

А.А. Жирунов

Научный руководитель: канд. техн. наук, доц. Е.П. Догадина  
Муромский институт Владимирского государственного университета  
602264, г. Муром Владимирской обл., ул. Орловская, д.23  
E-mail: kaf-eivt@yandex.ru

### Приложения ОС Windows «Шифрование текста»

Темой исследовательской работы является создание приложения ОС Windows «Шифрование текста». Интерфейс программы включает главное окно, включающее следующие несколько элементов [1, 2]:

- а) Два многострочных поля для ввода исходного текста и вывода результата (должно работать в обе стороны);
- б) Маленькое поле, активируемое автоматически для некоторых видов шифрования с использованием кодового слова;
- с) Выпадающий список для выбора алгоритма шифрования (дешифрования) текста.

В программе используется несколько методов шифрования:

а) Самым простым шифром является *ШИФР С ЗАМЕНОЙ БУКВ ЦИФРАМИ*. Каждой букве соответствует число по алфавитному порядку  $A=1$ ,  $B=2$ ,  $C=3$  и т.д. Например, слово «TOWN» можно записать как «20 15 23 14», но особой секретности и сложности в дешифровке это не вызовет.

б) *ШИФР ЦЕЗАРЯ*. Известный шифр. Сутью данного шифра является замена одной буквы другой, находящейся на некоторое постоянное число позиций левее или правее от неё в алфавите. Гай Юлий Цезарь использовал этот способ шифрования при переписке со своими генералами для защиты военных сообщений. Этот шифр довольно легко взламывается, поэтому используется редко. Сдвиг на 4.  $A=E$ ,  $B=F$ ,  $C=G$ ,  $D=H$  и т.д. Пример шифра Цезаря: зашифруем слово «DEDUCTION». Получаем: *GHGXFWLRQ*. (сдвиг на 3)

с) *ШИФР АТБАШ*. Один из наиболее простых способов шифрования. Первая буква алфавита заменяется на последнюю, вторая – на предпоследнюю и т.д. Пример: «SCIENCE» = *HXRVMXV*

д) *ШИФР ГРОНСФЕЛЬДА*. По своему содержанию этот шифр включает в себя шифр Цезаря, однако в шифре Гронсфельда используется числовой ключ. Зашифруем слово «THALAMUS», используя в качестве ключа число 4123. Вписываем цифры числового ключа по порядку под каждой буквой слова. Цифра под буквой будет указывать на количество позиций, на которые нужно сдвинуть буквы.

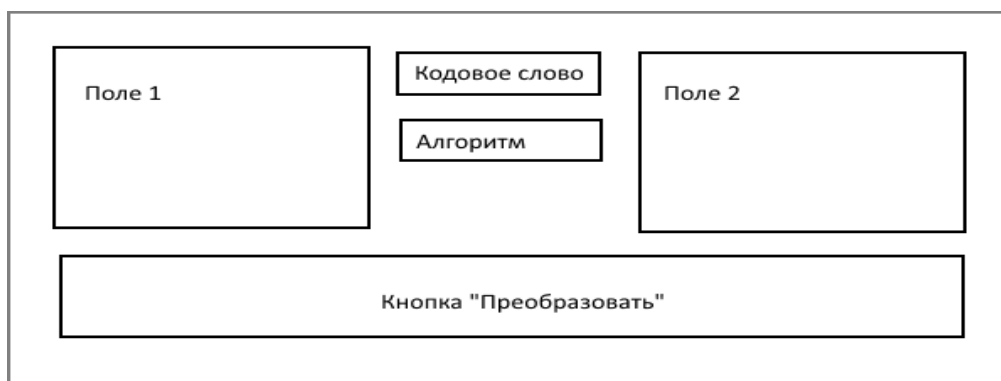


Рис.1. Интерфейс главного окна программы

### Литература

1. Архангельский А.Я. Работа с локальными базами данных в Delphi 7 – М.: ЗАО «Издательство БИНОМ», 2006.
2. Архангельский А.Я. Язык Pascal и основы программирования в Delphi. Учебное пособие – М.: ООО «Биноп-Пресс», 2004 – 496с.