РОСЖЕЛДОР

Федеральное государственное бюджетное образовательное учреждение высшего образования
«Ростовский государственный университет путей сообщения»
(ФГБОУ ВО РГУПС)

В.В. Доманский, А.В. Чернов

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ И ЗАЩИТА ИНФОРМАЦИИ

Практикум

Ростов-на-Дону
2016

УДК 681.3.06(07) + 06

Рецензент – кандидат технических наук, доцент В.В. Ильичева

Доманский, В.В.

Информационная безопасность и защита информации: практикум / В.В. Доманский, А.В. Чернов; ФГБОУ ВО РГУПС. – Ростов н/Д, 2016. – 44 с.: ил. – Библиогр.: с. 41.

В пособии в систематизированном виде изложены основные сведения и описание криптографических методов защиты информации. Подробно описаны и разобраны на примерах отдельные виды симметричных и асимметричных шифров.

Приведены лабораторные и практические работы, дополняющие курс «Информационная безопасность и защита информации», индивидуальные задания для самостоятельной работы.

Предназначено для студентов 3-го курса, аспирантов, преподавателей, а также широкого круга читателей, интересующихся вопросами информационной безопасности.

Соответствует государственным образовательным стандартам по специальностям «Сервис», «Туризм».

Одобрено к изданию кафедрой «Информатика».

Лабораторная работа № 1

Тема: Шифр простой замены. Пример создания программного кода, зашифровывающего и расшифровывающего сообщение по алгоритму шифра простой замены.

Задача. Создать программный код зашифровывающий, а затем расшифровывающий предложение, записанное на русском языке. Использовать шифр простой замены, в котором каждая буква русского алфавита заменяется другой буквой этого же алфавита. При этом замена осуществляется по правилу: первая буква заменяется последней, вторая – предпоследней и т.д. Так, А заменяется на Я, Б – на Ю, В – на Э и т. д.

Формализация задачи. Решение поставленной задачи сводится к замене букв исходного текста (алфавит по порядку) буквами алфавита, записанного в обратном порядке. *Исходные данные*: буквы русского алфавита, записанные в алфавитном порядке за исключением буквы Ё, буквы русского алфавита за исключением буквы Ё, выписанные в обратном порядке. Шифруемое сообщение: «простая замена – один из самых древних шифров». *Выходные данные:* сообщение до его шифровки, после шифровки и после расшифровки.

Разработка алгоритма. Для решения поставленной задачи определяем количество символов преобразуемой строки. Образуем новую строку по длине равную исходной строке. Далее организуем цикл, в котором просматриваем все символы преобразуемой строки, определяем позицию номер k этого символа в исходном алфавите. Если в исходном алфавите символ не найден, то в данную позицию новой строки заносим этот символ без изменений, в противном случае в данную позицию новой строки заносим символ из нового алфавита, позиция которого совпадает с позицией номер k исходного алфавита.

Реализация алгоритма на ЭВМ. Создадим программный код.

1 Запустите программу Microsoft Excel (Пуск – Все Программы – Microsoft Office Excel 2013).
2 Лист 1 рабочей книги Excel переименуйте. Назовите Лаб. раб. № 1.
3 Нажмите Alt-F11. Откроется окно редактирования VBA.
4 В редакторе VBA выполнить команду Insert/Module.
5 В стандартном модуле VBA поместить следующий код программы.

```
Private n As Long
'исходный алфавит
Const АБВ As String = "абвгдежзийклмнопрстуфхцчшщъыьэюя"
'новый алфавит
Const НовАБВ As String = "яюэьыъщшчцхфутсрпонмлкйизжедгвба"
Private Sub AnotherCipher()
Dim STR As String, strT As String, strR As String
‘строка которую будем зашифровывать
STR = "Простая замена один из самых древних шифров"
‘ переход к нижнему регистру
STR = LCase(STR)
‘печать в окно Immediate
Debug.Print STR
' шифровка
```

```
Decode STR, strR, АБВ, НовАБВ
Debug.Print strR
'расшифровка
Decode strR, strT, НовАБВ, АБВ
Debug.Print strT
End Sub

Private Sub Decode(STR, STRS, Oldkey, NewKey)
Dim n As Long, i As Long
Dim tmp As String
'определяем количество символов исходной строки
n = Len(STR)
'вводим преобразованную строку, состоящую из n пробелов
STRS = Space(n)
For i = 1 To n
'выделяем один символ исходной строки
tmp = Mid(STR, i, 1)
'определяем место символа исходной строки в исходном алфавите
k = InStr(1, Oldkey, tmp)
If k = 0 Then
'если в исходном алфавите такого символа нет
'то переносим его в новую строку не изменяя
Mid(STRS, i, 1) = tmp
Else
'заменяем соответствующий пробел на символ нового алфавита
Mid(STRS, i, 1) = Mid(NewKey, k, 1)
End If
Next i
End Sub
```

6 В программе применяется объект Debug, который представляет собой отладчик и позволяет выводить промежуточные значения (с помощью метода Print) в окно Immediate. Это окно отражается на экране выбором команды View/ Immediate Window и используется при отладке программ.

7 Синтаксис функций обработки строковых выражений приведен в Приложении табл. 1.

8 Выполнить команду Debug/Compile VBA. Отобразить окно Immediate с помощью команды View/ Immediate Window.

9 Для того чтобы проверить, как работает созданная программа, поместите курсор в поле кода подпрограммы `AnotherCipher`, нажмите клавишу F5 или выберите команду RUN/RUN SUB/USERFORM.

10 Результатом работы данной программы будет вывод в окно Immediate сообщения до его шифровки, после шифровки и после расшифровки рис. 1.

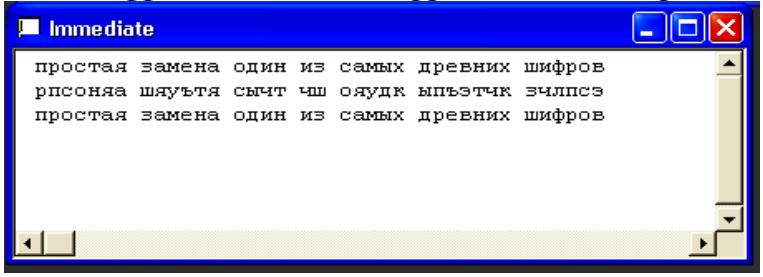

Рис. 1

Индивидуальные задания по лабораторной работе № 1

Варианты заданий приведены в табл. 1 и табл. 2. Уровень сложности заданий табл. 2 значительно выше.

Правильность работы шифраторов проверить: используя отладчик Debug, позволяющий выводить промежуточные значения (с помощью метода Print) в окно Immediate. Вывести в окно Immediate сообщения до его шифровки, после шифровки и после расшифровки.

Таблица 1

Создание программного кода шифра замены по правилу

<table>
<tr><th>№</th><th>Правило замены</th></tr>
<tr><td>0</td><td>Гласные буквы русского алфавита не изменяются. Первый десяток согласных заменяется на второй десяток согласных (второй – на первый) по следующей таблице:
<table>
<tr><td>Б</td><td>В</td><td>Г</td><td>Д</td><td>Ж</td><td>З</td><td>К</td><td>Л</td><td>М</td><td>Н</td></tr>
<tr><td>Щ</td><td>Ш</td><td>Ч</td><td>Ц</td><td>Х</td><td>Ф</td><td>Т</td><td>С</td><td>Р</td><td>П</td></tr>
</table>
(шифр типа масонской замены – «простая литорея»)</td></tr>
<tr><td>1</td><td>Заменить буквы сообщения, составленного на русском языке, согласно лозунговому шифру используя лозунг «право»</td></tr>
<tr><td>2</td><td>Заменить буквы сообщения, составленного на русском языке согласно шифру «Альбам»</td></tr>
<tr><td>3</td><td>Заменить буквы сообщения, составленного на русском языке согласно лозунговому шифру с лозунгом «зерно»</td></tr>
<tr><td>4</td><td>Заменить буквы сообщения, составленного на русском языке буквами циклически сдвинутого русского алфавита на 7 букв влево</td></tr>
<tr><td>5</td><td>Заменить буквы сообщения, составленного на английском языке согласно лозунговому шифру с лозунгом «phrase»</td></tr>
<tr><td>6</td><td>Заменить буквы сообщения, составленного на английском языке согласно лозунговому шифру с лозунгом «labour»</td></tr>
<tr><td>7</td><td>Заменить буквы английского сообщения согласно шифру Цезаря, примененному к английскому языку</td></tr>
<tr><td>8</td><td>Заменить буквы сообщения, составленного на русском языке согласно шифру Атбаш, примененному к русскому алфавиту</td></tr>
<tr><td>9</td><td>Заменить буквы сообщения, составленного на русском языке согласно шифру Цезаря, примененному к русскому алфавиту</td></tr>
</table>

Таблица 2

Создание программного кода шифра замены по правилу

<table>
<tr><th>№</th><th>Правило замены</th></tr>
<tr><td>0</td><td>Заменить буквы сообщения, составленного на русском языке согласно шифру простой колонной перестановки</td></tr>
<tr><td>1</td><td>Заменить буквы сообщения, составленного на английском языке их кодами согласно базовой таблице кодировки ASCII (шестн.)</td></tr>
<tr><td>2</td><td>Заменить буквы сообщения, составленного на русском языке их порядковыми номерами в алфавите</td></tr>
<tr><td>3</td><td>Заменить буквы сообщения, составленного на английском языке их порядковыми номерами в алфавите</td></tr>
<tr><td>4</td><td>Заменить буквы сообщения, составленного на русском языке их кодами согласно кодировке Windows 1251</td></tr>
<tr><td>5</td><td>Заменить буквы сообщения, составленного на английском языке их кодами согласно базовой таблице кодировки ASCII (дес.)</td></tr>
<tr><td>6</td><td>Заменить буквы сообщения, составленного на русском языке по следующей таблице
<table>
<tr><td>А</td><td>Б</td><td>В</td><td>Г</td><td>Д</td><td>Е</td><td>Ж</td><td>З</td><td>И</td><td>Й</td><td>К</td><td>Л</td><td>М</td><td>Н</td><td>О</td><td>П</td><td>Р</td></tr>
<tr><td>09</td><td>23</td><td>01</td><td>04</td><td>07</td><td>02</td><td>14</td><td>13</td><td>21</td><td>31</td><td>17</td><td>25</td><td>29</td><td>06</td><td>22</td><td>11</td><td>26</td></tr>
<tr><td>С</td><td>Т</td><td>У</td><td>Ф</td><td>Х</td><td>Ц</td><td>Ч</td><td>Ш</td><td>Щ</td><td>Ъ</td><td>Ы</td><td>Ь</td><td>Э</td><td>Ю</td><td>Я</td><td></td></tr>
<tr><td>00</td><td>19</td><td>30</td><td>08</td><td>18</td><td>16</td><td>28</td><td>03</td><td>27</td><td>32</td><td>15</td><td>10</td><td>20</td><td>24</td><td>12</td><td>05</td></tr>
</table></td></tr>
<tr><td>7</td><td>Заменить буквы сообщения, составленного на русском языке по следующей таблице
<table>
<tr><td>А</td><td>Б</td><td>В</td><td>Г</td><td>Д</td><td>Е</td><td>Ж</td><td>З</td><td>И</td><td>Й</td><td>К</td><td>Л</td><td>М</td><td>Н</td><td>О</td><td>П</td><td>Р</td></tr>
<tr><td>00</td><td>01</td><td>02</td><td>03</td><td>04</td><td>05</td><td>06</td><td>07</td><td>08</td><td>09</td><td>10</td><td>11</td><td>12</td><td>13</td><td>14</td><td>15</td><td>16</td></tr>
<tr><td>С</td><td>Т</td><td>У</td><td>Ф</td><td>Х</td><td>Ц</td><td>Ч</td><td>Ш</td><td>Щ</td><td>Ъ</td><td>Ы</td><td>Ь</td><td>Э</td><td>Ю</td><td>Я</td><td></td></tr>
<tr><td>17</td><td>18</td><td>19</td><td>20</td><td>21</td><td>22</td><td>23</td><td>24</td><td>25</td><td>26</td><td>27</td><td>28</td><td>29</td><td>30</td><td>31</td><td>32</td></tr>
</table></td></tr>
<tr><td>8</td><td>Заменить буквы сообщения, составленного на русском языке согласно шифра Виженера с ключом «победа»</td></tr>
<tr><td>9</td><td>Заменить буквы сообщения, составленного на русском языке согласно шифру Виженера с ключом «мысль»</td></tr>
</table>

Лабораторная работа № 2

Тема: создание пользовательской формы – Шифратор Цезаря.

Задача: задано:

а) исходный текст зашифровать с помощью шифра Цезаря;

б) шифротекст расшифровать, зная ключ – шифр Цезаря.

Формализация задачи. Определим исходные и выходные данные. Исходные данные – строка исходного текста – str .

Выходные данные: а) строка шифротекста strT;

б) строка расшифрованного (исходного) текста strR .

Разработка алгоритма. Для решения поставленной задачи можно применить стандартный алгоритм шифрования (расшифровывания) Цезаря. Применя-

ем операцию циклического (модульного) сложения. От обычного сложения эта операция отличается тем, что если сумма превышает число 32, то из нее вычитается 32, обратная операция – вычитание – характеризуется тем, что если в результате получается отрицательное число, то к нему прибавляется 32.

Реализация алгоритма на ЭВМ. Спроектируем пользовательскую форму.

