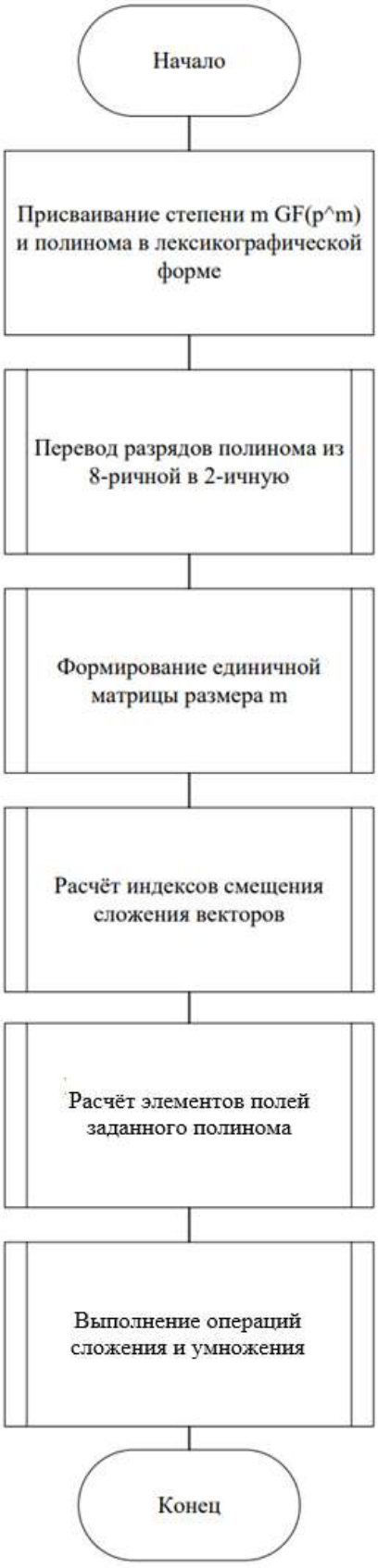

Рисунок 2 – схема алгоритма работы программы

5. Листинг программы

```
clear;

m=5; pol=75;

i = pol;
b = 0; cnt = 0; gcnt = 0;
while i~=0
    b = mod(i,10);
    binstr = dec2bin(b,3);
    cnt = 3;
    while cnt~=0
        gcnt = gcnt + 1;
        gal_base(gcnt) = binstr(cnt);
        %генерация индексов полинома
        cnt=cnt-1;
    end
    i = fix(i/10);
end
galmas = eye(m);
% i - string j - column
i = 0;
while i~=m
    i = i + 1;
    galmas(i,m+1) = i - 1;
    %расчёт индексов смещения сложения векторов
    if(gal_base(i) == '1')
        xorstr(i) = m - i + 1;
    else
        xorstr(i) = 0;
    end
end
i = m;
%xorstr =
while i~=2.^m - 1
    i = i + 1;
    j = 0;
    z = 0;
    while z~=m
        z = z + 1;
        galmas(i,z) = 0;
    end
    while j~=m
        j = j + 1;
        if(xorstr(j)>0)
            z = 0;
            while z~=m
                z = z + 1;
                galmas(i,z) = galmas(i,z) + galmas(i - xorstr(j),z);
                % расчёт новой строки путём складывания существующих
            end
        end
    end
    z = 0;
    while z~=m
        z = z + 1;
        galmas(i,z) = mod(galmas(i,z),2);
    end
    galmas(i,m+1) = i - 1;
end
```

```
fprintf('Таблица хранения переменных, где крайний правый столбец это степень
v:\n');
disp(galmas);

fprintf('Операция сложения:\n');
aa = 9; bb = 22;
res = summa(galmas,aa,bb,m);%(mas, a, b, m)
fprintf('%d строка:\n', aa);
disp(galmas(aa,1:m));
fprintf('%d строка:\n', bb);
disp(galmas(bb,1:m));
fprintf('Результат операции сложения %d и %d строки:\n', aa, bb);
disp(res);

fprintf('Операция умножения:\n');
aa = 9; bb = 22;
[res, step] = multiply(galmas,aa,bb,m);%(mas, a, b, m)
fprintf('%d строка:\n', aa);
disp(galmas(aa,1:m));
fprintf('%d строка:\n', bb);
disp(galmas(bb,1:m));
fprintf('Результат операции умножения %d и %d строки - %d строка:\n', aa, bb,
step);
disp(res);
%-------------------------------------------------------------------------
function res = summa(mas, a, b, m)
    for i=1:m
        res(i)=mod(mas(a,i)+mas(b,i),2);
    end
end
function [res, step] = multiply(mas, a, b, m)
    step = mod(a+b,2^m-1);
    res = mas(step+1,1:m);
    step = step + 1;
end
```

6. Вывод

В ходе лабораторной работы был изучен способ построения полей Галуа. Была разработана программа для расчёта элементов полей, в которой реализованы элементы умножения и сложения последовательностей.