

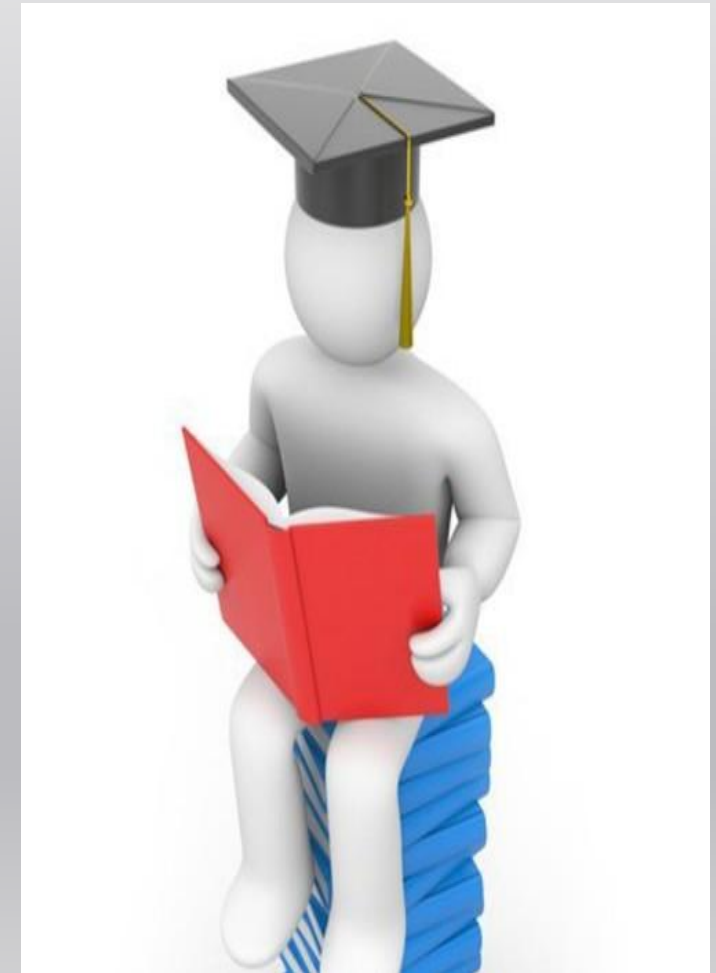
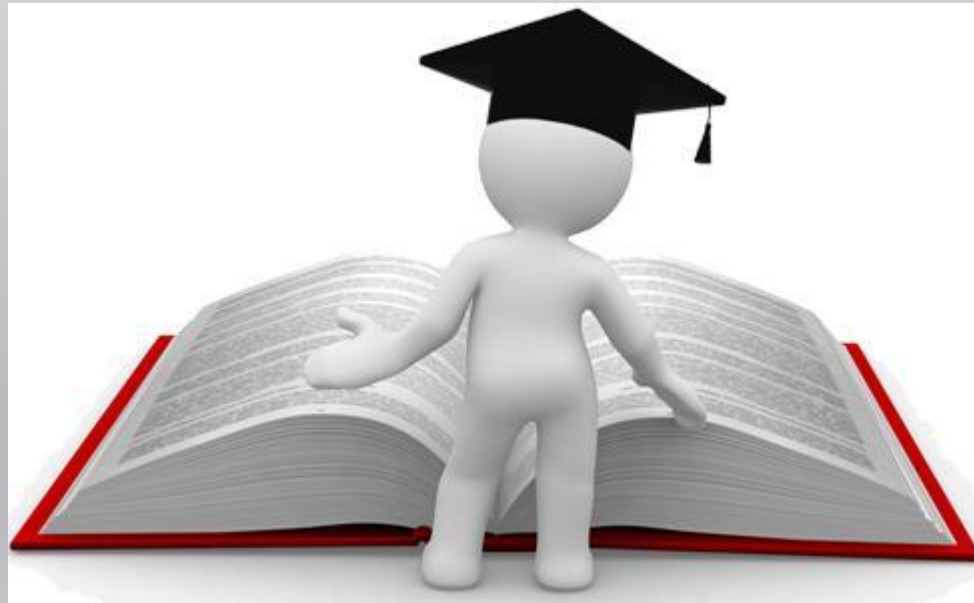
ПРОЕКТ

