

ГУАП

КАФЕДРА № 33

ОТЧЕТ  
ЗАЩИЩЕН С ОЦЕНКОЙ  
ПРЕПОДАВАТЕЛЬ

канд. техн. наук, доцент

должность, уч. степень, звание

подпись, дата

В. А. Рындюк

ициалы, фамилия

ОТЧЕТ О ЛАБОРАТОРНОЙ РАБОТЕ

Лабораторная работа по криптографии №2

по курсу: Защита информации

РАБОТУ ВЫПОЛНИЛ

СТУДЕНТ гр. №

41313

подпись, дата

М. Д. Быстров

ициалы, фамилия

Санкт-Петербург 2026

## **Задание**

**ЗАДАНИЕ 1.** Осуществить шифровку текста (с проверкой) путем двойной перестановки строк и столбцов по ключевому слову.

### **Вариант 3.**

РАСШИФРОВКА ПРОЦЕСС ОБРАТНОГО ПРИМЕНЕНИЯ ШИФРА

Ключевое слово: БРИГАНТИНА

Число строк таблицы 8 и 10.

### **Выполнение задания**

Для выполнения шифровки необходимо рассчитать кол-во колонок в таблице, имея длину текста и кол-во строк, а затем заполнить таблицу по колонкам. Далее переместить местами столбцы и строки в соответствии с ключевыми словами, и взять зашифрованное сообщение построчно.

Для расшифровки необходимо так же рассчитать кол-во колонок, построчно заполнить таблицу и произвести обратные перестановки, после чего прочитать исходное сообщение из колонок.

1. Число строк –8:

Исходное

сообщение:

РАСШИФРОВКА\_ПРОЦЕСС\_ОБРАТНОГО\_ПРИМЕНЕНИЯ\_ШИФРА

ПАРАМЕТРЫ: 8 строк, 6 столбцов, Ключ: БРИГАНТИНА

[ ИСХОДНАЯ ТАБЛИЦА (ЗАПОЛНЕНА ПО СТОЛБЦАМ) ]

Ключевая последовательность: Б Р И Г А Н

---

Р	В	Е	Т	И	–
А	К	С	Н	М	Ш
С	А	С	О	Е	И
Ш	–	–	Г	Н	Ф
И	П	О	О	Е	Р
Ф	Р	Б	–	Н	А
Р	О	Р	П	И	–
О	Ц	А	Р	Я	–

Ключ строки: БРИГАНТИ

[ ПОСЛЕ ПЕРЕСТАНОВКИ СТОЛБЦОВ ]

Ключевая последовательность: А Б Г И Н Р

---

И Р Т Е \_ В  
М А Н С Ш К  
Е С О С И А  
Н Ш Г \_ Ф \_  
Е И О О Р П  
Н Ф \_ Б А Р  
И Р П Р - О  
Я О Р А - Ц

[ ФИНАЛЬНАЯ ТАБЛИЦА (ПОСЛЕ ПЕРЕСТАНОВКИ СТРОК) ]

Ключевая последовательность: А Б Г И И Н Р Т

---

Е И О О Р П  
И Р Т Е \_ В  
Н Ш Г \_ Ф \_  
Е С О С И А  
Я О Р А - Ц  
Н Ф \_ Б А Р  
М А Н С Ш К  
И Р П Р - О

Зашифрованный текст: ЕИООРПИРТЕ\_ВНШГ\_Ф\_ЕСОСИАЯРА-  
ЦНФ\_БАРМАНСШКИРПР-О

[ ТАБЛИЦА ПОСЛЕ ОБРАТНЫХ ПЕРЕСТАНОВОК ]

Ключевая последовательность: Б Р И Г А Н

---

Р В Е Т И \_  
А К С Н М Ш  
С А С О Е И  
Ш \_ \_ Г Н Ф  
И П О О Е Р  
Ф Р Б \_ Н А

Р О Р П И -  
О Ц А Р Я -

Ключ строки: БРИГАНТИ

Расшифрованный текст:  
РАСШИФРОВКА\_ПРОЦЕСС\_ОБРАТНОГО\_ПРИМЕНЕНИЯ\_ШИФРА--

2. Число строк – 10.