1 Откройте документ Microsoft Excel.

2 Откройте окно редактирования VBA. Для этого на вкладке Разработчик нажмите кнопку Visual Basic.

3 В открывшемся окне выберите команду Insert/UserForm. В редакторе Visual Basic появятся: окно пользовательской формы и панель инструментов Панель элементов. На Панели элементов находятся все необходимые для проектирования формы элементы.

4 Используя диалоговое окно Свойства (для вызова этого окна, если оно отсутствует, выполните команду View/Properties Windows) и Панель элементов, простым перетаскиванием элементов управления на форму, создайте пользовательскую форму в виде, представленном на рис. 2.

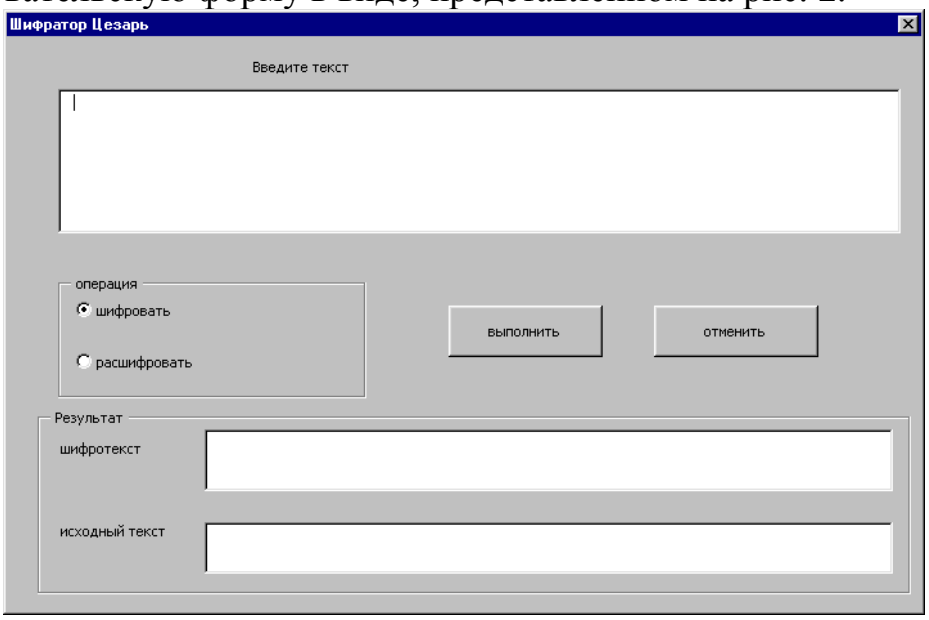

Рис. 2

5 Надписи, отображаемые на элементе управления, для формы – текст, отображаемый в строке заголовка формы, определите с помощью значения свойства Caption.

6 Чтобы написать процедуру обработки событий нажатия кнопки «Выполнить» или «Отменить» (событие Click), дважды щелкните на элементе управления CommandButton или воспользуйтесь командой контекстного меню View Code.

7 В окно редактирования кода необходимо ввести следующие процедуры:

```
Private Sub UserForm_Initialize()
CommandButton1.Caption = "выполнить"
CommandButton2.Caption = "отменить"
OptionButton1.Caption = "шифровать"
OptionButton2.Caption = "расшифровать"
'первоначальный выбор переключателя
```

```
OptionButton1.Value = True
OptionButton2.Value = False
End Sub

Sub текст(видимость)
'процедура управляет видимостью
Frame2.Visible = видимость
TextBox1.Visible = видимость
TextBox2.Visible = видимость
TextBox3.Visible = видимость
End Sub
Private Sub CommandButton1_Click()
Dim str As String, strT As String, strR As String
Dim n As Long, i As Long
str = TextBox1.Text
n = Len(str)
strT = Space(n)
If OptionButton1.Value = True Then
If TextBox1.Text = "" Then MsgBox ("Введите исходный текст"):
GoTo 1
'сдвиг на 3 знака шифровка
For i = 1 To n
Mid(strT, i, 1) = Caesar(Mid(str, i, 1), 3)
Next i
End If
TextBox2.Text = strT
If OptionButton2.Value = True Then
str = TextBox1.Text
n = Len(str)
strR = Space(n)
If TextBox1.Text = "" Then MsgBox ("Введите шифротекст"): GoTo
1
'сдвиг на -3 знака расшифровка
For i = 1 To n
Mid(strR, i, 1) = Caesar(Mid(str, i, 1), -3)
Next i
End If
TextBox3.Text = strR
1:
End Sub
Private Function Caesar(A, Sh)
Dim chrnew As Integer
Select Case Asc(A)
       Case 224 To 255 'строчные буквы
       chrnew = ModMew(Asc(A) + Sh - 224, 32) + 224
       Caesar = Chr(chrnew)
       Case 192 To 223 'прописные буквы
       chrnew = ModMew(Asc(A) + Sh - 192, 32) + 192
       Caesar = Chr(chrnew)
       Case Else
       Caesar = A
       End Select
End Function
```

```
Private Function ModMew(A, B)
If A >= 0 Then
ModMew = A Mod B
Else
ModMew = (B + A) Mod B
End If
End Function
Private Sub CommandButton2_Click()
'закрыть форму
UserForm1.Hide
'при закрытии формы очищаем текстовые поля
TextBox1.Text = ""
TextBox2.Text = ""
TextBox3.Text = ""
End Sub

Private Sub OptionButton1_Click()
OptionButton1.Value = True
расшифровать = False
End Sub

Private Sub OptionButton2_Click()
шифровать = False
OptionButton2.Value = True
End Sub
```

8 Для запуска формы с листа выполнить команду Вид/Панели инструментов/Элементы управления. На панели инструментов нажмите кнопку Режим конструктора. Выберите элемент управления Кнопка и перетащите ее на рабочий лист. По двойному щелчку на Кнопке попадаем в поле, в котором необходимо писать процедуру работы Кнопки

```
Private Sub CommandButton1_Click()
UserForm1.Show
End Sub
```

Индивидуальные задания по лабораторной работе № 2

Варианты заданий приведены в табл. 3 и табл. 4. Уровень сложности заданий табл. 4 значительно выше.

Правильность работы шифраторов проверить: предусмотрев вывод сообщения в окно Шифратора при шифровке, после шифровки и его расшифровке, а при расшифровке также после расшифровки и его повторной шифровки. Визуально сравнить результаты.

Таблица 3

№	Создать пользовательскую форму шифратора	№	Создать пользовательскую форму шифратора
0	Шифра Атбаш	5	Шифра «Альбам»
1	Шифра по правилу: буквы исходного сообщения заменяются буквами циклически сдвинутого на 6 букв влево русского алфавита	6	Шифра по правилу: буквы исходного сообщения на английском языке заменяются буквами циклически сдвинутого на 5 букв влево латинского алфавита
2	Лозунгового шифра с лозунгом «компьютер»	7	Лозунгового шифра с лозунгом «mail»
3	Шифра типа масонской замены – «простая литорея»	8	Лозунгового шифра с лозунгом «осень»
4	Лозунгового шифра с лозунгом «ache»	9	Лозунгового шифра с лозунгом «август»

Таблица 4

№	Создать пользовательскую форму шифратора	№	Создать пользовательскую форму шифратора
0	Шифра вертикальной перестановки с ключом «экзамен»	5	Шифра вертикальной перестановки с ключом «студент»
1	Шифра Виженера с ключом «экзамен»	6	Шифра простой колонной перестановки
2	Шифра со случайной гаммой	7	Шифра гаммирования с ключом 03 30 21
3	Шифра гаммирования с ключом 09 11 23 17	8	Шифра вертикальной перестановки с ключом «мечта»
4	Шифра вертикальной перестановки с ключом 5 3 1 2 4 6	9	Шифра Виженера с ключом «мелодия»

Лабораторная работа № 3

Тема: системы с закрытым ключом. Шифрование методом подстановки.

Цель работы: научиться выполнять шифрование текста в Microsoft Excel методом подстановки.

Суть метода: шифрование методом подстановки основано на замене в исходном тексте одних символов алфавита другими по определенному алгоритму или с помощью таблицы соответствия.

Задание 1. Шифрование средствами электронных таблиц.

Реализация алгоритма на ЭВМ

1 Запустите программу Microsoft Excel (Пуск – Все Программы – Microsoft Office Excel 2013).

2 Лист 1 рабочей книги Excel переименуйте. Назовите Лаб. раб. № 3.

3 На листе Лаб. раб. № 3 наберите исходные данные, как показано на рис. 3.

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
1	метод подстановки															
2	ключ=	13														
3																
4	исходный текст	с	о	л	н	е	ч	н	ы	й		д	е	н	ь	
5																

Рис. 3

4 Используем текстовые функции СИМВОЛ и КОДСИМВ. Заметим, что пустая ячейка листа Excel, соответствующая пробелу, имеет код символа 32. Воспользуемся логическими функциями: ЕСЛИ и ЕПУСТО, а также арифметической функцией остаток от деления ОСТАТ. Алфавит предполагаем состоящим из 256 элементов, то есть в данном случае любая буква русского алфавита может быть заменена любым символом из таблицы символов текстового редактора Word. Подстановка состоит в том, что к коду символа добавляется значение ключа и определяется символ, соответствующий этому коду.

Поместив курсор в ячейку B6, в строке формул сделайте запись =ЕСЛИ(ЕПУСТО(B4);СИМВОЛ(32);СИМВОЛ(ОСТАТ(КОДСИМВ(B4)+B2;256))).

5 Выполните авто заполнение ячеек B6-O6. В результате в строке 6 получим зашифрованную фразу «солнечный день» рис. 4.

6

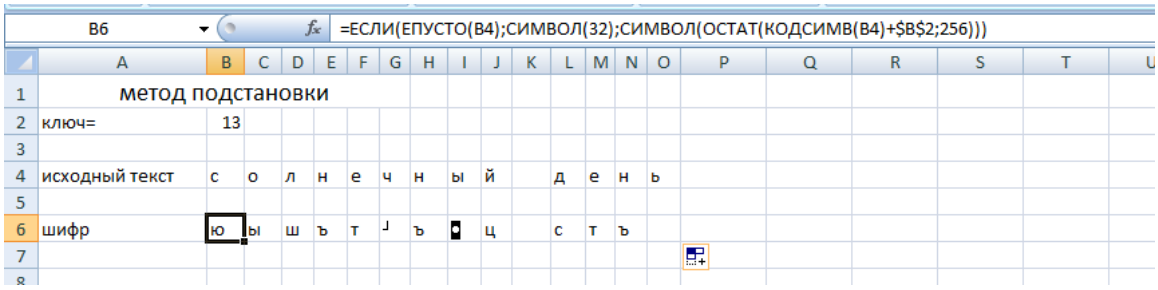

Рис. 4

7 Выполним расшифровку строки 6. При этом вместо проверки ЕПУСТО выполняем проверку на наличие в ячейке символа 32 и определяем символ, соответствующий коду, уменьшенному на значение ключа. Таким образом, поместив курсор в ячейку B8, в строке формул сделайте запись =ЕСЛИ(B6=СИМВОЛ(32);СИМВОЛ(32);СИМВОЛ(ОСТАТ(КОДСИМВ(B6)-B2;256)))

8 Выполните автозаполнение ячеек B8-O8. В результате в строке 8 получили расшифрованную фразу «солнечный день» рис. 5.

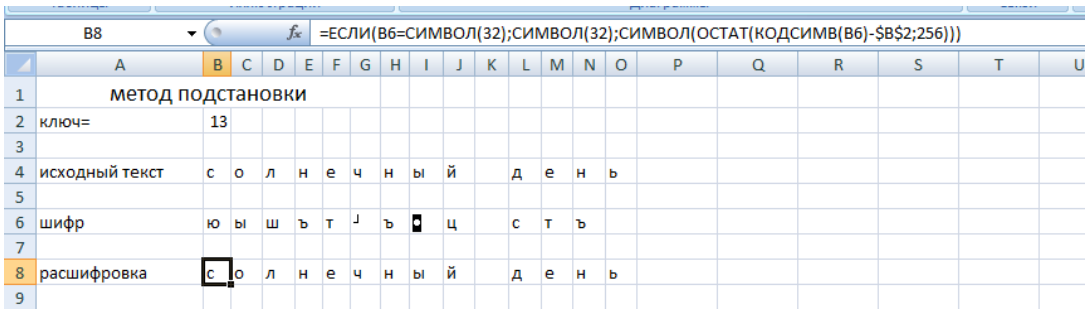

Рис. 5

Задание 2. Шифрование средствами VBA.

Реализация алгоритма на ЭВМ

1 Откройте лист Лаб. раб. № 3, нажмите Alt-F11. Откроется окно редактирования VBA.

2 В редакторе VBA выполнить команду Insert/Module.

3 Выберите команду Insert/UserForm. В редакторе Visual Basic появятся: окно пользовательской формы и панель инструментов Панель элементов. На Панели элементов находятся все необходимые для проектирования формы элементы.