Создание программы для шифрования и дешифрования
текста на языке Pascal

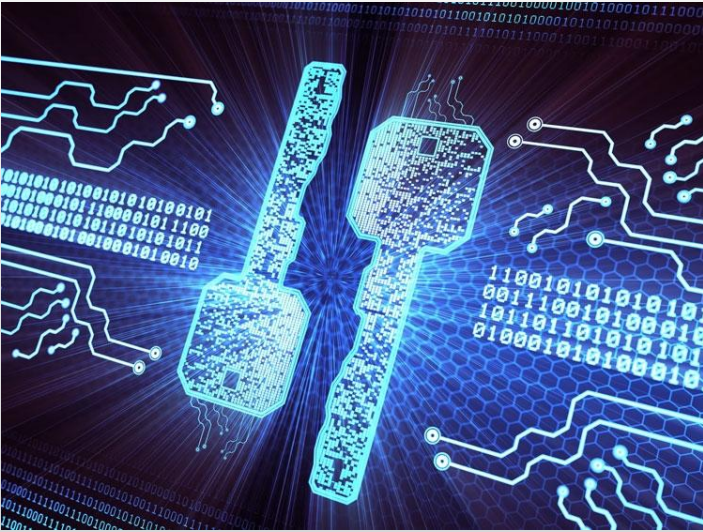
Выполнил ученик 10 «Б» класса

Сергеев Георгий Олегович

- **Актуальность проектной работы:** необходимость скрыть смысл написанного текста от возможных злоумышленников.
- **Цель проектной работы:** написать программу для шифрования и дешифрования текста на языке Pascal.
- **Задачи проектной работы:** собрать информацию о различных способах шифрования текста, разработать свой шифр, написать программу для шифрования и дешифрования текста на языке Pascal.



- **Шифрование** - это преобразование (кодирование) открытой информации в зашифрованную, недоступную для понимания посторонними
- **Ключ** – это параметр алгоритма шифрования, позволяющий выбрать одно конкретное преобразование из всех вариантов, предусмотренных алгоритмом. Знание ключа позволяет свободно зашифровывать и расшифровывать сообщения.
- **Криптостойкость шифра** – это устойчивость шифра к расшифровке без знания ключа.



