# Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики

Кафедра информатики и прикладной математики

## Методы и средства защиты компьютерной информации

Моноалфавитные подстановки Лабораторная работа 2 Вариант 17

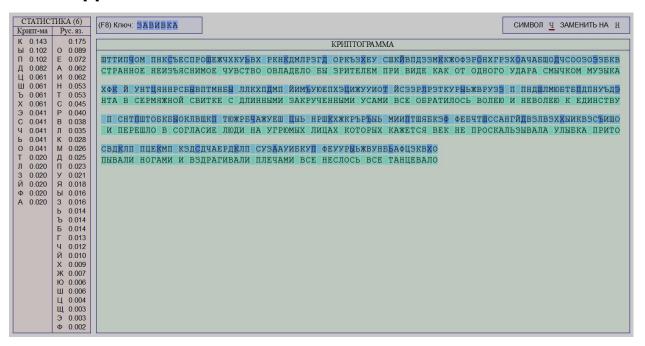


**Старался**: Шкаруба Н.Е. Группа: Р3418

# Цель работы:

Научиться методу шифрования и расшифровки текста методом полиалфавитных подстановок.

# Расшифрованный текст:

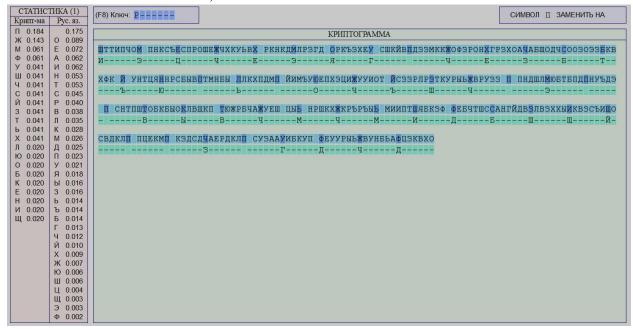


# Ключ

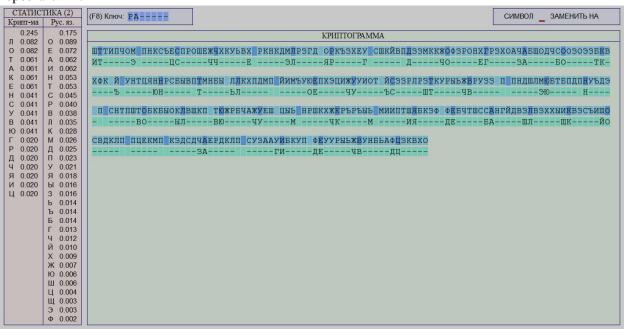
ЗАВИВКА

## Протокол криптоанализа:

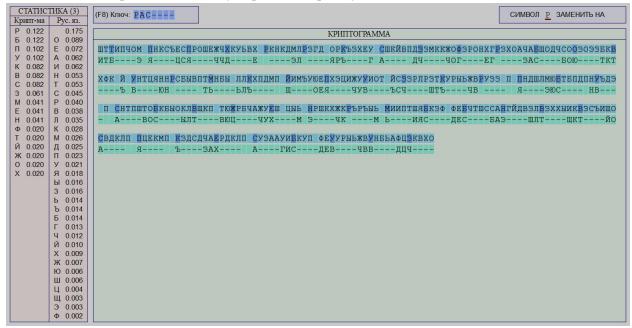
- 1) Прежде всего определяем период шифра. Для данной криптограммы UC = 0.0370, поэтому исходя из таблицы, длины ключа равны 3, 4 или 5. Предположим, длина ключа равна 4, ибо UC ближе к 0.0370 (4)
- 2) В общем, перебирая статистику больше часа во всевозможных длинах ключа, я обнаруживал, что у меня разницы между буквами криптограммы и русского языка были подозрительно маленькими, и не такими как в примере. Поэтому я решил попробовать всевозможные длины ключа.
- 3) Как оказалось, у ключа, состоящего из 7ми букв было что-то более-менее похожие на большие цифры в примере, хоть это и противоречило таблице (мой ключ 0.0370 не находится в диапазоне 0.0315, 0.0365). Решил играться с ним.
- 4) Пробуем заменить букву П на " ", расстояние между первой буквой и второй маленькое, с остальными большое. Если что, готов поменять



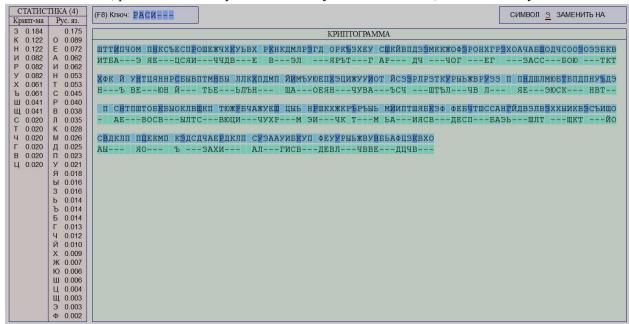
5) Заменяем " " на " ", рассояние между другими буквами кроме первой - большое, готов переставлять.