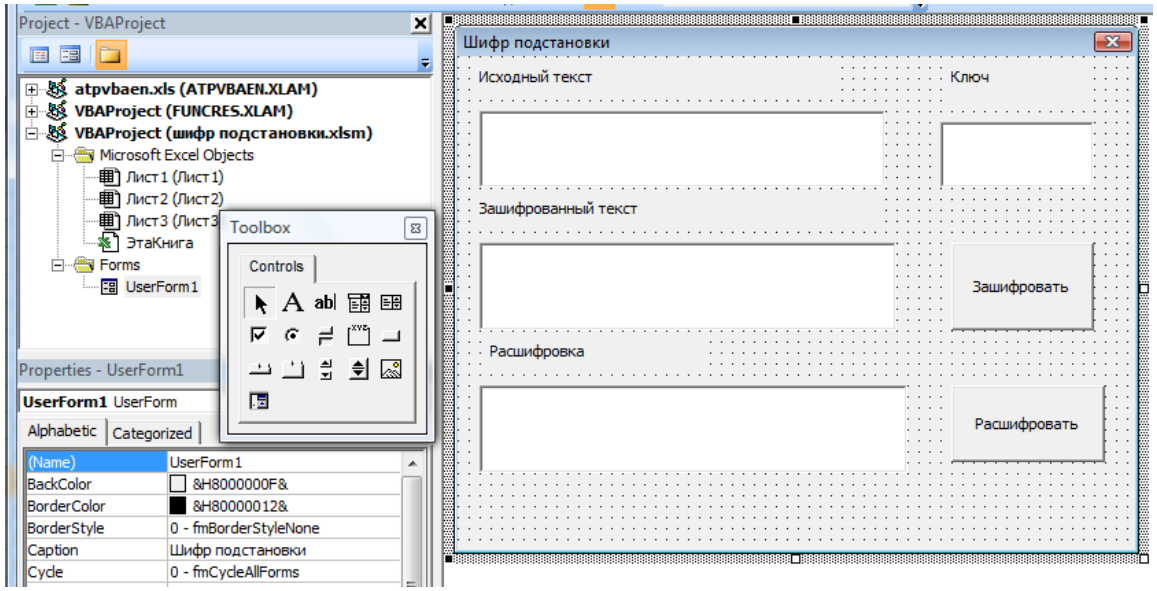

Рис. 6

4 Используя диалоговое окно Свойства (для вызова этого окна, если оно отсутствует, выполните команду View/Properties Windows) и Панель элементов, простым перетаскиванием элементов управления на форму, создайте пользовательскую форму в виде, представленном на рис. 6.

5 Надписи, отображаемые на элементе управления, для формы – текст, отображаемый в строке заголовка формы, определите с помощью значения свойства Caption.

6 Чтобы написать процедуру обработки событий нажатия кнопки «зашифровать» (событие Click), дважды щелкните на элементе управления CommandButton1 или воспользуйтесь командой контекстного меню View Code.

7 В окно редактирования кода необходимо ввести следующий текст:

```
Private Sub CommandButton1_Click()
'шифровка
m = TextBox1.Value
n = Len(m)
c = Space(n)
k = TextBox4.Value
If TextBox1.Text = "" Then MsgBox "Введите текст": GoTo 1
If TextBox4.Text = "" Then MsgBox "Введите ключ": GoTo 1
For i = 1 To n
r = Ca(Mid(m, i, 1), k)
c = c & r
Next i
TextBox2.Value = c
1:
End Sub
Private Function Ca(A, Sh)
Dim chrnew As Integer
Select Case Asc(A)
       Case 224 To 255 'строчные буквы
       chrnew = ModMew(Asc(A) + Sh - 224, 32) + 224
       Ca = Chr(chrnew)
       Case 192 To 223 'прописные буквы
       chrnew = ModMew(Asc(A) + Sh - 192, 32) + 192
       Ca = Chr(chrnew)
       Case Else
       Ca = A
       End Select
End Function
Private Function ModMew(A, B)
If A >= 0 Then
ModMew = A Mod B
Else
ModMew = (B + A) Mod B
End If
End Function

Private Sub CommandButton2_Click()
'расшифровка
m = TextBox2.Value
c = Space(n)
k = TextBox4.Value
If TextBox2.Text = "" Then MsgBox "Введите шифротекст": GoTo 1
If TextBox4.Text = "" Then MsgBox "Введите ключ": GoTo 1
n = Len(m)
For i = 1 To n
r = Ca(Mid(m, i, 1), -k)
c = c & r
Next i
TextBox3.Value = c
1:
End Sub
```

8 Выполните команду Debug/Compile VBA.

9 Для того чтобы проверить, как работает созданная программа, поместите курсор в поле кода программы и нажмите клавишу F5 или выберите команду RUN/RUN SUB/USERFORM.

10 В результате диалог будет выглядеть, как представлено на рис. 7.

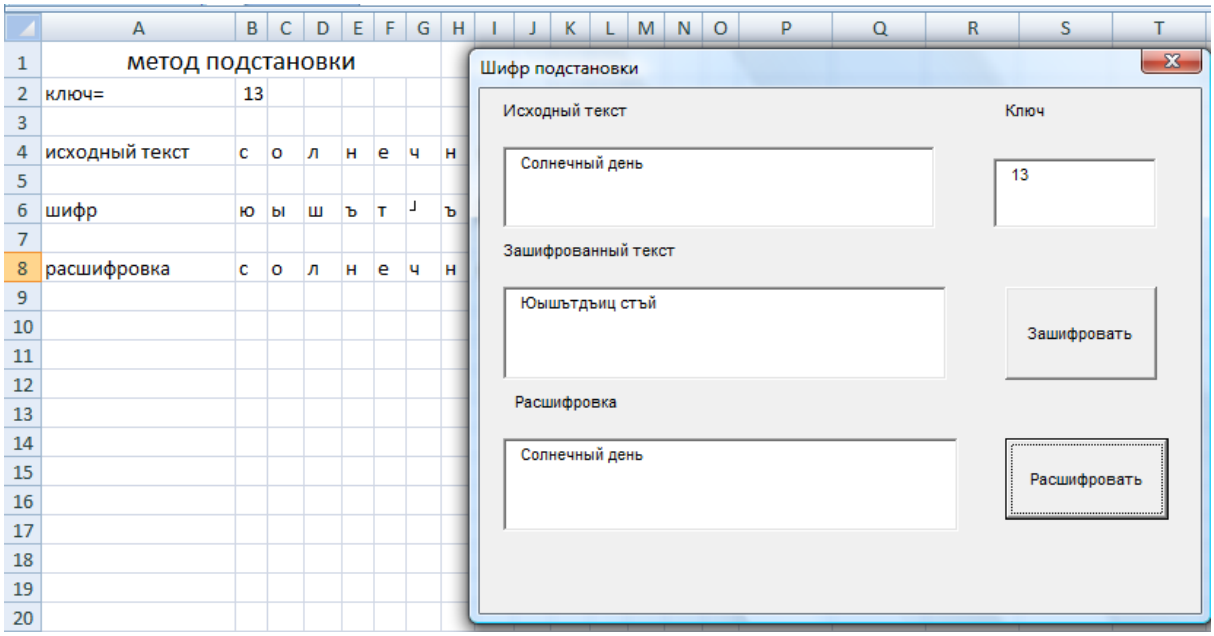

Рис. 7

11 Для запуска формы с листа Лаб. раб. № 3 создадим кнопку запуска программы. Обычную кнопку (элемент управления формы) и кнопку команды (элемент ActiveX) можно использовать для запуска макроса, выполняющего определенные действия при нажатии пользователем кнопки.

12 Для добавления кнопки (элемент управления формы) ознакомитесь, доступна ли вкладка Разработчик. Если вкладка Разработчик недоступна, то ее нужно отобразить:

a. Нажмите кнопку Microsoft Office  , а затем щелкните Параметры Excel.

b. В категории Основные в разделе Основные параметры работы с Excel установите флажок **Показывать вкладку «Разработчик» на ленте**, а затем нажмите кнопку ОК.

13 На вкладке Разработчик в группе Элементы управления нажмите кнопку **Вставить**, а затем в разделе Элементы управления формы выберите элемент Кнопка  .

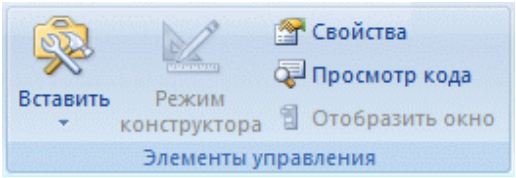

Рис. 8

14 Щелкните на листе место, где должен быть расположен левый верхний угол кнопки. Подпишите кнопку «Запуск программы».

15 Для запуска формы с листа Лаб. раб. № 3 щелкните на кнопке «Запуск программы» правой кнопкой мышки. В контекстном меню выберите команду **Назначить макрос**… В появившемся диалоговом окне нажмите кнопку **Создать**. В результате попадаем в поле, в котором необходимо писать процедуру работы Кнопки

```
Private Sub CommandButton1_Click()
UserForm1.Show
End Sub
```

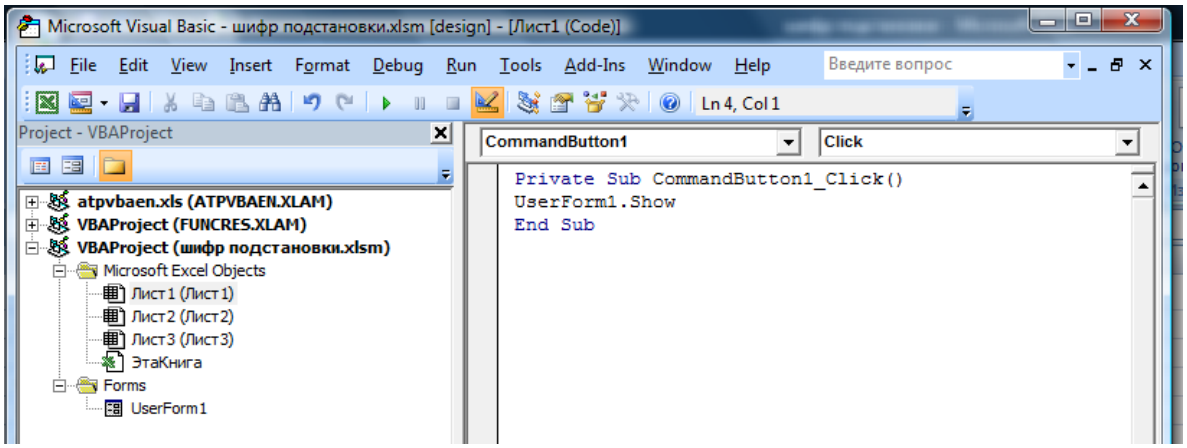

Рис. 9.

16 Перейдите на лист Лаб. раб № 3 и проверьте работу кнопки «Запуск программы».

17 Нажмите кнопку Microsoft Office  , выберите команду Сохранить как Книга Excel с поддержкой макросов.

Индивидуальные задания по лабораторной работе № 3

Задание 1. Работа алгоритма шифрования средствами электронных таблиц была проверена на значениях ключа до 50. Было обнаружено, что реализованный таким образом алгоритм шифрования для фразы «солнечный день» не работает при следующих значениях ключа: 4, 5, 9, 15, 18, 19, 21, 23, 27, 28, 50. Объясните: в чем причина?

Задание 2. Реализованный алгоритм шифрования средствами VBA позволяет шифровать фразы, записанные на русском языке. При этом в зашифрованном тексте строчная буква появляется на месте строчной буквы в исходном тексте. Пробелы в шифротексте появляются в тех же позициях, в каких они находятся в исходном тексте. Объясните причину указанных недостатков.

Задание 3. Сравните зашифрованный текст, полученный при шифровании средствами электронных таблиц, и зашифрованный текст, полученный при шифровании средствами VBA. Объясните причину различия шифротекстов.

Задание 4. Зашифровать выражения. Варианты заданий приведены в табл. 5.

Таблица 5

№	Текст	№	Текст
1	Высокие деревья больше подвластны ветрам, а честолюбивые люди – ударам судьбы. Пенн	11	Никто так не падок на лесть, как тот честолюбец, который хотел бы быть первым, но не смог им стать. Спиноза
2	Чем тоньше лед, тем больше всем хочется узнать, выдержит ли он. Биллингс	12	Моя заветная мечта – сказать десятком предложений то, на что другим требуется целая книга. Ницше
3	Однажды испорченную репутацию, вероятно, можно восстановить, но мир будет все время оглядываться на то место, где была трещина. Холл	13	Если Вы подберете голодную собаку и устроите ей роскошную жизнь, она никогда не укусит Вас. В этом главная разница между собакой и человеком. Марк Твен
4	Важно не только уметь сказать нужную вещь в нужный момент, но и уметь не сказать не нужного, когда очень хочется. Сала	14	Истинная дружба – медленно растущее растение, которое должно быть испытано в беде и несчастье, прежде чем заслужить такое название. Джордж Вашингтон
5	Молчание – самое совершенное выражение презрения. Бернард Шоу	15	Наша необразованность в основном преодолима. Мы не знаем, потому что не хотим знать. Хаксли
6	Не насмехайся над природными недостатками тех, кто не может их исправить. Жестоко бить калеку его же костылями. Фуллер	16	Чтобы добиться успеха в этом мире, недостаточно быть просто глупым, нужно еще иметь хорошие манеры. Вольтер
7	Лицемер: человек, убивший своих родителей... и просящий о снисхождении на основании того, что он сирота. Линкольн	17	Бояться надо не тех, кто не согласен с вами, а тех, кто не согласен с Вами и боится Вам об этом сказать. Наполеон
8	Веселость нрава дарит нам долголетие в жизни, а потом и в памяти окружающих. Она рождена добром. Бови	18	Музыка стоит на втором месте после молчания, когда речь идет о том, чтобы выразить невыразимое. Хаксли
9	Испробуй все возможности. Всегда важно знать, что ты сделал все, что мог. Диккенс	19	Гордец редко бывает благодарным, ибо всегда считает, что получил меньше, чем заслуживает. Бичер
10	Необходимость – мать изобретательности. Свифт	20	Я обычно сужу о человеке по тому, что вызывает его смех. Мизнер

Лабораторная работа № 4

Тема: системы с закрытым ключом. Шифр многоалфавитной замены.