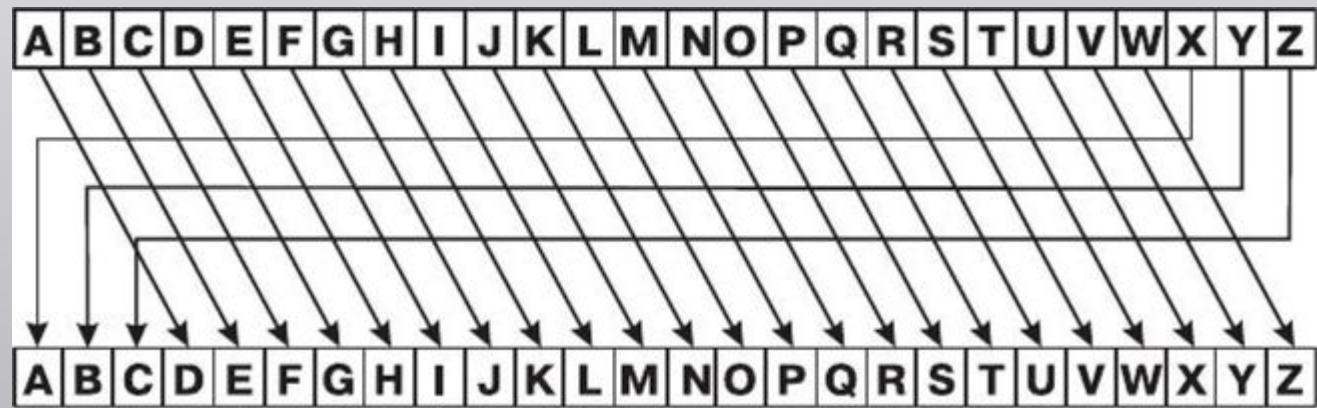
Шифр простой замены

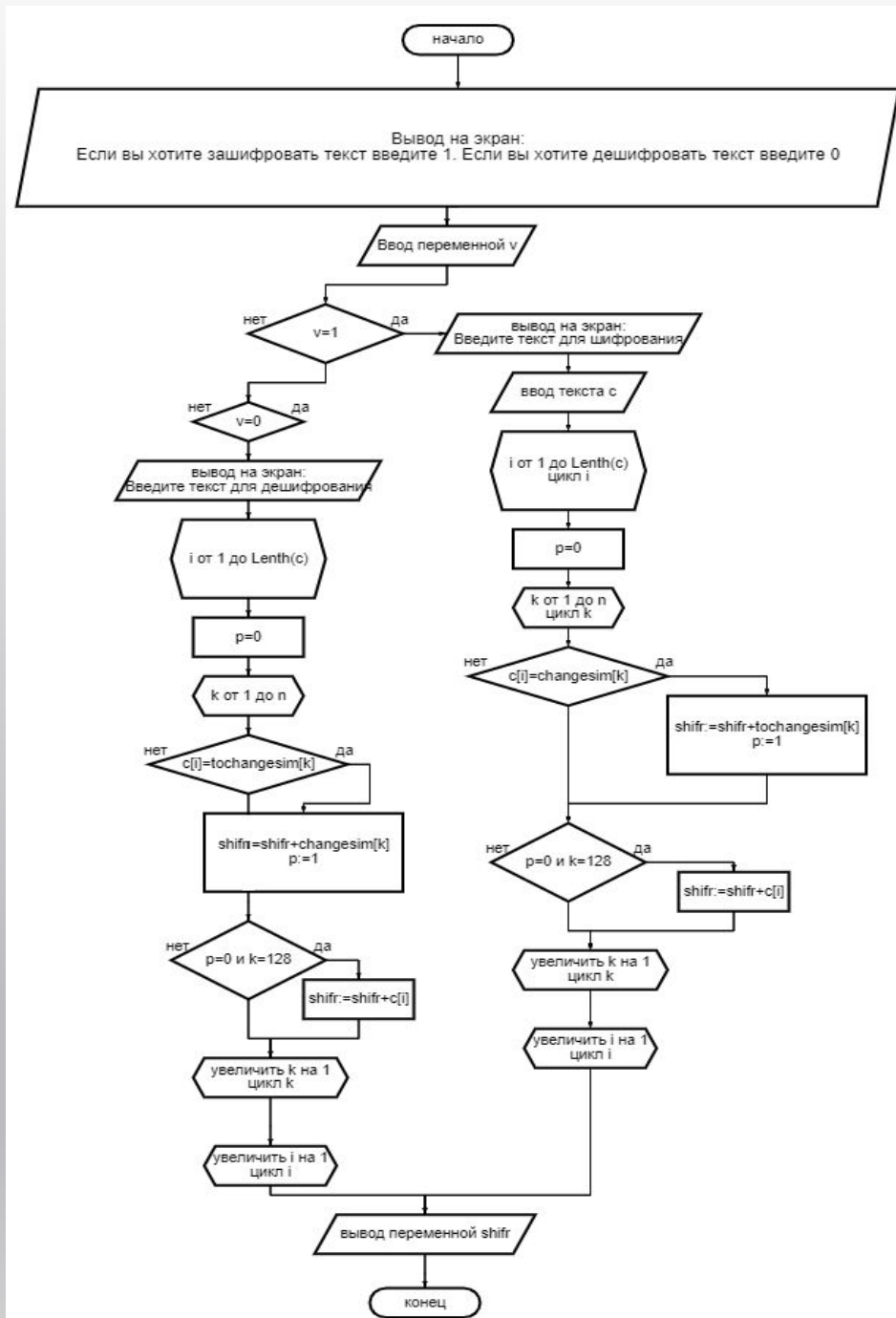
- **моноалфавитный шифр** — класс методов шифрования, которые сводятся к созданию по определённому алгоритму таблицы шифрования, в которой для каждой буквы открытого текста существует единственная сопоставленная ей буква шифр-текста. Само шифрование заключается в замене букв согласно таблице. Для расшифровки достаточно иметь ту же таблицу, либо знать алгоритм, по которому она генерируется.