Исходное сообщение:  
РАСШИФРОВКА\_ПРОЦЕСС\_ОБРАТНОГО\_ПРИМЕНЕНИЯ\_ШИФРА  
ПАРАМЕТРЫ: 10 строк, 5 столбцов, Ключ: БРИГАНТИНА

[ ИСХОДНАЯ ТАБЛИЦА (ЗАПОЛНЕНА ПО СТОЛБЦАМ) ]

Ключевая последовательность: Б Р И Г А

-----  
Р А О П \_  
А \_ Б Р Ш  
С П Р И И  
Ш Р А М Ф  
И О Т Е Р  
Ф Ц Н Н А  
Р Е О Е -  
О С Г Н -  
В С О И -  
К \_ \_ Я -

Ключ строки: БРИГАНТИНА

[ ПОСЛЕ ПЕРЕСТАНОВКИ СТОЛБЦОВ ]  
Ключевая последовательность: А Б Г И Р

-----  
\_ Р П О А  
Ш А Р Б \_  
И С И Р П  
Ф Ш М А Р

P	I	E	T	O
A	Φ	H	H	Ц
-	R	E	O	E
-	O	H	G	C
-	B	I	O	C
-	K	Я	-	-

[ ФИНАЛЬНАЯ ТАБЛИЦА (ПОСЛЕ ПЕРЕСТАНОВКИ СТРОК) ]

Ключевая последовательность: А А Б Г И И Н Н Р Т

---

P	I	E	T	O
-	K	Я	-	-
-	R	П	O	A
Φ	Ш	M	A	R
I	C	И	R	П
-	O	H	G	C
A	Φ	H	H	Ц
-	B	I	O	C
Ш	A	R	Б	-
-	R	E	O	E

Зашифрованный текст: РИЕТО-КЯ РПОАФШМАРИСИРП-ОНГСАФННЦ-  
ВИОСШАРБ\_РЕОЕ

[ ТАБЛИЦА ПОСЛЕ ОБРАТНЫХ ПЕРЕСТАНОВОК ]

Ключевая последовательность: Б Р И Г А

---

P	A	O	П	-
A	-	Б	R	Ш
C	П	R	И	И
Ш	R	A	M	Ф
И	O	T	E	Р
Φ	Ц	H	H	А
P	E	O	E	-

О	С	Г	Н	-
В	С	О	И	-
К	-	-	Я	-

## Ключ строки: БРИГАНТИНА

Расшифрованный текст (по столбцам):

**РАСШИФРОВКА ПРОЦЕСС ОБРАТНОГО ПРИМЕНЕНИЯ ШИФРА----**

**ЗАДАНИЕ 2.** Осуществить шифровку текста (с проверкой), используя два возможных варианта магических квадратов, приведенных ниже.

Таблица 2.8

32	30	18	4	16	11
15	28	14	12	8	34
13	7	19	29	17	26
23	1	5	20	27	35
6	36	31	25	10	3
22	9	24	21	33	2
16	33	5	23	8	26
15	34	24	6	25	7
20	1	27	9	36	18
19	2	28	10	35	17
30	12	13	31	3	22
11	29	14	32	4	21

Ниже приведены варианты задания по шифровке текста.

### **Вариант 3.**

## Исходный текст:

<i>Л</i>	<i>О</i>	<i>Г</i>	<i>И</i>	<i>Ч</i>	<i>Е</i>	<i>С</i>	<i>К</i>	<i>И</i>	<i>Й</i>	*	<i>Т</i>	<i>И</i>	<i>П</i>	*	<i>Д</i>	<i>А</i>	<i>Н</i>	<i>Ы</i>	<i>Х</i>	*
<b><i>В</i></b>	*	<i>О</i>	<i>В</i>	<i>Ј</i>	<i>Е</i>	<i>С</i>	<b><i>Т</i></b>	*	<i>P</i>	<i>A</i>	<i>S</i>	<i>C</i>	<i>A</i>	<b><i>L</i></b>						

## Выполнение задания

Для выполнения задания необходимо вписать исходный текст в заданный магический квадрат в ячейки, числа в которых соответствуют порядковому номеру символов в исходном тексте, для получения шифротекста выписать текст из квадрата построчно.

Обратная операция: построчно вписать текст в квадрат, выписать символы в порядке, соответствующем числам магического квадрата – в результате получим исходное сообщение.