Суть метода: шифрование производится по алгоритму многоалфавитной замены с использованием таблицы Виженера. Шифрование средствами VBA.

Реализация алгоритма на ЭВМ

1 Запустите программу Microsoft Excel (Пуск – Все Программы – Microsoft Office Excel 2013).

2 Лист 1 рабочей книги Excel переименуйте. Назовите Лаб. раб. № 4.

3 В каждую ячейку первой строки листа, начиная с ячейки A1, последовательно введите буквы русского алфавита.

4 На вкладке Разработчик в группе Элементы управления нажмите кнопку **Вставить**, а затем в разделе Элементы ActiveX выберите элемент Поле (элемент ActiveX**).**  Вставьте данное текстовое поле в строку 3.

5 На вкладке Разработчик в группе Элементы управления нажмите кнопку **Вставить**, а затем в разделе Элементы ActiveX выберите элемент Кнопка (элемент управления формы)  . Выберите на листе место, где должен быть расположен левый верхний угол кнопки. Подпишите кнопку «Подготовка».

6 В результате двойного щелчка на кнопке «Подготовка» попадаем в поле (Microsoft Excel Object Лист 1), в котором необходимо писать процедуру работы Кнопки

```
Private Sub CommandButton1_Click()
Dim i, j, n, c As Integer
Dim st As String
st = TextBox1.Text
n = Len(st)
Cells(4, 35).Value = n
If TextBox1.Text = "" Then MsgBox "Введите набор символов"
For j = 0 To n - 1
For i = 1 To n
Cells(5 + j, i).Value = Mid(st, j + i, 1)
If i + j > n Then
For c = 1 To (j)
Cells(5 + j, i + c - 1).Value = Mid(st, c, 1)
Next c
GoTo 1
End If
Next i
1:
Next j
End Sub
```

7 Выполните команду Debug/Compile VBA.

8 Вернитесь на лист Лаб. раб. № 4. В результате щелчка по кнопке «Подготовка» на лист будет выведено сообщение "Введите набор символов" (рис. 10). Это предполагает, что может быть введен произвольный алфавит, за исключением числовых значений.

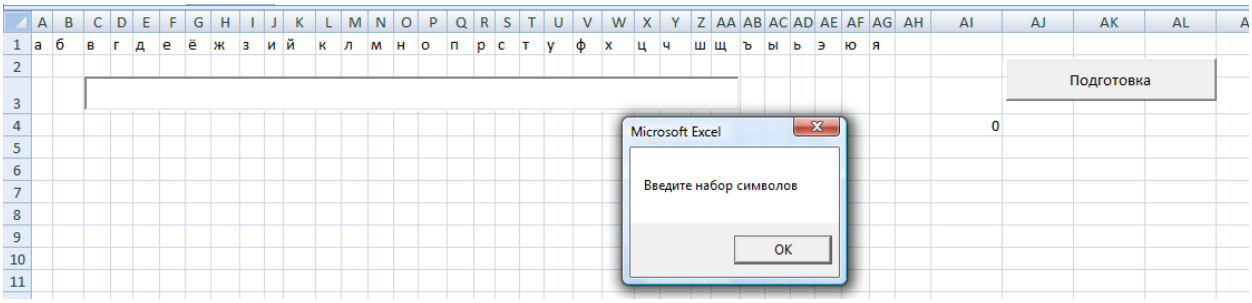

Рис. 10

9 Вводим в текстовое поле строки 3 русский алфавит «абвгдеёжзийклмнопрстуфхцчшщъыьэюя », дополнив его после буквы «я» пробелом.

10 Щелчок на кнопке «Подготовка» приведет к тому, что в строках с 5 по 38 будет представлена таблица Виженера, которая частично видна на рис. 24.

11 Нажмите Alt-F11. Откроется окно редактирования VBA.

12 В редакторе VBA выполнить команду Insert/Module. Выберите команду Insert/UserForm. В редакторе Visual Basic появятся: окно пользовательской формы и панель инструментов Панель элементов. На Панели элементов находятся все необходимые для проектирования формы элементы.

13 Используя диалоговое окно Свойства (для вызова этого окна, если оно отсутствует, выполните команду View/Properties Windows) и Панель элементов, простым перетаскиванием элементов управления на форму, создайте пользовательскую форму в виде, представленном на рис. 11.

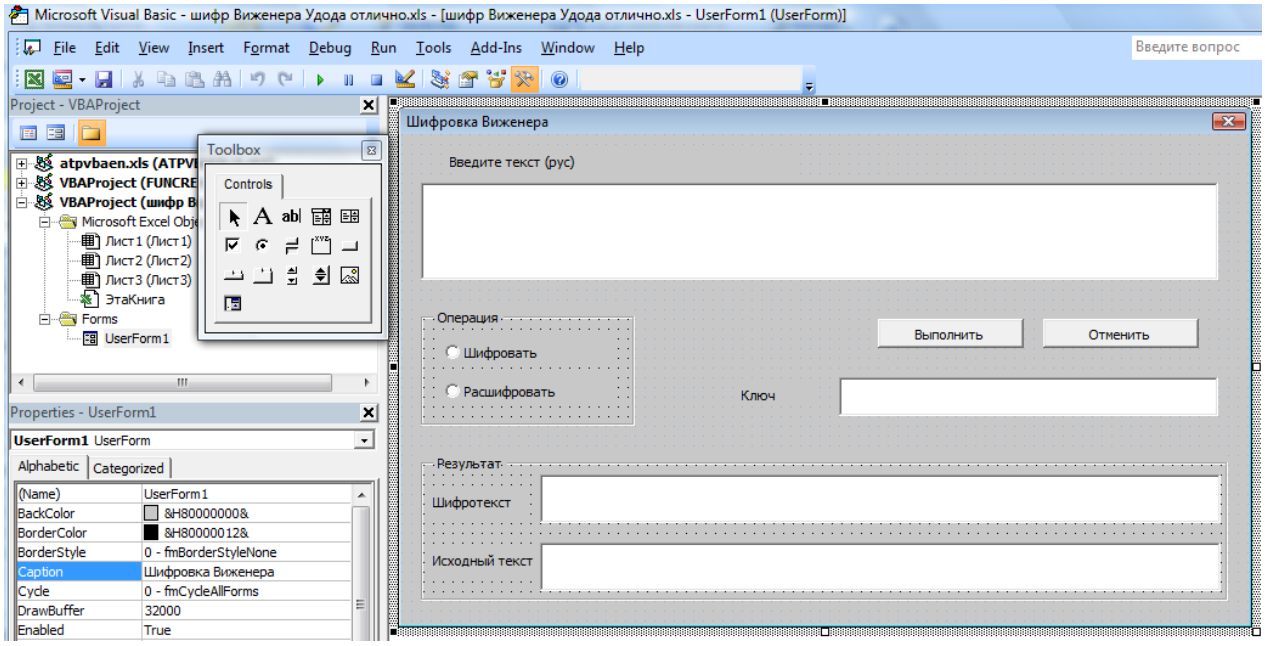

Рис. 11

14 Чтобы написать процедуру обработки событий нажатия кнопки «зашифровать» (событие Click), дважды щелкните на элементе управления CommandButton1 или воспользуйтесь командой контекстного меню View Code.

15 В окно редактирования кода необходимо ввести следующий текст:

```
Private Sub UserForm_Initialize()
```

```
CommandButton1.Caption = "Выполнить"
CommandButton2.Caption = "Отменить"
OptionButton1.Caption = "Шифровать"
OptionButton2.Caption = "Расшифровать"
OptionButton1.Value = True
OptionButton2.Value = False
End Sub


Sub текст(видимость)
Frame2.Visible = видимость
TextBox1.Visible = видимость
TextBox2.Visible = видимость
TextBox3.Visible = видимость
End Sub

Private Sub CommandButton1_Click()
Dim str As String, strT As String, strR As String, key As
String, bb As String, st As String, s As String
Dim n, c, k, l As Long, i, j As Long
Dim a, b, x As Integer

str = TextBox1.Text
n = Len(str)
strT = Space(n)
key = TextBox4.Text
k = Len(key)
c = Sheets("Лист1").Cells(4, 35).Value
bb = Space(n)
x = 1

If OptionButton1.Value = True Then
If TextBox1.Text = "" Then MsgBox "Введите исходный текст":
GoTo 1
If TextBox4.Text = "" Then MsgBox "Введите ключ": GoTo 1
'прописывание текста через ключ
For i = 1 To n
If x <= k Then
Mid(bb, i, 1) = Mid(key, x, 1)
Else:
x = 1
Mid(bb, i, 1) = Mid(key, x, 1)
End If
x = x + 1
Next i
'MsgBox bb

'кодирование
For i = 1 To n
For j = 1 To c
If Sheets("Лист1").Cells(4 + j, 1).Value = Mid(bb, i, 1) Then
a = j + 4
Next j
```

```
For l = 1 To c
If Sheets("Лист1").Cells(5, l).Value = Mid(str, i, 1) Then
b = l
GoTo 2
Else:
If l = c Then
s = Mid(str, i, 1)
MsgBox "Такого символа нет: " & s & "!": GoTo 1
End If

End If
Next l
2:
Mid(strT, i, 1) = Sheets("Лист1").Cells(a, b).Value
Next i
End If
TextBox2.Text = strT

'расшифровка
If OptionButton2.Value = True Then
If TextBox1.Text = "" Then MsgBox "Введите шифротекст": GoTo 1
If TextBox4.Text = "" Then MsgBox "Введите ключ": GoTo 1

st = TextBox1.Text
n = Len(st)
strR = Space(n)
bb = Space(n)
x = 1
key = TextBox4.Text
k = Len(key)
'пропись через ключ
For i = 1 To n
If x <= k Then
Mid(bb, i, 1) = Mid(key, x, 1)
Else:
x = 1
Mid(bb, i, 1) = Mid(key, x, 1)
End If
x = x + 1
Next i
'MsgBox bb

For i = 1 To n
For j = 1 To c
If Mid(bb, i, 1) = Sheets("Лист1").Cells(4 + j, 1).Value Then
a = j + 4
For l = 1 To c
If Mid(st, i, 1) = Sheets("Лист1").Cells(a, l).Value Then
b = l
GoTo 3
Else:
If l = c Then
```

```
s = Mid(st, i, 1)
MsgBox "Такого символа нет: " & s & "!": GoTo 1
End If

End If
Next l
End If
Next j
3:
Mid(strR, i, 1) = Sheets("Лист1").Cells(5, b).Value
Next i

End If
TextBox3.Text = strR
1:
End Sub

Private Sub CommandButton2_Click()
UserForm1.Hide
TextBox1.Text = ""
TextBox2.Text = ""
TextBox3.Text = ""
End Sub

Private Sub OptionButton1_Click()
OptionButton1.Value = True
Расшифровать = False
End Sub

Private Sub OptionButton2_Click()
Шифровать = False
OptionButton2.Value = True
End Sub
```

16 Перейдите на лист Лаб. раб. № 4. На вкладке Разработчик в группе Элементы управления нажмите кнопку **Вставить**, а затем в Элементы ActiveX выберите элемент Кнопка (элемент управления формы)  . Выберите на листе место, где должен быть расположен левый верхний угол кнопки. Подпишите кнопку «Форма».

17 Для запуска формы с листа Лаб. раб. № 4 с помощью кнопки «Форма» необходимо в Microsoft Excel Object Лист 1 поместить следующий код работы Кнопки

```
Private Sub CommandButton2_Click()
UserForm1.Show
End Sub
```

18 В результате окно диалога шифрования будет выглядеть, как представлено на рис. 12.

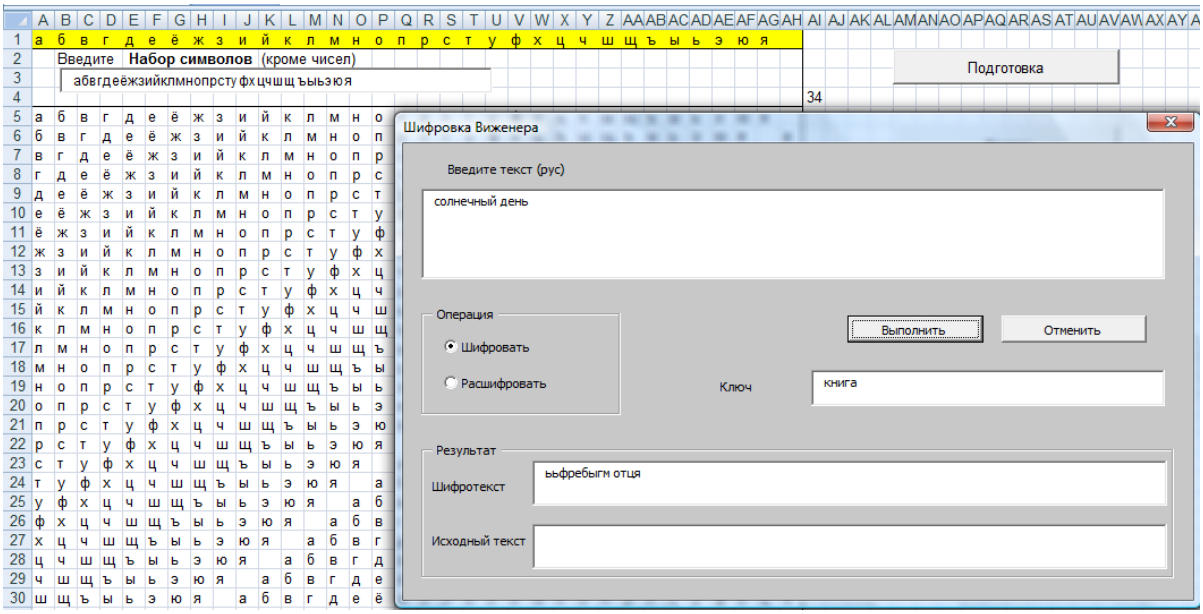

Рис. 12

19 Окно диалога расшифровки показано на рис. 13.

