Министерство науки и высшего образования Российской Федерации

Федеральное государственное бюджетное образовательное учреждение высшего образования

«Рязанский государственный радиотехнический

университет имени В.Ф. Уткина»

Кафедра «ЭВМ»

Отчет о лабораторной работе №2

«Шифры перестановки на примере шифра кардано»

по дисциплине

«Защита информации»

Выполнили:

Студенты группы 045

Анохин В.А.

Вашкулатов Н.А.

Проверили:

доц. Крошилина С.В.

доц. Тишкина В.В.

**Цель работы**: разработать алгоритмы шифрования и дешифрования сообщений с применением решетки Кардано.

**Ход работы**

На рисунках 1 – 3 показаны схемы алгоритмов данной программы.

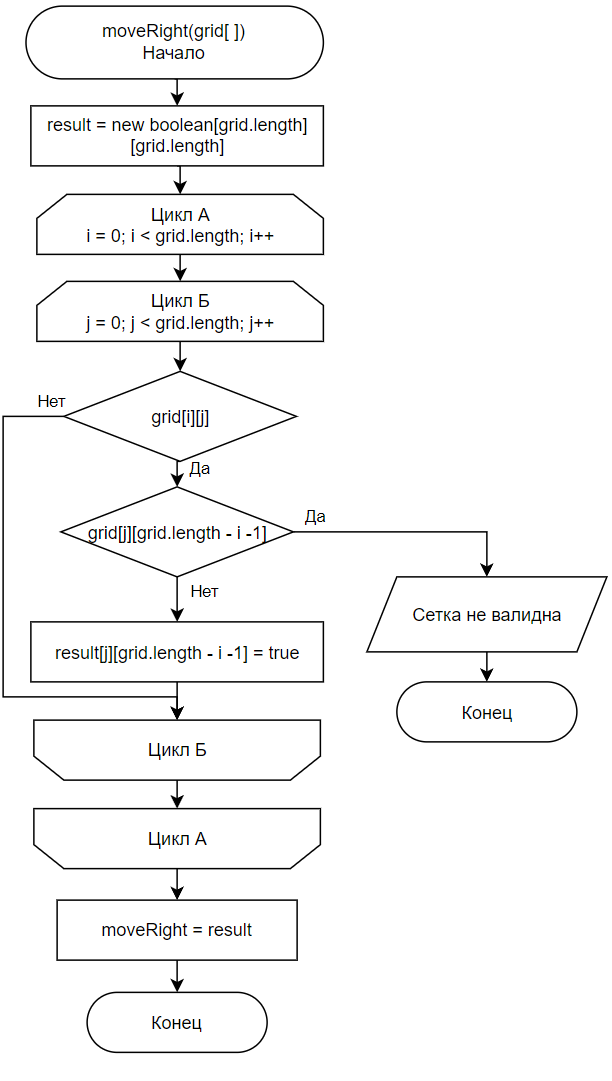


Рисунок 1 – Схема подпрограммы moveRight

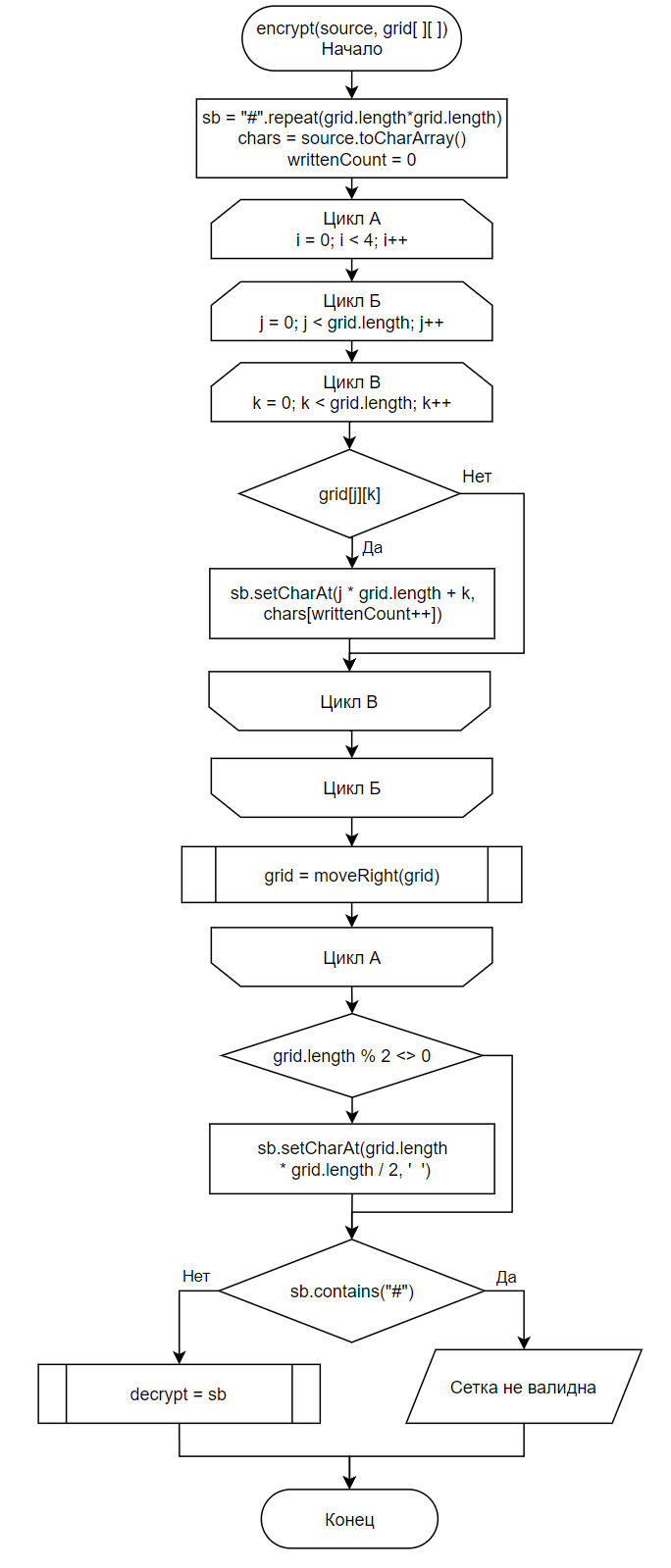


Рисунок 2 – Схема подпрограммы encrypt

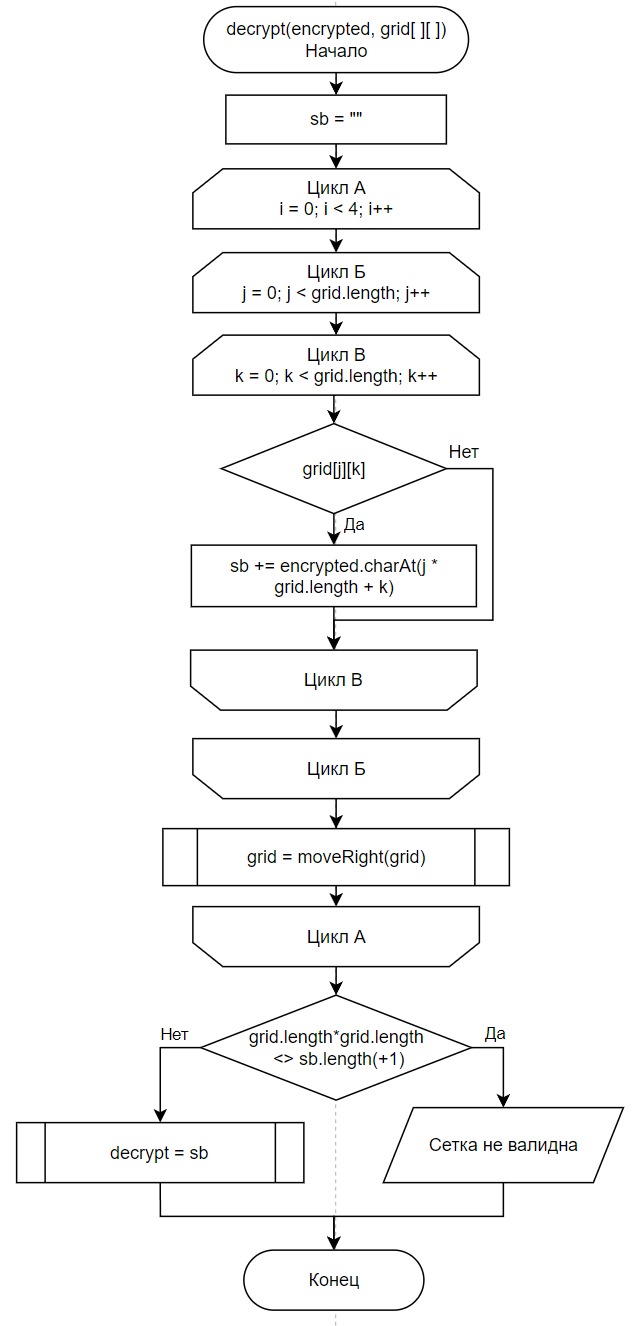


Рисунок 3 – Схема подпрограммы decrypt

**Код программы:**

public class Cardano {

public static String encrypt(String source, boolean[][] grid) {

var sb = new StringBuilder();

//заполняем пробелами

sb.append("#".repeat(grid.length \* grid.length));

char[] chars = source.toCharArray();

int writtenCount = 0;

for (int i = 0; i < 4; i++) {

for (int j = 0; j < grid.length; j++) {

for (int k = 0; k < grid.length; k++) {

if (grid[j][k]) {

//записали на нужное место