## 1. Первый магический квадрат

--- Магический квадрат ---

32		30		18		4		16		11
15		28		14		12		8		34

13		7		19		29		17		26
23		1		5		20		27		35
6		36		31		25		10		3
22		9		24		21		33		2

Исходный текст: 'ЛОГИЧЕСКИЙ\*ТИП\*ДАНЫХ\*В\*ОБЪЕКТ\*PASCAL'

Текст после обработки: 'ЛОГИЧЕСКИЙ\*ТИП\*ДАНЫХ\*В\*ОБЪЕКТ\*PASCAL'

Длина текста: 36

--- Матрица с вставленными символами ---

A		*		Н		И		Д		*
*		C		П		Т		К		С
И		С		ы		т		А		Ј
*		Л		Ч		Х		Е		А
E		L		P		В		Й		Г
B		И		0		*		S		0

Зашифрованный текст: 'А\*НИД\*\*СПТКСИСЫТАЈ\*ЛЧХЕАЕLPВИГВИО\*SO'

--- Матрица дешифровки ---

A		*		Н		И		Д		*
*		C		П		Т		К		С
И		С		ы		т		А		Ј
*		Л		Ч		Х		Е		А
E		L		P		В		Й		Г
B		И		0		*		S		0

Расшифрованный текст: 'ЛОГИЧЕСКИЙ\*ТИП\*ДАНЫХ\*В\*ОБЪЕКТ\*PASCAL'

## 2. Второй магический квадрат

--- Магический квадрат ---

16		33		5		23		8		26
15		34		24		6		25		7
20		1		27		9		36		18

19		2		28		10		35		17
30		12		13		31		3		22
11		29		14		32		4		21

Исходный текст: 'ЛОГИЧЕСКИЙ\*ТИП\*ДАНЫХ\*В\*ОБЪЕКТ\*PASCAL'

Текст после обработки: 'ЛОГИЧЕСКИЙ\*ТИП\*ДАНЫХ\*В\*ОБЪЕКТ\*PASCAL'

Длина текста: 36

--- Матрица с вставленными символами (Шифрование) ---

Д		S		Ч		*		К		Ј
*		C		О		E		B		C
X		L		E		I		L		H
Y		O		C		Й		A		A
*		T		И		R		G		B
*		T		П		A		I		*

Зашифрованный текст: 'ДСЧ\*КЈ\*СОЕВСХЛЕИЛНЫОСЈАА\*ТИРГВ\*ТПАИ\*'

--- Матрица дешифровки (заполнена построчно) ---

Д		S		Ч		*		К		Ј
*		C		О		E		B		C
X		L		E		I		L		H
Y		O		C		Й		A		A
*		T		И		R		G		B
*		T		П		A		I		*

Расшифрованный текст: 'ЛОГИЧЕСКИЙ\*ТИП\*ДАНЫХ\*В\*ОБЪЕКТ\*PASCAL'

**ЗАДАНИЕ 3.** Осуществить шифровку текста (с проверкой), воспользовавшись методом многоалфавитной замены. Ниже приведены варианты ключевых слов и заданий по шифровке текста.

### Вариант 3.

Исходный текст:

T	H	G	P	Z	B	E	P	Ь	В	E	C	Ь	M	A	Ч	И	С	Т	О	П	Л	
O	T	H	Ы	Й																		

Варианты ключевых слов:

### Выполнение задания.

На первом этапе необходимо сопоставить исходный либо зашифрованный текст зацикленному ключевому слову посимвольно.

Для шифровки/десифровки необходимо воспользоваться таблицей шифра:

А	Б	В	Г	Д	Е	Ж	З	И	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ь	Ы	Ѣ	Э	Ю	Я																															
А	А	Б	В	Г	Д	Е	Ж	З	И	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ь	Ы	Ѣ	Э	Ю	Я																														
Б	Я	А	Б	В	Г	Д	Е	Ж	З	И	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ь	Ы	Ѣ	Э	Ю	Я																													
В	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ь	Ы	Ѣ	Э	Ю	Я																												
Г	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ь	Ы	Ѣ	Э	Ю	Я																											
Д	Ѣ	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ь	Ы	Ѣ	Э	Ю	Я																										
Е	Ы	Ѣ	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ь	Ы	Ѣ	Э	Ю	Я																									
Ж	Ь	Ы	Ѣ	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ь	Ы	Ѣ	Э	Ю	Я																								
З	Щ	Ь	Ы	Ѣ	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ь	Ы	Ѣ	Э	Ю	Я																							
И	Ш	Щ	Ь	Ы	Ѣ	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ь	Ы	Ѣ	Э	Ю	Я																						
К	Ч	Щ	Щ	Ь	Ы	Ѣ	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ь	Ы	Ѣ	Э	Ю	Я																					
Л	Ц	Ч	Щ	Щ	Ь	Ы	Ѣ	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ь	Ы	Ѣ	Э	Ю	Я																				
М	Х	Ц	Ч	Щ	Щ	Ь	Ы	Ѣ	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ь	Ы	Ѣ	Э	Ю	Я																			
Н	Ф	Х	Ц	Ч	Щ	Щ	Ь	Ы	Ѣ	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ь	Ы	Ѣ	Э	Ю	Я																		
О	У	Ф	Х	Ц	Ч	Щ	Щ	Ь	Ы	Ѣ	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ь	Ы	Ѣ	Э	Ю	Я																	
П	Т	У	Ф	Х	Ц	Ч	Щ	Щ	Ь	Ы	Ѣ	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ь	Ы	Ѣ	Э	Ю	Я																
Р	С	Т	У	Ф	Х	Ц	Ч	Щ	Щ	Ь	Ы	Ѣ	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ь	Ы	Ѣ	Э	Ю	Я															
С	Р	С	Т	У	Ф	Х	Ц	Ч	Щ	Щ	Ь	Ы	Ѣ	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ь	Ы	Ѣ	Э	Ю	Я														
Т	П	Р	С	Т	У	Ф	Х	Ц	Ч	Щ	Щ	Ь	Ы	Ѣ	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ь	Ы	Ѣ	Э	Ю	Я													
У	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Щ	Щ	Ь	Ы	Ѣ	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ь	Ы	Ѣ	Э	Ю	Я												
Ф	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Щ	Щ	Ь	Ы	Ѣ	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ь	Ы	Ѣ	Э	Ю	Я											
Х	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Щ	Щ	Ь	Ы	Ѣ	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ь	Ы	Ѣ	Э	Ю	Я										
Ц	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Щ	Щ	Ь	Ы	Ѣ	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ь	Ы	Ѣ	Э	Ю	Я									
Ч	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Щ	Щ	Ь	Ы	Ѣ	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ь	Ы	Ѣ	Э	Ю	Я								
Ш	И	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Щ	Щ	Ь	Ы	Ѣ	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ь	Ы	Ѣ	Э	Ю	Я							
Щ	З	И	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Щ	Щ	Ь	Ы	Ѣ	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ь	Ы	Ѣ	Э	Ю	Я						
ь	Ж	З	И	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Щ	Щ	Ь	Ы	Ѣ	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ь	Ы	Ѣ	Э	Ю	Я					
ы	Е	Ж	З	И	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Щ	Щ	Ь	Ы	Ѣ	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ь	Ы	Ѣ	Э	Ю	Я				
ъ	Д	Е	Ж	З	И	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Щ	Щ	Ь	Ы	Ѣ	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ь	Ы	Ѣ	Э	Ю	Я			
Э	Г	Д	Е	Ж	З	И	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Щ	Щ	Ь	Ы	Ѣ	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ь	Ы	Ѣ	Э	Ю	Я		
ю	В	Г	Д	Е	Ж	З	И	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Щ	Щ	Ь	Ы	Ѣ	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ь	Ы	Ѣ	Э	Ю	Я	
я	Б	В	Г	Д	Е	Ж	З	И	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Щ	Щ	Ь	Ы	Ѣ	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ь	Ы	Ѣ	Э	Ю	Я

В таблице по строкам (в левой колонке) ищется буква ключевого слова, по колонкам (в верхней строке) – буква шифруемого текста. На пересечении индексов найденных букв находится буква, на которую необходимо произвести замену в исходном тексте.

Для расшифровки текста необходимо также определить строку для поиска по букве ключевого слова, в этой строке найти символ из зашифрованного текста, в первом элементе колонки которого будет символ исходного текста.

## 1. Ключевое слово КОШКА

Исходный текст:	ТИГРЗВЕРЬВЕСЬМАЧИСТОПЛОТНЫЙ
Ключевое слово:	кошакошкакошкакошкако
Шифр:	иымжзшшсвъгвваоышиоэцнты
Расшифровка:	тигрзверъвесъмачистоплотныи

## 2. Ключевое слово ПРЫЖОК

Исходный текст:	ТИГРЗВЕРЬВЕСЬМАЧИСТОПЛОТНЫЙ
Ключевое слово:	прыжокпрыжокпрыжокпры
Шифр:	гщикъщаяъшэмъесызгюфдаиумо
Расшифровка:	тигрзверъвесъмачистоплотныи

**ЗАДАНИЕ 4.** Шифровка текста на русском языке произведена с использованием шифра двойной замены. Осуществить дешифрацию текста, приведенного ниже, если известно, что шифровальная таблица имеет размерность 6х6. Ниже приведены варианты шифротекста.

### Вариант 3.

Шифр: итоеонч.аист.скдкрянившстргесусепевуриииилтнсгтгии  
Ключевое слово: **БРИГАНТИНА, БАТАРЕЯ или ТРОТУАР**  
Размерность таблицы 7x7

Размерность таблицы 7x7

### Выполнение задания.

Ключевое слово найдено перебором: **ТРОТУАР**.