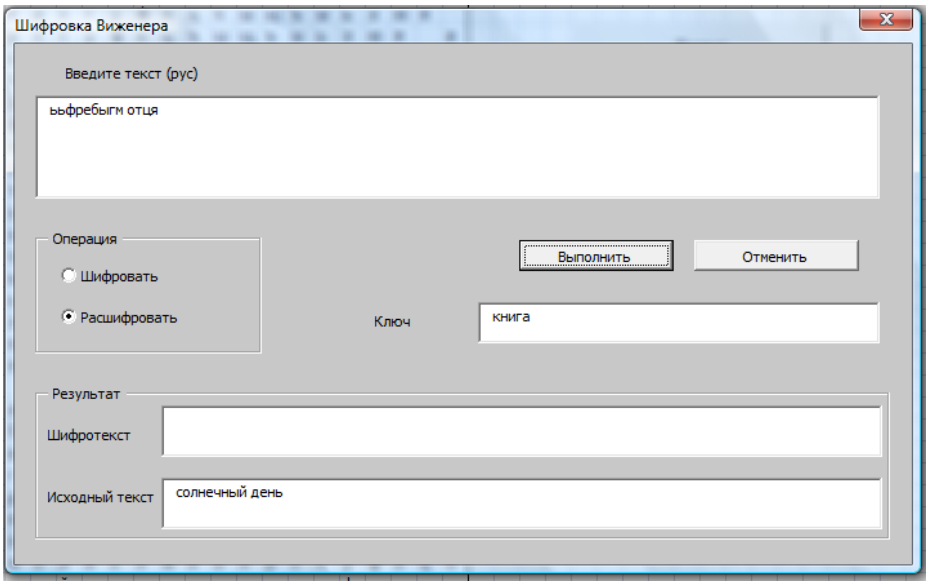

Рис. 13

20 Нажатие кнопки «Отменить» приведет к закрытию окна формы.

Замечание. Обратите внимание, что и исходный, и зашифрованный текст необходимо вводить в поле Введите текст (рус). Для того чтобы не набирать шифротекст вручную, его достаточно выделить и скопировать нажатием клавиш Ctrl+c. Для того чтобы вставить скопированный текст, поместите курсор в поле Введите текст (рус) и нажмите клавиши Ctrl+v.

Лабораторная работа № 5

Тема: системы с закрытым ключом. Шифрование методом перестановки.

Суть метода: шифрование методом подстановки основано на перестановке символов в исходном тексте по определенному алгоритму. В данной лабора-

торной работе будем использовать маршрутную перестановку, а именно простую колонную перестановку. Шифрование производим средствами VBA.

Реализация алгоритма на ЭВМ

1 Откройте лист Лаб. раб. № 5 нажмите Alt-F11. В открывшемся окне редактирования VBA выполните команду Insert – UserForm. Создайте на форме три текстовых поля и две кнопки. Первое текстовое поле будет содержать исходный текст, второе – шифротекст, третье поле – ключ, определяющий размер таблицы перемешивания символов. Окончательный вид UserForm представлен на рис. 14.

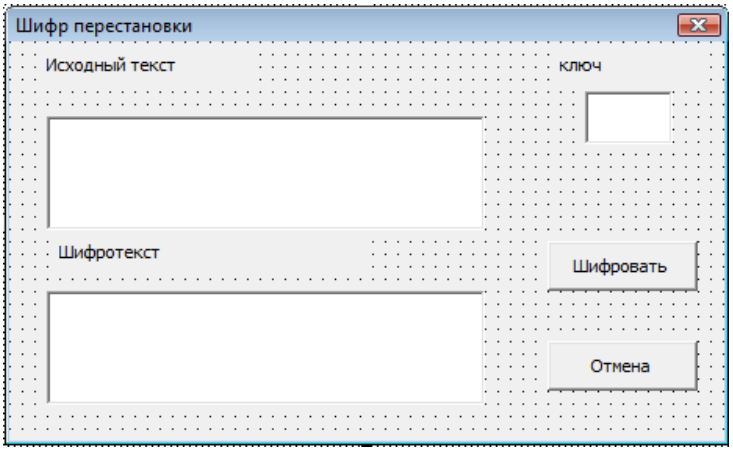

Рис. 14

2 Процедуру обработки событий нажатия кнопки «Шифровать» введем в окно редактирования кода

```
Private Sub CommandButton1_Click()
Dim i, j As Integer
Dim M, c As String
M = TextBox1.Value
k1 = TextBox3.Value
k = Len(M)
If TextBox1.Text = "" Then MsgBox "Введите исходный текст": GoTo
1
If TextBox3.Text = "" Then MsgBox "Введите ключ": GoTo 1
'проверка ключа
If k1 = 1 Then MsgBox ("Введите другой ключ, на этом ключе вы не
получите шифротекст"): GoTo 1
'определение размера прямоугольника, в который вписываем текст
If (k Mod k1) = 0 Then
k2 = k / k1
Else
k2 = k \ k1 + 1
End If
'проверка ключа
If k2 = 1 Then MsgBox ("Введите другой ключ, на этом ключе вы не
получите шифротекст"): GoTo 1
For j = 1 To k1
For i = 1 To k2
Cells(i, j) = Mid(M, j + (i - 1) * k1, 1)
Next i
```

```
Next j
c = ""
For j = 1 To k1
For i = 1 To k2
c = c & Cells(i, j)
Next i
Next j
TextBox2.Value = c
1:
End Sub
```

3 Процедуру обработки событий нажатия кнопки «Отмена» введем в окно редактирования кода

```
Private Sub CommandButton2_Click()
'закрыть форму
UserForm1.Hide
TextBox1.Text = ""
TextBox2.Text = ""
TextBox3.Text = ""
End Sub
```

4 В результате введения исходного текста и ключа в поле формы после нажатия кнопки «Шифровать» диалоговое окно примет вид, показанный на рис. 15.

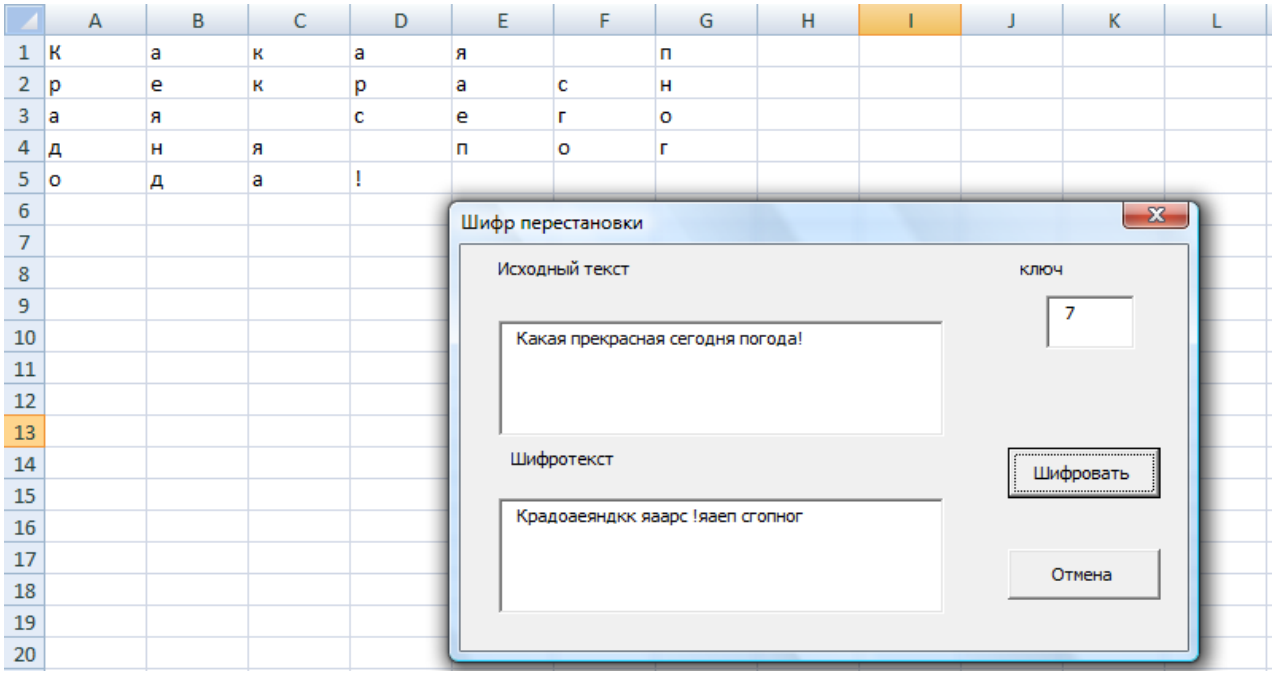

Рис. 15

5 Нажатие кнопки «Отмена» приведет к закрытию окна формы.

Индивидуальные задания по лабораторной работе № 5

Задание 1. Поэкспериментируйте, вводя различные значения ключа. При каких значениях ключа не удается зашифровать текст и почему?

Задание 2. Создайте средство расшифровки.

Задание 3. Зашифровать выражения. Варианты заданий приведены в табл. 5.

Лабораторная работа № 6

Тема: создание пользовательской формы – Шифратор файлов.

Задача: задано:

а) из диалогового окна Открытие документа выбирается исходный текстовый файл(*.txt), который требуется зашифровать с помощью шифра простой перестановки;

б) зашифрованный файл необходимо расшифровать, зная ключ – шифр простой перестановки.

Формализация задачи. Определим исходные и выходные данные. Исходные данные – произвольный текстовый файл. (Воспользуйтесь имеющимся файлом «Текст» или в редакторе Блокнот создайте свой текстовый файл)
Выходные данные – а) зашифрованный файл;
б) расшифрованный (исходный) файл.

Разработка алгоритма. Для решения поставленной задачи создадим программу, позволяющую выбрать необходимый текстовый файл, считать содержимое выбранного файла и с помощью подпрограммы осуществить шифрование (расшифровывания). Шифрование (Расшифрование) осуществим согласно правилу, по которому буквы в тексте переставляются в обратном порядке.

Реализация алгоритма на ЭВМ. Спроектируем форму пользователя.

1 Откройте документ Microsoft Excel.

2 Выполните команду Сервис/Макрос/Редактор Visual Basic.

3 Выберите команду Insert/UserForm. В редакторе Visual Basic появятся: окно пользовательской формы и панель инструментов Панель элементов.

4 Используя диалоговое окно Свойства (для вызова этого окна, если оно отсутствует, выполните команду View/Properties Windows) и Панель элементов, простым перетаскиванием элементов управления на форму, создайте пользовательскую форму в виде, представленном на рис. 16.

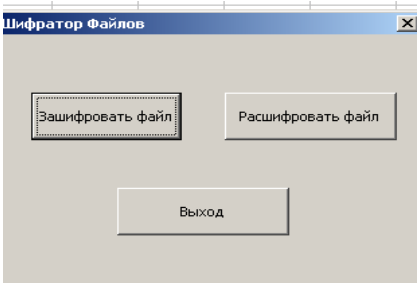

Рис. 16

5 В окно редактирования кода необходимо ввести следующие процедуры:

```
Private Sub Перестановка(strTest, strS)
'процедура выполняет перестановку символов в строке
Dim i As Long, n As Long
n = Len(strTest)
strS = Space(n)
For i = 1 To n
tmp = Mid(strTest, n - i + 1, 1)
```

```
Mid(strTest, n - i + 1, 1) = Mid(strTest, i, 1)
Debug.Print strTest
Mid(strS, i, 1) = tmp
Next i
Debug.Print strS
End Sub

Private Sub CommandButton1_Click()
‘процедура выбора файла и его шифрования
Dim FSys As New FileSystemObject
Dim sFname As Variant
Dim Tfile As TextStream
Dim TextOfFile As String, CryptoText As String
    Set FSys = CreateObject("Scripting.FileSystemObject")
    sFname = Application.GetOpenFilename("Txt file (*.txt),
*.txt")
    If sFname = False Then
    MsgBox "Файл не выбран"
    Exit Sub
    End If
    Set Tfile = FSys.OpenTextFile(sFname, ForReading, False,
TristateFalse)
   TextOfFile = Tfile.ReadAll
    Tfile.Close
TextOfFile = LCase(TextOfFile)
Перестановка TextOfFile, CryptoText
Set Tfile =
FSys.CreateTextFile(Application.GetSaveAsFilename("Зашифрованный
текст", fileFilter:="Текстовые файлы (*.txt), *.txt"))
        Tfile.Write CryptoText
    Tfile.Close
Set Tfile = Nothing
Set FSys = Nothing
End Sub

Private Sub CommandButton2_Click()
‘процедура выбора файла и его расшифрования
Dim FSys As New FileSystemObject
Dim Tfile As TextStream
Dim TextOfFile As String, CryptoText As String
Dim sFname As Variant
     Set FSys = CreateObject("Scripting.FileSystemObject")
   sFname = Application.GetOpenFilename("Txt file (*.txt),
*.txt")
    If sFname = False Then
    MsgBox "Файл не выбран"
    Exit Sub
    End If
    Set Tfile = FSys.OpenTextFile(sFname, ForReading, False,
TristateFalse)
   TextOfFile = Tfile.ReadAll
    Tfile.Close
TextOfFile = LCase(TextOfFile)
```

```
Перестановка TextOfFile, CryptoText
    Set Tfile =
FSys.CreateTextFile(Application.GetSaveAsFilename("Расшифрованны
й текст", fileFilter:="Текстовые файлы (*.txt), *.txt"))
        Tfile.Write CryptoText
    Tfile.Close
Set Tfile = Nothing
Set FSys = Nothing
End Sub

Private Sub CommandButton3_Click()
'закрыть форму
UserForm1.Hide
End Sub
```

При нажатии кнопки «Зашифровать файл» («Расшифровать файл») появится окно «Открытие документа». При помощи этого окна пользователь может выбрать требуемый файл. Нажатие кнопки «Открыть» приведет к тому, что выбранный текстовый файл будет загружен в буфер обмена. В коде также осуществляется проверка на пустоту выбранного файла. Если файл не выбран, то на экран выводится диалоговое окно с сообщением. Для корректной работы программы необходимо установить ссылку на Microsoft Scripting Runtime в диалоговом окне References – VBA Project, которое отображается на экране выбором команды Tools/ References.