sb.setCharAt(j \* grid.length + k, chars[writtenCount++]);

}

}

}

//повернули сетку

grid = moveRight(grid);

}

if (grid.length % 2 != 0) {

sb.setCharAt(grid.length \* grid.length / 2, ' ');

}

var result = sb.toString();

if (result.contains("#")) throw new IllegalArgumentException("Сетка не валидна");

return sb.toString();

}

public static String decrypt(String encrypted, boolean[][] grid) {

var sb = new StringBuilder();

for (int i = 0; i < 4; i++) {

//Чтение из таблицы по сетке

for (int j = 0; j < grid.length; j++) {

for (int k = 0; k < grid.length; k++) {

if (grid[j][k]) {

//записали на нужное место

sb.append(encrypted.charAt(j \* grid.length + k));

}

}

}

//поворот сетки

grid = moveRight(grid);

}

if(grid.length \* grid.length != sb.length() + 1) throw new IllegalArgumentException("Сетка не валидна");

return sb.toString();

}

static boolean[][] moveRight(boolean[][] grid) {

boolean[][] result = new boolean[grid.length][grid.length];

for (int i = 0; i < grid.length; i++) {

for (int j = 0; j < grid.length; j++) {

if (grid[i][j]) {

//поворот на 90

if (grid[j][grid.length - i - 1]) throw new IllegalArgumentException("Сетка не валидна");

else result[j][grid.length - i - 1] = true;

}

}

}

return result;

}

}

**Вывод**: в ходе выполнения работы были разработаны алгоритмы шифрования и дешифрования сообщений с применением решетки Кардано.