Ход расшифровки:

[ТАБЛИЦА ДЛЯ РАСШИФРОВКИ ]

Ключевая последовательность: А О Р Р Т Т У

-----  
И Т О Е О Н Ч  
. А И С Т . С  
К Д К Р Я Н И  
В В С Т Р Г Е  
С У С Е П Е В  
У Р И И И Л Т

Н С Г Т Г И И

[ ТАБЛИЦА ПОСЛЕ ОБРАТНЫХ ПЕРЕСТАНОВОК ]

Ключевая последовательность: Т Р О Т У А Р

п с у е в с е  
я к д н и к р  
т и а . с . с  
и и р л т у и  
г г с и и н т  
о о т н ч и е  
р с в г е в т

Ключ строки: ТРОТУАР

РАСШИФРОВАННЫЙ ТЕКСТ  
**пятигорскиигосударствен.лингвистическ.университет**

(по столбцам):

**ЗАДАНИЕ 5.** Осуществить криптоанализ шифровки. Предполагается, что шифровка текста произведена одним из шести нижеперечисленных вариантов магического квадрата размерностью 6x6. Ниже приведены варианты задания по криптоанализу текста Таблица 2.9.1 – 29.6.

Таблица 2.9.1

32	30	18	4	16	11
15	28	14	12	8	34
13	7	19	29	17	26
23	1	5	20	27	35
6	36	31	25	10	3
22	9	24	21	33	2

Таблица 2.9.2.

16	33	5	23	8	26
15	34	24	6	25	7
20	1	27	9	36	18
19	2	28	10	35	17
30	12	13	31	3	22
11	29	14	32	4	21

Таблица 2.9.3.

7	33	3	20	31	17
21	14	8	1	35	32
30	25	34	5	2	15
16	23	29	27	6	10
24	12	9	36	11	19
13	4	28	22	26	18

Таблица 2..94.

12	29	13	31	4	22
11	30	32	14	21	3
20	1	27	9	36	18
19	2	28	10	35	17
34	16	5	23	7	26
15	33	6	24	8	25

Таблица 2.9.5

31	9	2	22	27	20
3	32	7	21	23	25
35	1	6	26	19	24
4	36	29	13	18	11
30	5	34	12	14	16
8	28	33	17	10	15

Таблица 2.9.6.

29	7	6	20	25	24
9	32	1	27	23	19
31	3	8	22	21	26
2	34	33	11	16	15
36	5	28	18	14	10
4	30	35	13	12	17

### Вариант 3.

Возможные варианты магических квадратов: 1,2 или 3.

Перехваченный шифр текста:

**еиобтедвя-нэтпсомаелчтылсчттоеоаолхт**

### **Выполнение задания.**

Перебором найден подходящий магический квадрат – это квадрат номер 2.

Ход расшифровки:

--- Магический квадрат ---

16		33		5		23		8		26
15		34		24		6		25		7
20		1		27		9		36		18
19		2		28		10		35		17
30		12		13		31		3		22
11		29		14		32		4		21

--- Матрица дешифровки (заполнена построчно) ---

е		и		о		б		т		е
д		в		я		-		н		з
т		п		с		о		м		а
е		л		ч		т		ы		л
с		ч		т		т		о		е
о		а		о		л		х		т

Расшифрованный текст: 'плохо-этото что делает тебя несчастливым'

**ЗАДАНИЕ 6.** Осуществить криптоанализ шифровки. Предполагается, что шифровка текста произведена методом многоалфавитной замены. Ниже приведены варианты задания по криптоанализу текста и возможные варианты ключевых слов.

### **Вариант 3.**

Возможные варианты ключевых слов:  
ШУЛЕР, ВОПРОС, ПАРОЛЬ

Перехваченный шифр текста:  
ЫЬЩСЮХЛУЗЩАЛЬОТЬГД

### **Выполнение задания:**

Подбором найдено ключевое слово – «ПАРОЛЬ»

Ход расшифровки:

Ключевое слово:                   вопросвопросвопросво

Шифр:                                ЫЬЩСЮХЛУЗЩАЛЬОТЬГД

Расшифровка:

**экзаменационный билет**

## **Вывод**

В ходе выполнения второй лабораторной работы были получены навыки применения на практике шифра двойной перестановки с ключевым словом, шифра магическим квадратом и шифра многоалфавитной замены.

Произведено шифрование текста различными шифрами в соответствии с вариантом.

Произведен подбор параметров шифров для расшифровки исходного сообщения.