Правильность работы шифраторов проверить:

1) поместить зашифрованный файл на рабочий стол и сравнить его содержание с исходным файлом.

2) с помощью шифратора расшифровать зашифрованный файл, поместить его на рабочий стол и сравнить его содержание с содержанием исходного файла.

Для промежуточной отладки может быть использован отладчик Debug.

Лабораторная работа № 7

Тема: создание пользовательской формы – Вычисление хеш-функции.

Задача: создать пользовательскую форму, вычисляющую хеш-функцию произвольного текста.

Формализация задачи. Определим исходные и выходные данные.

a) Исходные данные – Входной текст, состоящий из слов русского языка.
b) Выходные данные – вычисленная хеш-функция. Длина хеш-кода должна составлять 256 бит.

Разработка алгоритма. Для решения поставленной задачи создается пользовательская форма с программным кодом, позволяющим для исходного текста составить хеш-функцию. Расчет хеш-функции выполняется на основе создания случайных значений начального хэша и хэш-модуля.

Реализация алгоритма на ЭВМ

1 Откройте документ Microsoft Excel.

2 Выполните команду Сервис/Макрос/Редактор Visual Basic.

3 Выберите команду Insert/UserForm. В редакторе Visual Basic появятся: окно пользовательской формы и панель инструментов Панель элементов.

4 Используя диалоговое окно Свойства (для вызова этого окна, если оно отсутствует, выполните команду View/Properties Windows) и Панель элементов, простым перетаскиванием элементов управления на форму, создайте пользовательскую форму в виде, представленном на рис. 17.

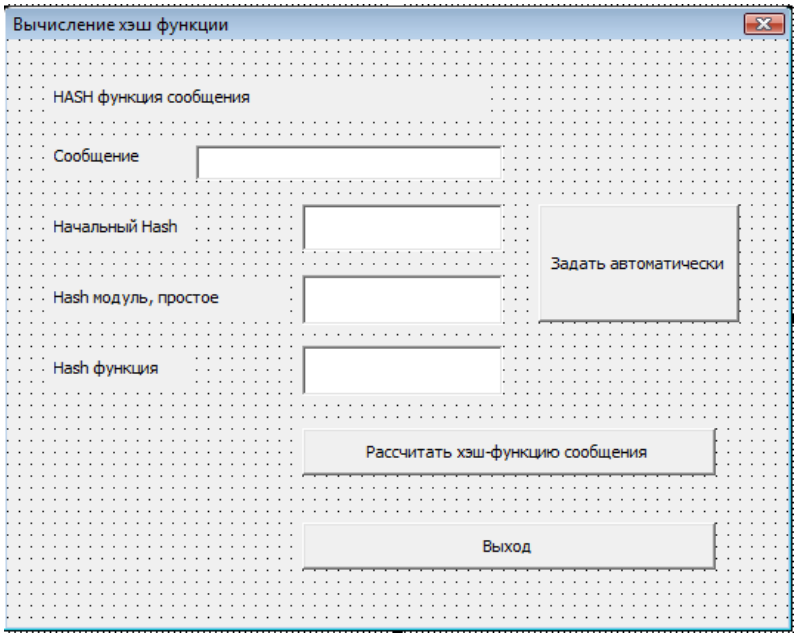

Рис. 17

5 Процедуру обработки событий нажатия кнопки «Задать автоматически», позволяющую рассчитать начальные значения начального хэша и хэш-модуля, введем в окно редактирования кода

```
Private Sub CommandButton2_Click()
K = 0
Randomize
Z = Round(1000 * Rnd())
I = 1
D = 0
While K <> 1
For I = 1 To Z
If (Z \ I) = (Z / I) Then D = D + 1
Next I
If D = 2 Then K = 1: GoTo 1 Else Z = Z - 1: K = 0: D = 0
Wend
1: H0 = Z
TextBox2.Text = H0

K = 0
Randomize
Z = Round(1000 * Rnd())
I = 1
D = 0
While K <> 1
For I = 1 To Z
If (Z \ I) = (Z / I) Then D = D + 1
Next I
```

```
If D = 2 Then K = 1: GoTo 2 Else Z = Z - 1: K = 0: D = 0
Wend
2: P = Z
TextBox3.Text = P
TextBox4.Text = ""
End Sub
```

6 Процедуру обработки событий нажатия кнопки «Рассчитать хеш-функцию сообщения» введем в окно редактирования кода

```
Dim S As String
Dim m() As Integer
Dim H0, H, P, Z, K, D As Integer
Private Sub CommandButton1_Click()
S = TextBox1.Text
H0 = Val(TextBox2.Text)
P = Val(TextBox3.Text)
If S = "" Then
       MsgBox ("Задана пустая строка сообщения")
       End If
If H0 = 0 Then
       MsgBox ("Не задан начальный хэш")
       End If
If P = 0 Then
       MsgBox ("Не задан хэш модуль")
       End If

For I = 1 To Len(S)
ReDim m(I)
m(I) = Val(Mid(S, I, 1))
Next

For I = 1 To Len(S)
H = ((m(I) + H0) ^ 2) Mod P
H0 = H
Next
TextBox4.Text = H
End Sub
```

7 Процедуру обработки событий нажатия кнопки «Выход» запишем в окно редактирования кода

```
Private Sub CommandButton3_Click()
'закрыть форму
UserForm1.Hide
TextBox1.Text = ""
TextBox2.Text = ""
TextBox3.Text = ""
TextBox4.Text = ""
End Sub
```

8 В результате введения исходного текста сообщения и выполнения операций автоматического задания начальных значений начального хэша и хэш-

модуля после нажатия кнопки «Шифровать» диалоговое окно примет вид, показанный на рис. 18.

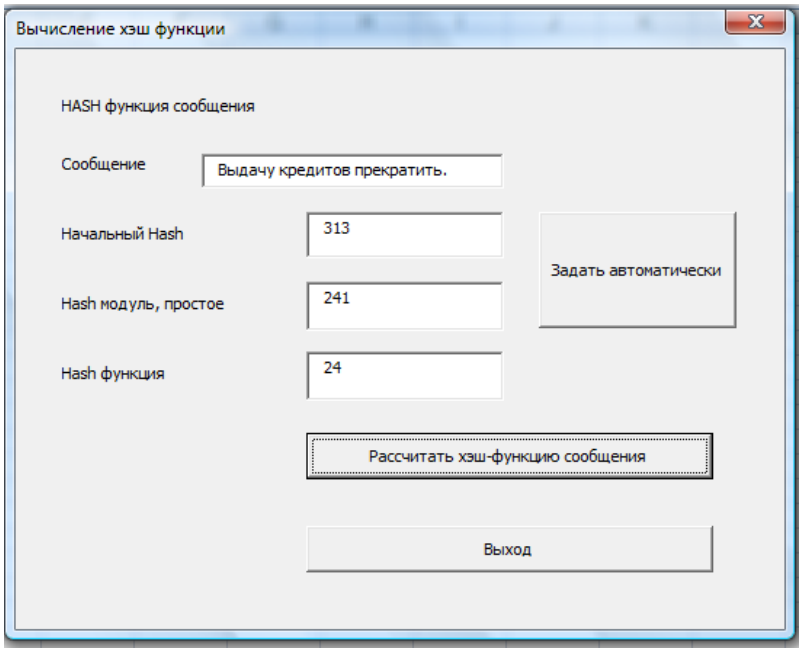

Рис. 18

9 Нажатие кнопки «Выход» приведет к закрытию формы.

Лабораторная работа № 8

Тема: вычисление хеш-функции по заданному варианту.

Поэкспериментируйте с созданной в лабораторной работе № 7 пользовательской формой, задавая различные начальные значения начального хэша и хэш-модуля для одного и того же текста сообщения. Объясните, почему так происходит? Отвечает ли созданная в лабораторной работе 7 хеш-функция всем необходимым требованиям, предъявляемым к хеш-функции?

Поэкспериментируйте с созданной пользовательской формой, задавая различные исходные сообщения: сообщения, содержащие числа, сообщения на английском или немецком языках. Проанализируйте результат.

Индивидуальные задания по лабораторной работе № 8

Вычислите по своему варианту задания хеш-функцию для выражения, приведенного в табл. 5.

Лабораторная работа № 9

Тема: создание пользовательской формы, реализующей алгоритм шифра RSA.

Задача. По двум простым числам p, q вычислить число n, равное произведению p и q ($n = pq$), а также сгенерировать случайным образом целое число E, взаимно простое с произведением $(p - 1)(q - 1)$ и секретный ключ D. Используя секретный ключ D, зашифровать произвольное числовое сообщение (таким сообщением может быть хеш-функция некоторого текстового сообщения).

С целью проверки правильности выполнить расшифровку сообщения.

Формализация задачи. Определим исходные и выходные данные.

Исходные данные – число m, удовлетворяющее требованию m≤ n – 1, два простых числа p, q.

Выходные данные – секретный ключ шифрования D, пара целых чисел – открытый ключ: n и E, а также зашифрованное и расшифрованное исходное число m.

Разработка алгоритма. Для решения поставленной задачи создадим программу, позволяющую вычислить открытый ключ: n и E и соответствующий ему секретный ключ D, считать содержимое исходного числового сообщения и с помощью программы осуществить шифрование и расшифровывание с использованием полученных ключей. Для удобства пользователя создадим процедуру, которая выводит в окно формы таблицу простых чисел.

Реализация алгоритма на ЭВМ. Спроектируем форму пользователя.

1 Откройте документ Microsoft Excel.

2 Выполните команду Сервис/Макрос/Редактор Visual Basic.

3 Выберите команду Insert/UserForm. В редакторе Visual Basic появятся: окно пользовательской формы и панель инструментов Панель элементов.

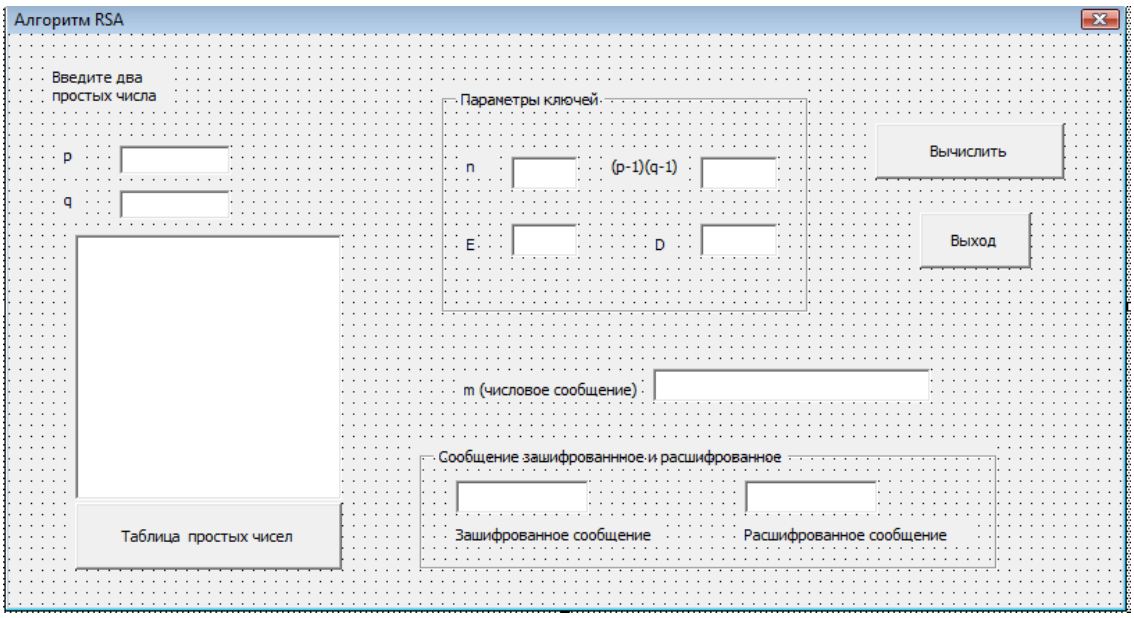

Рис. 19

4 Используя диалоговое окно Свойства (для вызова этого окна, если оно отсутствует, выполните команду View/Properties Windows) и Панель элементов, простым перетаскиванием элементов управления на форму, создайте пользовательскую форму в виде, представленном на рис. 19.

