МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования

«Тихоокеанский государственный университет»

Кафедра «Программное обеспечение вычислительной техники и автоматизированных систем»

Лабораторная работа №4

По предмету «Защита информации»

«Полиалфавитная подстановка»

Выполнил:

студент группы ПО(б) –81

Пшеничный Д. О.

Проверил:

Резак Е. В.

Хабаровск – 2022г.

**Цель:**

1. Реализовать зашифрование и расшифрование своей фамилии и имени.

2. В качестве ключа использовать свое отчество.

3. Алфавит – кириллица, матрица 4х8. В начале матрицы поставить ключ без повторяющихся символов, затем оставшийся алфавит.

4. Объединить символы «Ь» и «Ъ» в одну ячейку.

**Теория:**

**Полиалфавитная** подстановка использует несколько алфавитов шифртекста. Пусть используется k алфавитов.

Тогда открытый текст Х = X1X2 ... XkXk+1 ... X2kX2k+1... заменяется шифртекстом

Y = F1(X1)F2(X2)...Fk(Xk)Fk+1(Xk+1)...F2k(X2k)F2k+1(X2k+1),

где Fi(Xj) – символ шифртекста алфавита i для символа открытого текста Xj.

Полиграммная замена формируется из одного алфавита с помощью специальных правил.

**Ручной расчет:**

**Ключ:** «олегович»

**Исходный текст:** «пшеничный данил»

**Биграммы:** ПШ ЕН ИЧ НЫ ЙД АН ИЛ

**Матрица:**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| О | Л | Е | Г | В | И | Ч | А |
| Б | Д | Ё | Ж | З | Й | К | М |
| Н | П | Р | С | Т | У | Ф | Х |
| Ц | Ш | Щ | Ы | Ь | Э | Ю | Я |

**Порядок замен:**

ПШ находятся в одном столбце --> ШЛ

ЕН находятся в разных столбцах и строках --> ОР

ИЧ находятся в одной строке --> ЧА

НЫ находятся в разных столбцах и строках --> СЦ

ЙД находятся в одной строке --> КЁ

АН находятся в разных столбцах и строках --> ОХ

ИЛ находятся в одной строке --> ЧЕ

**Зашифрованный текст:** ШЛОРЧАСЦКЁОХЧЕ

**Скриншот работы программы:**

**Изображение выглядит как текст

Автоматически созданное описание**

**Расшифровка:**

ШЛ находятся в одном столбце --> ПШ

ОР находятся в разных столбцах и строках --> ЕН

ЧА находятся в одной строке --> ИЧ

СЦ находятся в разных столбцах и строках --> НЫ

КЁ находятся в одной строке --> ЙД

ОХ находятся в разных столбцах и строках --> АН

ЧЕ находятся в одной строке --> ИЛ

**Скриншот работы программы:**

**Изображение выглядит как текст

Автоматически созданное описание**

**Вывод:** в ходе выполнения лабораторной работы были изучены алгоритмы с использованием полиалфавитной подстановки.