А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р
09	23	01	04	07	02	14	13	21	31	17	25	29	06	22	11	26
С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я		
00	19	30	08	18	16	28	03	27	32	15	10	20	24	12	05	

Шифр Цезаря

- В данном шифре каждая буква в слове или тексте заменяется другой, которая находится на некоторое постоянное число позиций левее или правее от неё в алфавите



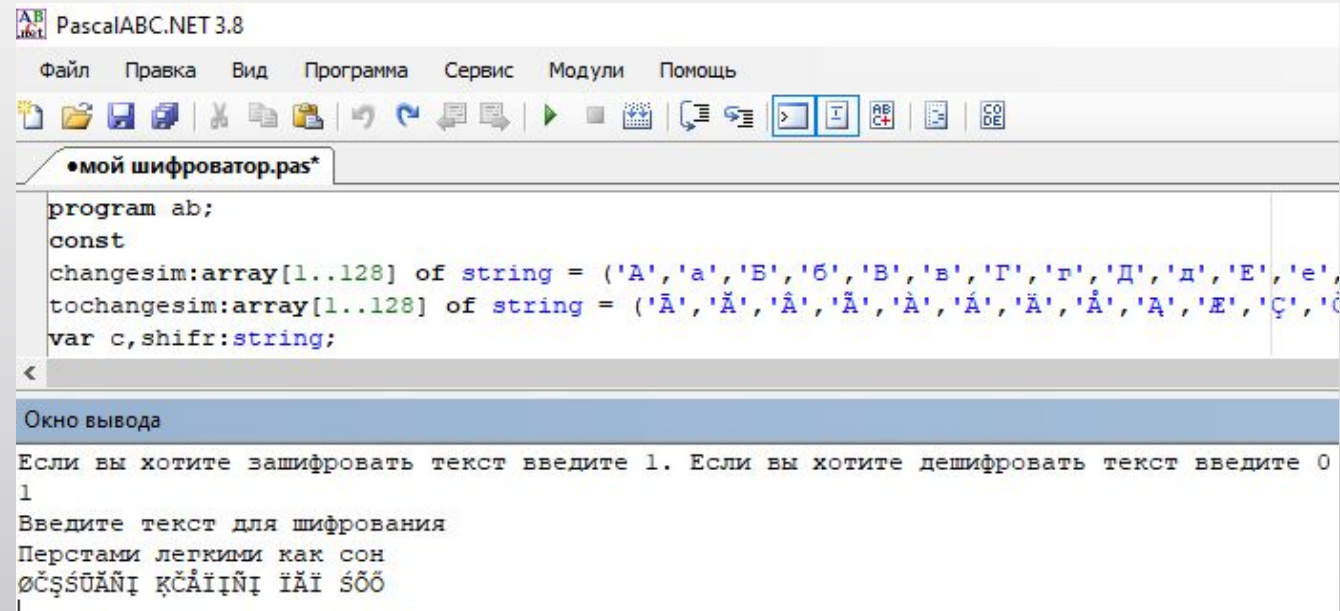




мой шифроватop.pas

```
program ab;
const
changesim:array[1..128] of string = ('A','a','B','б','B','b','Г','г','Д','д','E','e','Ё','ё','Ж','ж','З','з','И','и','Й','й','K','к','Л','л','M','м','H','h','O','o','П','п','P','p','C','c','T','т','V','v','Ф','ф','X','x','Ц','ц','Ч','ч');
tochangesim:array[1..128] of string = ('Ă','ă','Â','â','Ă','ă','Á','á','Ä','ä','Ж','ç','Ĉ','ĉ','Đ','đ','È','è','Ĝ','ĝ','Ĥ','ĥ','İ','i','Í','í','Î','î','I','I','Ķ','ĳ','Ń','ń','Ō','ó','Ŏ','ö','Ø','ø','Š','š','Š','š','T','t','Ū','ū','Ū','ú','Ū','ú','Ž','ž','Ž','ž','Œ','œ');
var c,shifr:string;
i,k:byte;
v,p:integer;
begin
  writeln('Если вы хотите зашифровать текст введите 1. Если вы хотите дешифровать текст введите 0');
  readln(v);
  if v=1 then
  begin
    writeln('Введите текст для шифрования');
    readln(c);
    for i:=1 to Length(c) do
    begin
      p:=0;
      for k:=1 to 128 do
      begin
        if c[i]=changesim[k] then
        begin
          shifr:=shifr+tochangesim[k];p:=1;
        end;
        if (p=0) and (k=128) then shifr:=shifr+c[i];
      end;
    end;
    writeln(shifr);
  end;
  if v=0 then
  begin
    writeln('Введите текст для дешифрования');
    readln(c);
    for i:=1 to Length(c) do
    begin
      p:=0;
      for k:=1 to 128 do
      begin
        if c[i]=tochangesim[k] then
        begin
          shifr:=shifr+changesim[k];p:=1;
        end;
        if (p=0) and (k=128) then shifr:=shifr+c[i];
      end;
    end;
    writeln(shifr);
  end;
end.
```