5 С созданной формой свяжите следующий программный код, обеспечивающий выполнение операций, реализуемых при нажатии на кнопках формы.

```
Option Explicit
Private Sub CommandButton1_Click()
If Not IsNumeric(Text1.Text) Then
MsgBox ("введите число p")
```

```
Return
End If
If Not IsNumeric(Text2.Text) Then
MsgBox ("введите число q")
Return
End If
If Not IsNumeric(Text7.Text) Then
MsgBox ("введите число m")
Return
End If
Dim p As Long, q As Long, n As Long, e As Long, PHI As Long, d
As Long, m As Long, c As Long
p = Text1.Text
q = Text2.Text
If (check_prime(p) = False) Then
    MsgBox ("p слишком велико или не является про-
стым,обратитесь к таблице простых чисел")
Else
    If (check_prime(q) = False) Then
        MsgBox ("q слишком велико или не является про-
стым,обратитесь к таблице простых чисел")
    Else
        n = p * q
        Text3.Text = n
        PHI = (p - 1) * (q - 1)
        e = getE((PHI))
        d = getD((e), (PHI))
        Text4.Text = PHI
        Text5.Text = d
        Text6.Text = e
        m = Text7.Text
        If m > n - 1 Then MsgBox ("число m не может быть за-
шифровано"): GoTo 1
        If m ^ e > 2147483647 Then MsgBox ("число m не может
быть зашифровано, в данной программе"): GoTo 1
        c = (m ^ e) Mod n
        Text8.Text = c
        m = decrypt(c, n, d)
        Text9.Text = m
        Label12.Caption = "Ключ дешифрования =<" + Str(d) +
"," + Str(n) + ">"
        Label13.Caption = "Ключ шифрования   =<" + Str(e) +
"," + Str(n) + ">"
    End If
End If
1:
End Sub


Private Function check_prime(ByVal val As Long) As Boolean
Dim primes, i As Integer, prime As Boolean
primes = Array(1, 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37,
41, 43, 47, 53, _
```

```
    59, 61, 67, 71, 73, 79, 83, 89, 97, 101, 103, 107, 109,
113, 127, 131, 137, _
    139, 149, 151, 157, 163, 167, 173, 179, 181, 191, 193,
197, 199, 211, 223, 227, _
    229, 233, 239, 241, 251, 257, 263, 269, 271, 277, 281,
283, 293, 307, 311, 313, _
    317, 331, 337, 347, 349, 353, 359, 367, 373, 379, 383,
389, 397)
check_prime = False
For i = 0 To 78
    If (val = primes(i)) Then
        prime = True
    End If
Next i
check_prime = prime
End Function


Private Function decrypt(ByVal c As Long, ByVal n As Long,
ByVal d As Long) As Long
Dim i As Long
Dim g As Long
Dim f As Long
On Error GoTo errorhandler
If (d Mod 2 = 0) Then
    g = 1
Else
    g = c
End If
For i = 1 To Int(d / 2)
    f = c * c Mod n
    g = f * g Mod n
Next i
decrypt = g
Exit Function

errorhandler:
Select Case Err.Number
    Case 6
        Status.Text = "Переполнение, задайте меньшие значения"
    Case Else
        Status.Text = "Ошибка вычисления"
End Select
End Function


Private Function getD(ByVal e As Long, ByVal PHI As Long) As
Long
Dim u(3) As Long
Dim v(3) As Long
Dim q As Long
Dim temp1 As Long
Dim temp2 As Long
```

```
Dim temp3 As Long
u(0) = 1: u(1) = 0: u(2) = PHI: v(0) = 0: v(1) = 1: v(2) = e
While (v(2) <> 0)
    q = Int(u(2) / v(2))
    temp1 = u(0) - q * v(0)
    temp2 = u(1) - q * v(1)
    temp3 = u(2) - q * v(2)
    u(0) = v(0)
    u(1) = v(1)
    u(2) = v(2)
    v(0) = temp1
    v(1) = temp2
    v(2) = temp3
Wend
If (u(1) < 0) Then
    getD = (u(1) + PHI)
Else
    getD = u(1)
End If
End Function


Private Function getE(ByVal PHI As Long) As Long
Dim great As Long
Dim e As Long
great = 0
e = 2

While (great <> 1)
    e = e + 1
    great = get_common_denom(e, PHI)
Wend
getE = e
End Function


Private Function get_common_denom(ByVal e As Long, ByVal PHI
As Long) As Long

Dim great As Long, temp As Long, a As Long
If (e > PHI) Then
    While (e Mod PHI <> 0)
        temp = e Mod PHI
        e = PHI
        PHI = temp
    Wend
    great = PHI
Else
    While (PHI Mod e <> 0)
        a = PHI Mod e
        PHI = e
        e = a
    Wend
```

```
    great = e
End If
get_common_denom = great
End Function


Private Sub show_primes()
Dim no_primes As Long, i As Long, prime As Boolean, j As Long
Status.Text = "1"
no_primes = 1
For i = 2 To 400
    prime = True
    For j = 2 To (i / 2)
        If ((i Mod j) = 0) Then
            prime = False
        End If
    Next j
    If (prime = True) Then
        no_primes = no_primes + 1
        Status.Text = Status.Text + ", " + Str(i)
    End If
Next i
Status.Text = Status.Text + vbCrLf + "Количество первых про-
стых чисел:" + Str(no_primes)
End Sub


Private Sub CommandButton2_Click()
Unload Me
'при закрытии формы очищаем текстовые поля
Text1.Text = ""
Text2.Text = ""
Text3.Text = ""
Text4.Text = ""
Text5.Text = ""
Text6.Text = ""
Text7.Text = ""
Text8.Text = ""
Text9.Text = ""
End Sub


Private Sub CommandButton4_Click()
'обращение к процедуре вывода простых чисел в поле формы
Call show_primes
End Sub
```

6 В результате нажатия кнопки «Таблица простых чисел» диалоговое окно примет вид, показанный на рис. 20.

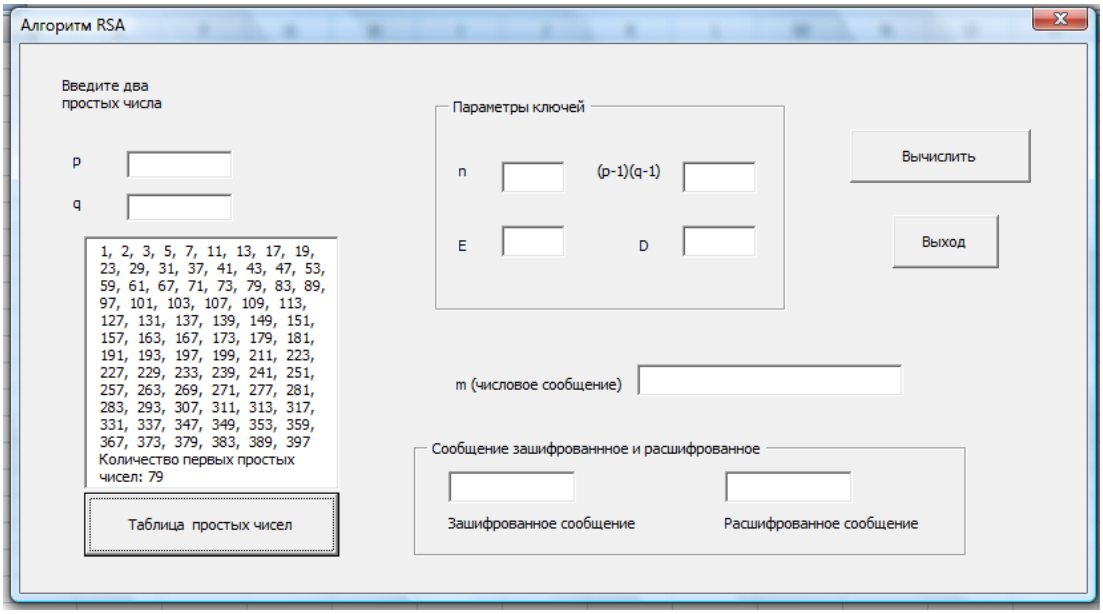

Рис. 20

7 В итоге введения исходного текста сообщения и двух простых чисел *p*, *q* после нажатия кнопки «Вычислить» диалоговое окно примет вид, показанный на рис. 21.

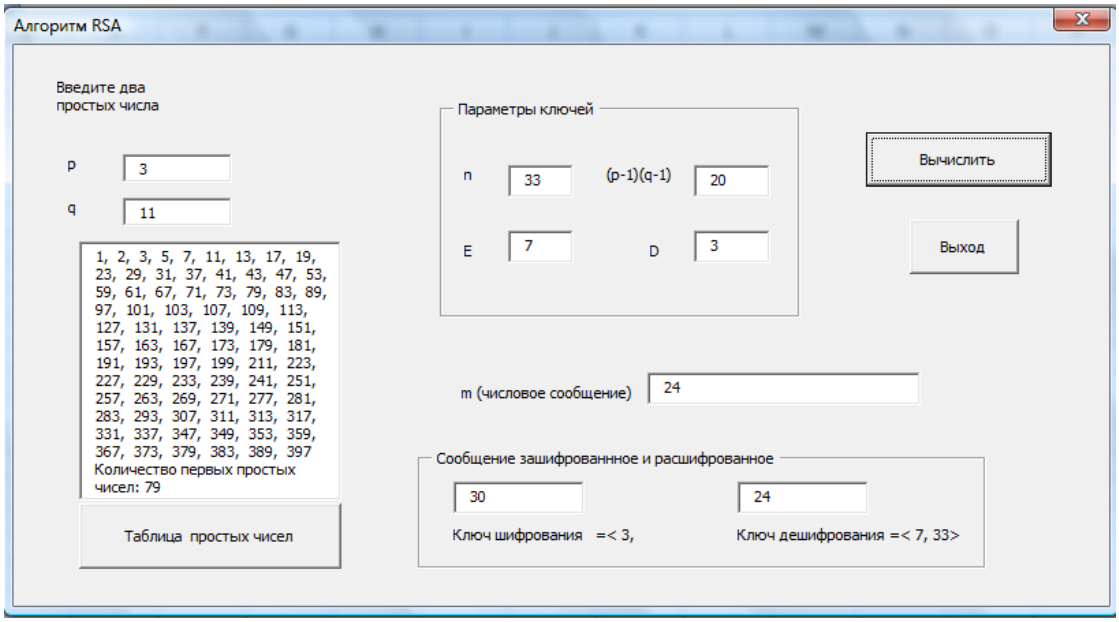

Рис. 21

8 Нажатие кнопки «Выход» приведет к закрытию формы.

Индивидуальные задания по лабораторной работе № 9

Задание 1. Поэкспериментируйте с созданной пользовательской формой, задавая различные начальные *p*, *q* для одного и того же текста сообщения. Проанализируйте результаты.

Задание 2. Поэкспериментируйте с созданной пользовательской формой, задавая различные исходные сообщения. Проанализируйте результаты.

Задание 3. Для вычисленной по своему варианту в индивидуальном задании к лабораторной работе № 7 хеш-функции выражения, приведенного в табл. 15, рассчитайте с использованием созданной в лабораторной работе № 8 формы

значения открытого ключа: n и E и соответствующего ему секретного ключа D для пары $p = 3$, $q = 11$. Проанализируйте результат.

Лабораторная работа № 10

Тема: симметричные криптосистемы.

Цель работы: разработать криптографическую защиту информации, содержащейся в файле данных, с помощью алгоритма шифрования, указанного в варианте. Для этого:

1 Разработать алгоритмы шифрования и дешифрования блока (потока) открытого текста заданной длины из алфавита Zn на заданном ключе с помощью метода, указанного в варианте (Если это позволяет алгоритм, длину блока взять кратной 8 бит).

2 Определить алфавит криптосистемы (открытого текста и шифротекста). Если алфавит не задан в варианте, выбрать его самостоятельно, так, чтобы он включал в себя символы используемого в примере открытого текста. Например, русский, английский, ASCII. Поставить символам исходного алфавита в соответствие символы из алфавита Zn (n – основание алфавита).

3 Написать программу генерации случайных ключей шифра, оценить размерность ключевого пространства.

4 Написать программу, реализующую шифрование на заданном ключе открытого текста, состоящего из символов заданного алфавита. Открытый текст, ключ и шифротекст должны быть представлены отдельными файлами.

5 Написать программу для реализации алгоритма дешифрования полученного файла шифротекста при известном ключе.

6 Провести тестирование программ:

a) на коротких тестовых примерах;

b) на текстах в несколько страниц.

Лабораторная работа № 11

Тема: криптоанализ симметричных криптосистем.

Задача. Провести эксперимент по определению практической стойкости, алгоритма, разработанного в лабораторной работе 9.

Считать, что противнику известен алгоритм шифрования. Выбрать наилучший с его точки зрения алгоритм подбора ключа и обосновать свой выбор.

Использовать методы:

- анализа статистических свойств шифротекста (частот появления букв);
- силовую атаку (полный перебор ключей);
- другие (если есть более эффективные).

