Министерство образования и науки Российской Федерации

Федеральное государственное бюджетное образовательное учреждение высшего образования

«Пермский национальный исследовательский политехнический университет»

Электротехнический факультет

Кафедра «Информационные технологии и автоматизированные системы»

Направление 09.03.01 – «Информатика и вычислительная техника»

Дисциплина: «Защита информации»

Профиль: «Автоматизированные системы обработки информации и управления»

Семестр 7

ОТЧЕТ

по лабораторной работе №1

Тема: «Шифры перестановки и замены»

Выполнил: студент группы АСУ-15-1б

Цветков Д.В. \_\_\_\_\_\_\_\_\_\_\_

Проверил: доцент кафедры ИТАС

Шереметьев В. Г. \_\_\_\_\_\_\_\_\_\_\_

Дата \_\_\_\_\_\_

Пермь, 2018

**ЦЕЛЬ РАБОТЫ**

Получить практические навыки по применению шифров перестановки и шифров простой замены.

**ЗАДАНИЕ**

Реализовать шифрование текстового сообщения, используя любой нестандартный метод перестановки.

**ТЕОРЕТИЧЕСКИЕ СВЕДЕНИЯ**

При использовании шифра «Перевернутые группы» алгоритм шифрования заключается в следующем. Буквы в сообщении делятся на несколько групп (по 2, 4, 5 и т.д. символов). Далее после разбиения на группы, строку внутри каждой группы переворачивают.

Получившаяся криптограмма уже будет представляется бессмысленной комбинацией букв. При желании можно в определенном порядке переставить и группы. Например, так, чтобы последняя группа стала первой, предпоследняя — второй и так далее.

Однако следует обратить внимание на то, что после такой перестановки чтение этого текста от конца приводит к получению исходного сообщения. В результате несанкционированный пользователь может прочитать открытый текст, даже не зная шифра. Поэтому при практическом использовании данного шифра желательно переставлять группы так, чтобы не допускать подобных ошибок.

**ХОД РАБОТЫ**

Реализуем метод «Перевернутые группы». На рисунке 1 представлена программа для шифрования сообщения. Она имеет два входных поля: «Фраза для зашифровки» и «Кол-во символов в группе». С помощью регулярного выражения входная строка делится на группы, затем строка внутри каждой группы переворачивается.

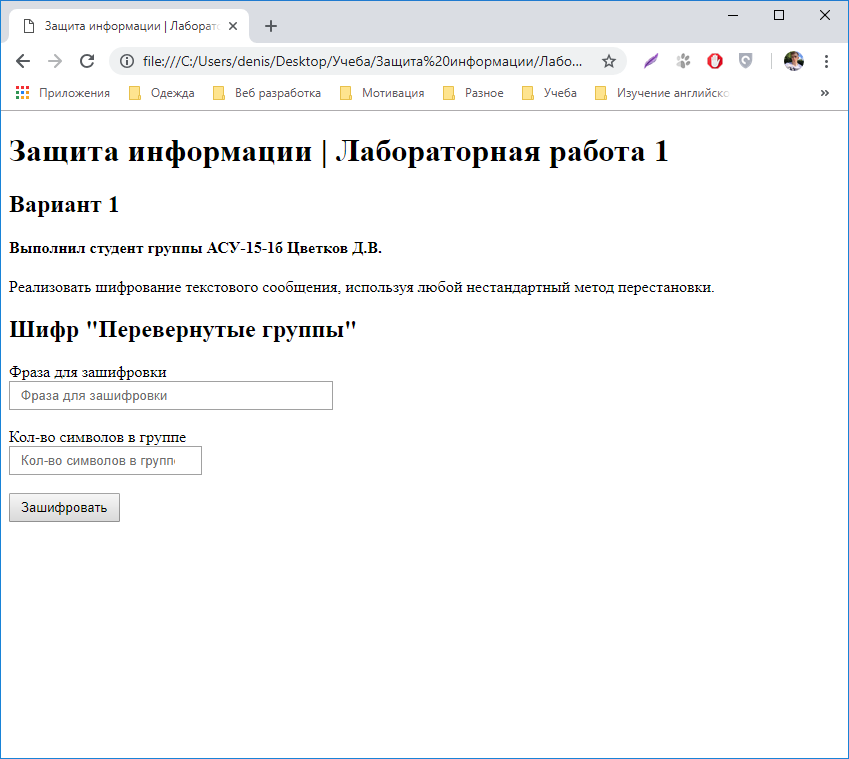


Рисунок 1 – Форма для шифрования.

Пример работы программы представлен на рисунке 2.

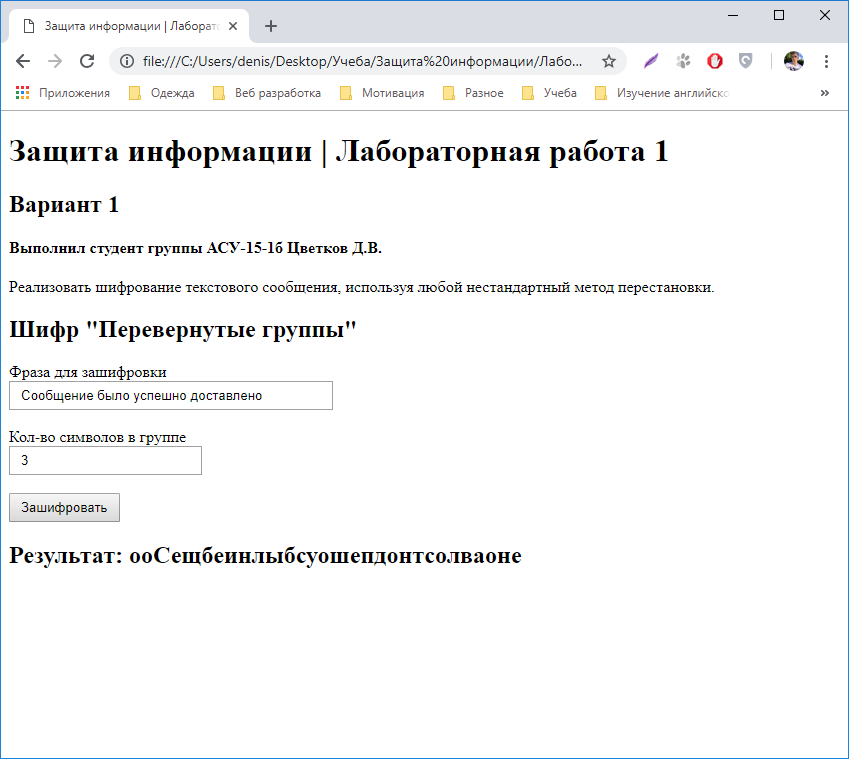


Рисунок 2 – Пример работы программы.

**ПРИЛОЖЕНИЕ А**

**Листинг программы**

$(function(){

function reverse(s){

return s.split("").reverse().join("");

}

function shareToGroups(text,param){

var reg = new RegExp('(.{1,'+param+'})', 'gim');

return text.match(reg);

}

$('#form-data>input[type=submit]').click(function(e){

e.preventDefault();

var text = $('#data').val().replace(/\s+/g, '');

var count\_symbols = $('#count-symbols').val();

arr = shareToGroups(text, count\_symbols) || '';

for(var i=0; i < arr.length; i++){

arr[i]=reverse(arr[i]);

}

var result = arr.join('');

$('#result').text('Результат: '+result);

});

});