Пример работы программы

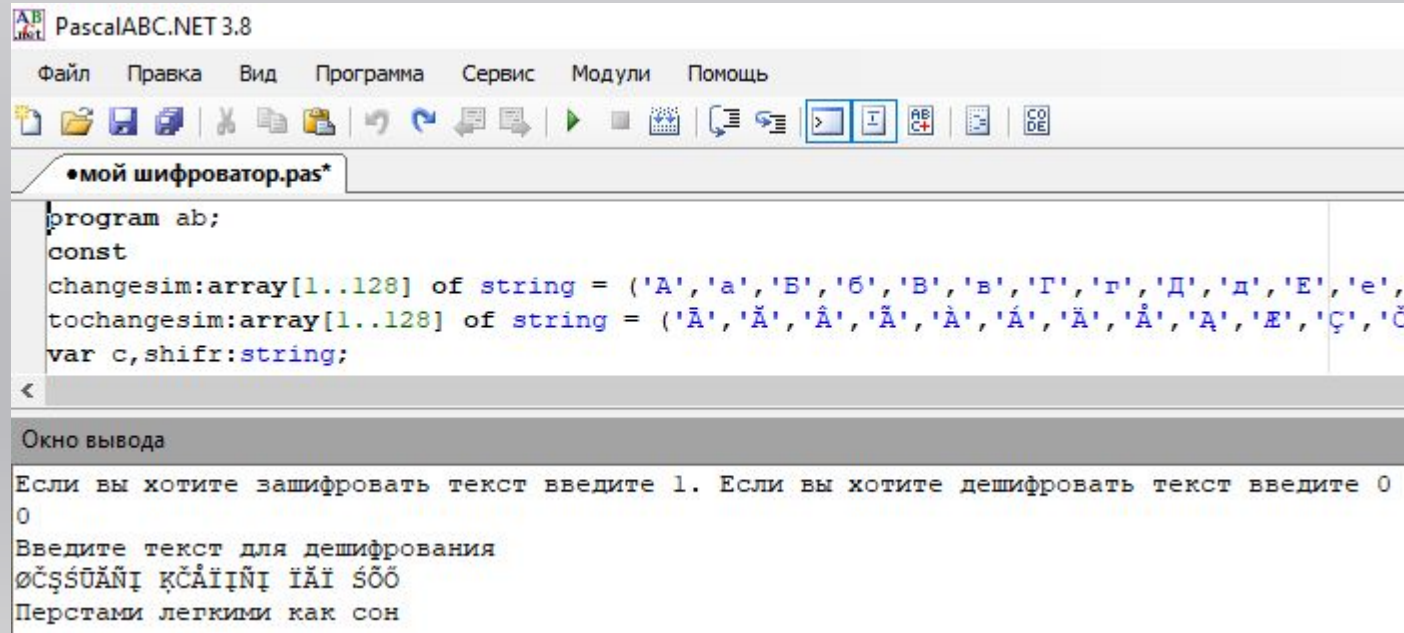


The screenshot shows the PascalABC.NET 3.8 IDE with a menu bar (Файл, Правка, Вид, Программа, Сервис, Модули, Помощь) and a toolbar. The main window displays a Pascal program named "мой шифроватор.pas" with the following code:

```
program ab;
const
changesim:array[1..128] of string = ('A','a','B','b','V','v','Г','г','Д','д','E','e',
tochangesim:array[1..128] of string = ('Ă','ă','Â','â','À','á','Ă','ă','Ą','ę','Ç','ç')
var c,shifr:string;
```

Below the code is an output window titled "Окно вывода" containing the following text:

```
Если вы хотите зашифровать текст введите 1. Если вы хотите дешифровать текст введите 0
1
Введите текст для шифрования
Перстами легкими как сон
øĈşşŪĂŃı ꞙĈĂİİŃı İĂİ şŌŌ
```

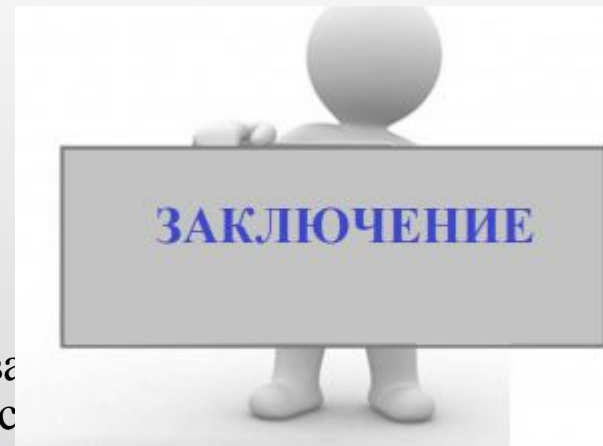


The screenshot shows the PascalABC.NET 3.8 IDE with the same menu bar and toolbar. The main window displays the same Pascal program as above. The output window titled "Окно вывода" contains the following text:

```
Если вы хотите зашифровать текст введите 1. Если вы хотите дешифровать текст введите 0
0
Введите текст для дешифрования
øĈşşŪĂŃı ꞙĈĂİİŃı İĂİ şŌŌ
Перстами легкими как сон
```

Заключение

- В процессе выполнения работы мне довелось узнать очень многое о шифровании, я написал свою программу для шифрования и дешифрования текста, создал свой шифр.
- В ходе проектной работы я выполнил все поставленные задачи:
- собрал информацию о различных способах шифрования текста
- разработал свой шифр
- написал программу для шифрования и дешифрования текста на языке Pascal
- Решил поставленную проблему, а именно решил какой шифр лучше использовать в программе – шифр подстановки.
- Выполнил цель продукта - написал программу для шифрования и дешифрования текста на языке Pascal.





**Спасибо
за
внимание !**