С помощью программы, реализующей выбранный алгоритм криптоанализа, провести эксперимент по вскрытию шифротекстов различного размера. При использовании статистического криптоанализа использовать табл. 5 и табл. 6 или подсчитать частоты появления букв используемого алфавита в тексте, частью которого является текст примера. Для проверки на «осмысленность» по-

лученного текста создать мини-словарь из части слов, встречающихся в тексте примера.

Построить графики зависимости времени криптоанализа от параметров алгоритма шифрования (длины или других параметров ключа, размера шифротекста или др., в зависимости от алгоритмов шифрования и криптоанализа).

Проведите эксперимент по определению параметров, необходимых для практической криптостойкости алгоритма шифрования, разработанного в лабораторной работе № 9. А именно: размер передаваемого текста, размер и характеристики ключа, объем ключевого пространства и другие параметры алгоритма шифрования. Практической криптостойкостью в данной работе будем считать невозможность взлома шифра противником, имеющим в распоряжении один ПК мощности, равной мощности компьютера, на котором делалась работа, и один час времени.

Индивидуальные задания по лабораторным работам № 10, 11

Таблица 16

№	Задание	№	Задание
1	Шифрующие таблицы с числовым ключом	13	Аффинная система подстановок Цезаря
2	Шифр Гронсфельда с ключевым словом	14	Шифр Вижинера с числовым ключом
3	Алгоритм, реализующий идею «диска Альберти» для русского алфавита.	15	Алгоритм, реализующий идею «диска Альберти» для английского алфавита
4	Шифр Цезаря с ключевым словом	16	Шифрующие таблицы Трисемуса
5	Шифрующие таблицы с перестановкой по ключу – размеру таблицы	17	Шифр гаммирования с генератором ключей на основе датчика случайных чисел
6	Полибианский квадрат для русского алфавита	18	Полибианский квадрат для английского алфавита
7	Шифр Гронсфельда с числовым ключом	19	Шифр Вижинера с ключевым словом
8	Шифр Кардано без поворотов	20	Шифр Вернама
9	Шифр Плейфера	21	Шифр Хилла для 3-грамм
10	Шифрующие таблицы с ключевым словом	22	Шифрующие таблицы с двойной перестановкой по ключевому слову
11	Шифр Цезаря многоалфавитный	23	Шифр Уинстона
12	Шифр гаммирования с линейным конгруэнтным генератором ключей	24	Шифрующие таблицы с двойной перестановкой по числовому ключу
	***Дополнительные варианты* (*повышенной сложности*):**		
25	Магические квадраты		
26	Шифр Кардано с поворотами		

Лабораторная работа № 12

Тема: криптографические протоколы на основе асимметричных криптосистем.

Разработать алгоритмы, реализующие криптографические протоколы (см. вариант задания) взаимодействия удаленных абонентов на основе асимметричных криптосистем.

Написать программы, реализующие эти протоколы для всех участников. Значения модуля криптосистемы выбирать не менее 50 бит. Для вычислений с большими числами можно использовать специальные программы. Для проверки чисел на простоту использовать комбинированный алгоритм на основе тестов Леманна или Рабина-Миллера. Хеширование выполнять на основе любого блочного симметричного алгоритма (например, с использованием сети Фейстеля или алгоритма из предыдущих лаб. работ) по одной из схем, данных в лекциях.

Проверить правильность выполнения протокола для малых значений параметров криптосистемы (контрольный пример).

Продемонстрировать выполнение протокола для нормальных значений параметров криптосистемы.

Индивидуальные задания по лабораторной работе № 12

Таблица 17

№	Задания	№	Задания
1	Протокол обмена секретным документом комбинированным методом шифрования на основе криптосистемы RSA	14	Протокол двустороннего подписания контракта на основе алгоритма цифровой подписи Эль Гамаля
2	Протокол двустороннего подписания контракта на основе алгоритма цифровой подписи ГОСТ Р 34.10-94	15	Протокол обмена несекретным документом с цифровой подписью на основе алгоритма ГОСТ Р 34.10-94
3	Протокол обмена несекретным документом с цифровой подписью на основе алгоритма RSA	16	Протокол двустороннего подписания контракта на основе алгоритма цифровой подписи RSA
4	Протокол обмена секретным документом, зашифрованным с помощью алгоритма RSA	17	Протокол обмена несекретным документом с цифровой подписью DSA
5	Протокол идентификации абонента с помощью алгоритма цифровой подписи DSA	18	Протокол обмена секретным документом с цифровой подписью на основе алгоритма RSA
6	Протокол обмена несекретным документом с невидимой цифровой подписью на основе алгоритма RSA	19	Протокол византийского соглашения для трех участников на основе схемы Шамира проверяемого разделения секрета

Окончание табл. 17

№	Задания	№	Задания
7	Протокол идентификации абонента с помощью алгоритма цифровой подписи ГОСТ Р 34.10-94	20	Протокол обмена несекретным документом с цифровой подписью на основе алгоритма Эль Гамаля
8	Протокол генерации сеансового секретного ключа на основе криптосистемы RSA	21	Протокол экспоненциального ключевого обмена по методу Диффи-Хеллмана
9	Протокол двустороннего подписания контракта на основе алгоритма цифровой подписи DSA	22	Протокол вычисления дискретного логарифма со скрытием информации от оракула
10	Протокол обмена несекретным документом со слепой цифровой подписью на основе алгоритма RSA	23	Протокол обмена секретным документом, зашифрованным с помощью алгоритма Эль Гамаля
11	Протокол аутентификации Шнорра	24	Протокол «подбрасывания монеты по телефону»
12	Протокол идентификации абонента с помощью алгоритма цифровой подписи RSA	25	Протокол идентификации абонента с помощью алгоритма цифровой подписи Эль Гамаля
13	Протокол вычисления ключа доступа при разделении секрета между тремя участниками по схеме Шамира проверяемого разделения секрета	26	Протокол обмена секретным документом комбинированным методом шифрования на основе экспоненциального ключевого обмена по методу Диффи-Хеллмана

Библиографический список

1 **Герман, О.Н.** Теоретико-числовые методы в криптографии : учебник для вузов / О.Н. Герман, Ю.В. Нестеренко. – М. : Академия, 2012. – 271 с.
2 **Родичев, Ю.А.** Информационная безопасность: нормативно-правовые аспекты : учеб. пособие для вузов / Ю.А. Родичев. – М.; СПб. : Питер, 2008. – 271 с.
3 **Расторгуев, С.П.** Основы информационной безопасности : учеб. пособие для вузов / С.П. Расторгуев. – М. : Академия, 2007. – 187 с.
4 **Куприянов, А.И.** Основы защиты информации : учеб. пособие для вузов / А.И. Куприянов, А.В. Сахаров, В.А. Шевцов. – 2-е изд., стер. – М. : Академия, 2007. – 254 с.
5 **Доманский, В.В.** Компьютерные технологии и информатика : учеб.-метод. пособие / В.В. Доманский, Ф.К. Голубев, Т.В. Потанина. – М., 2014. – 54 с.
6 **Мамаев, Э.А.** Информационная безопасность и защита информации : метод. указ. к лаб. работам / Э.А. Мамаев, Т.В. Потанина. – Ростов н/Д : РГУПС, 2007. – 37 с.
7 **Доманский, В.В.** Информационные системы : метод. указ. к лаб. работам / В.В. Доманский. – Ростов н/Д : РГУПС, 2006. – 27 с.
8 Введение в криптографию / под общ. ред. В.В. Ященко. – М. : МЦНМО, «ЧеРо», 1998.
9 **Ерош, И.Л.** Дискретная математика. Математические вопросы криптографии : учеб. пособие / И.Л. Ерош. – СПб. : СПбГУАП, 2001.
10 **Пазизин, С.В.** Основы защиты информации в компьютерных системах / С.В. Пазизин. – М. : ТВП/ОПиПМ, 2003. – 178 с.
11 **Пазизин, С.В.** Основы защиты информации в компьютерных системах : учеб. пособие / С.В. Пазизин. – М. : ТВП, 2001.
12 **Проскурин, Г.В.** Принципы и методы защиты информации / Г.В. Проскурин. – М. : МИЭМ, 1997.
13 **Рябко, Б.Я.** Криптографические методы защиты информации / Б.Я Рябко, А.Н. Фионов. – М .: Горячая линия – Телеком, 2005.
14 **Саломаа, А.** Криптография с открытым ключом / А. Саломаа. – М. : Мир, 1996.
15 **Сычев, Ю.Н.** Основы информационной безопасности / Ю.Н. Сычев. – М. : 2006.
16 **Шеннон, К.** Предсказание и энтропия печатного английского текста. В кн. Работы по теории информации и кибернетике / К. Шеннон. – М. : Иностранная литература, 1963.
17 **Шеннон, К.** Теория связи в секретных системах. В кн. Работы по теории информации и кибернетике / К. Шеннон. – М. : Иностранная литература, 1963.
18 **Корниенко, А.А.** Информационная безопасность и защита информации на железнодорожном транспорте : учеб. для вузов. В 2 ч. Ч. 1. Методология и система обеспечения информационной безопасности на железнодорожном

транспорте / Учеб.-метод. центр по образованию на ж.-д. трансп. / А.А. Корниенко ; ред. А.А. Корниенко. – М., 2014. – 435 с.

19 **Корниенко, А.А.** Информационная безопасность и защита информации на железнодорожном транспорте : учебник для вузов. В 2 ч. Ч. 2. Программно-аппаратные средства обеспечения информационной безопасности на железнодорожном транспорте / Учеб.-метод. центр по образованию на ж.-д. трансп. / А.А. Корниенко ; ред. А. А. Корниенко. – М., 2014. – 447 с.

20 **Корниенко, А.А.** Средства защиты информации на железнодорожном транспорте (Криптографические методы и средства) : учеб. пособие для вузов ж.-д. трансп / А.А. Корниенко, М.А. Еремеев, С.Е. Ададуров ; ред. А.А. Корниенко. – М. : Маршрут, 2006. – 253 с.

21 **Скиба, В.Ю.** Руководство по защите от внутренних угроз информационной безопасности : научное издание / В.Ю. Скиба, В.А. Курбатов. – М. ; СПб. : Питер, 2008. – 319 с.

22 **Гуда, А.Н.** Информатика. Общий курс : учебник для вузов / А.Н. Гуда, М.А. Бутакова, Н.М. Нечитайло, А.В. Чернов ; ред. В.И. Колесников. – 4-е изд. – М. : Дашков и К° ; Ростов н/Д : Наука-Спектр, 2011. – 399 с.

23 **Романова, Ю.Д.** Информатика и информационные технологии : учеб. пособие / Ю.Д. Романова, П.А. Музычкин, И.Г. Лесничая и [др.]; ред. Ю.Д. Романова. – 5-е изд., испр. и доп. – М. : Эксмо, 2011. – 704 с.

24 **Могилев, А.В.** Информатика : учеб. пособие для вузов / А.В. Могилев , Н.И. Пак, Е.К. Хеннер ; ред. Е.К. Хеннер. – 2-е изд., стер. – М. : Академия, 2012. – 841 с.

25 **Бутакова, М.А.** Основы информатики : учеб. пособие / М.А. Бутакова, А.Н. Гуда. – Ростов н/Д : РГУПС, 2004. – 84 с.

26 **Бутакова, М.А.** Информационные технологии : метод. указ. к лаб. работам. Ч. 1 / М.А. Бутакова, А.В. Чернов. – Ростов н/Д : РГУПС, 2001. – 64 с.

27 **Чернов, А.В.** Информационные технологии : метод. указ. к лаб. работам. Ч. 2 / А.В. Чернов, М.А. Бутакова. – Ростов н/Д : РГУПС, 2001. – 48 с.

28 **Нечитайло, Н.М.** Информатика. Эффективная работа с Microsoft Office / Н.М. Нечитайло, Т.В. Потанина. – Ростов н/Д : РГУПС, 2003. – 142 с.

29 **Бутакова, М.А.** Практикум по Excel : учеб. пособие / М.А. Бутакова, И.В. Дегачева, А.А. Чекулаева. – Ростов н/Д : РГУПС, 2000. – 60 с.

30 **Доманский, В.В.** Компьютерные сети. Интернет. Защита информации : учеб. пособие / В.В. Доманский. – Ростов н/Д : РГУПС, 2004. – 70 с.

31 **Куприянов, А.И.** Основы защиты информации : учеб. пособие для вузов / А.И. Куприянов, А.В. Сахаров, В.А. Шевцов. – 2-е изд., стер. – М. : Академия, 2007. – 254 с.

32 **Бутакова, М.А.** Информационные технологии в управлении : учеб. пособие / М.А. Бутакова, В.В. Доманский, Т.В. Потанина, Л.Н. Педченко. – Ростов н/Д, 2014. – 100 с.

Содержание

Учебное издание

Доманский Василий Валерьевич
Чернов Андрей Владимирович

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ И ЗАЩИТА ИНФОРМАЦИИ

Редактор Н.С. Федорова
Техническое редактирование и корректура Н.С. Федоровой

Подписано в печать 08.09.16. Формат 60×84/16.
Бумага газетная. Ризография. Усл. печ. л. 2,6.
Тираж экз. Изд. № 53. Заказ .

Редакционно-издательский центр ФГБОУ ВО РГУПС.

Адрес университета: 344038, г. Ростов н/д, пл. Ростовского Стрелкового Полка Народного Ополчения, 2.