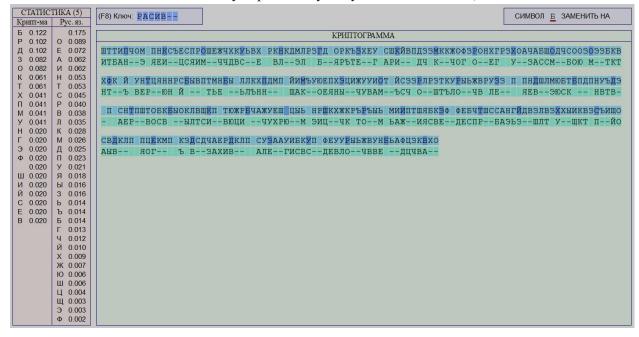
6) Заменяем Р на " ", расстояние между первой и второй буквой - никакое, готов заменить.



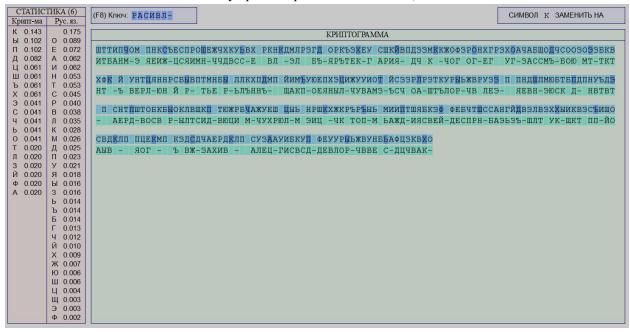
7) Заменяем 3 на " ", расстояние между остальными буквами - большое, изменять не думаю.



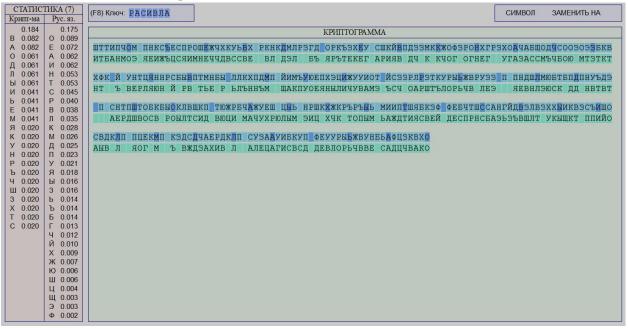
8) Заменяем Б на " ". Расстояние между первыми двумя буквами - маленькое, готов менять



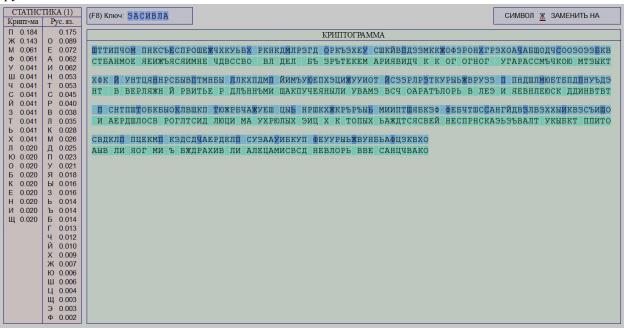
9) Заменяем К на " ". Расстояние между тремя первыми - маленькое, готов менять.



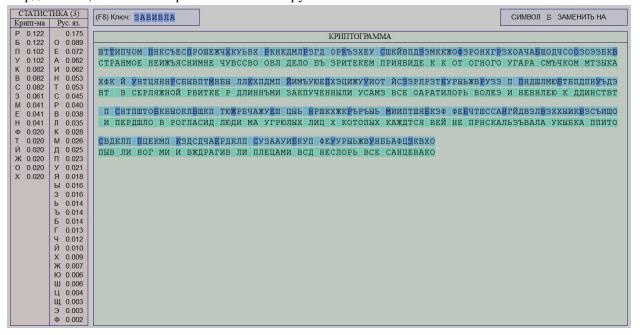
10) Наконец заменяем " " на " ", расстояние большое, оставляю



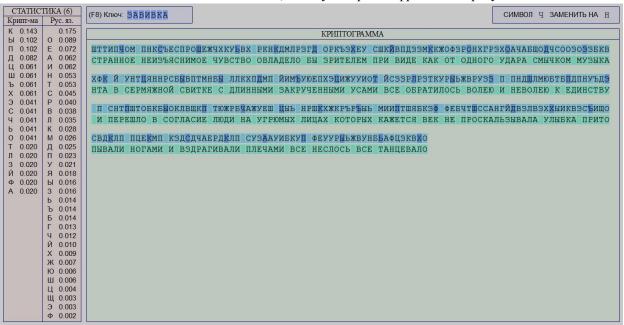
11) Меня смутил твердый знак и маленькое расстояние между буквами. Меняю в первой группе Ж на " "



12) Появилось ощущение, что я вижу что-то русское. Меня опять таки смутил ещё один твердый знак, и маленькое расстояние в 3ей группе. Меняю Б на " "



13) Ну вот уже и видно русские слова! Осталось немного поправить! Меняю СТРАНМОЕ на СТРАННОЕ - Ч на Н, и получаю расшифрованный результат



Спасибо за внимание!

Задание, если честно, не понравилось, потому что я просто бился в стену, уповая на ИС, и лишь чудо и интуиция вывели меня на решение!