# ЛАБОРАТОРНАЯ РАБОТА №5

Теория информационной безопасности и методология защиты информации

Выполнили: ст. гр. 4401 Галимов Э.Р.

Вариант № 3

Цель лабораторной работы:

Познакомиться с методом криптоанализа зашифрованных сообщений, основанного на анализе частотности символов. Реализовать программу дешифровки файла.

## ТЕКСТ ПРОГРАММЫ

<?php

main();

function main(){

$finalText='';

if(!isset($\_POST['text'])){

echo('<form method="POST">

<input type="textfield" name="text">

<input type="submit">

</form>');

}else{

$text=$\_POST['text'];

//алгоритм

$distribution=[' ','о','е','а','и','н','т','с','р','в','л','к','м','д','п','у','я','з','ы','б','г','ч','й','ь','х','ё','ж','ш','ю','ц','ъ','щ','э','ф'];

$mass=[];

$newSplitted=[];

$splitted = preg\_split('//u', $text, null, PREG\_SPLIT\_NO\_EMPTY);

foreach($splitted as $letter){

isset($mass[$letter]) ? $mass[$letter]=$mass[$letter]+1 : $mass[$letter]=1;

}

arsort($mass);

foreach($splitted as $key=>$letter){

$newSplitted[$key]['letter']=$letter;

$newSplitted[$key]['changed']=0;

}

$mass=array\_keys($mass);

for($i=0; $i<count($distribution); $i++){

foreach($newSplitted as &$value){

if ($value['letter']==$mass[$i] && !$value['changed']){

$value['letter']=$distribution[$i];

}

}

}

foreach($newSplitted as $letter){

$finalText=$finalText.$letter['letter'];

}

//алгоритм

echo $finalText;

}}