МИНОБРНАУКИ РОССИИ
Федеральное государственное бюджетное
образовательное учреждение высшего образования
«Юго-Западный государственный университет»
(ЮЗГУ)

Кафедра информационной безопасности

УТВЕРЖДАЮ
Проректор по учебной работе
_____ О.Г. Локтионова
«19» 04 2021 г.

ШИФРОВАНИЕ С ПОМОЩЬЮ ТАБЛИЦЫ ВИЖЕНЕРА

Методические указания по выполнению практических работ
для студентов направления подготовки (специальности)
02.03.03 математическое обеспечение и администрирование
информационных систем

Курск 2021

2

УДК 004.56.5(076.5)
Составитель: А.Л. Марухленко, А.Л. Ханис

Рецензент
Кандидат технических наук, доцент кафедры
информационной безопасности А.Г. Спеваков

Шифрование с помощью таблицы Виженера : методические указания по выполнению практических работ студентов всех форм обучения / Юго-Зап. гос. ун-т; сост.: А.Л. Ханис. - Курск, 2021. - 19 с. Библиогр.: с. 19.

Содержат сведения по вопросам шифрования и расшифрования с помощью таблицы Виженера. Указывается порядок выполнения практической работы, пример выполнения работы, правила оформления, содержание отчета, варианты заданий.

Методические указания соответствуют требованиям программы по направлению подготовки бакалавров: математическое обеспечение и администрирование информационных систем.

Предназначены для студентов направления подготовки бакалавров 02.03.03.

Текст печатается в авторской редакции

Подписано в печать 19.04.21. Формат 60x84 1/16.
Усл.печ. л. 1,1 Уч.-изд. л. 1. Тираж 30 экз. Заказ. 825 Бесплатно.
Юго-Западный государственный университет.
305040, г. Курск, ул. 50 лет Октября, 94.

1. ЦЕЛЬ РАБОТЫ

Получение навыков создания зашифрованного сообщения при помощи алгоритма шифрования Виженера.

2. ТЕОРЕТИЧЕСКАЯ ЧАСТЬ

В целях изменения естественных статистических зачастую образование букв исходного алфавита применяются многоалфавитные шифры, которые подразделяются на несколько видов. В многоалфавитных подстановках для изменения символов первоначального текста используют несколько алфавитов. Зачастую, алфавиты, который используется в целях изменения первоначального алфавита, представляют из себя нечто иное как первоначальные алфавиты, зафиксированные в некотором порядке.

Рассмотрим метод многоалфавитной подстановки, принцип работы которого заключается в использовании таблицы Виженера. Данный метод образовался в 16 века, французский ученый Блез Виженер описал его в своем научном труде «Трактате о шифрах», который был опубликован в 1585 году.

В рассматриваемом криптографическом алгоритме шифрования данным методом многоалфавитных подстановок применяется квадратная матрица с числом элементов M*M, где M — число символов в первоначальном алфавите. В первую строку первоначальной квадратной матрицы вносятся буквы в точно такой же очередности, как и в первоначальном алфавите, в следующую строку записывают тот же последовательный набор букв, но уже с заданным сдвигом влево на одну позицию, в последующих строках повторяется сдвиг на одну позицию предыдущей строки.

Подготовка таблицы шифрования

АБВГДЕ.....ЭЮЯ
БВГДЕЖ.....ЮЯА
ВГДЕЖЗ.....ЯАБ
ГДЕЖЗИ.....АБВ
ДЕЖЭИК.....БВГ
ЕЖЗИКЛ.....ВГД

ЯАБВГД.....ЬЭЮ

Чтобы применить алгоритм шифрования к заданному тексту необходимо выбрать секретное состояние, которое представляет из себя определенное слово или случайный набор символов первоначального алфавита. Далее из заполненной квадратной матрицы выводят подматрицу шифрования. К данной таблице применим ключ шифрования «весна» и посмотрим на результат применения криптографического алгоритма.

Составление подматрицы шифрования

АБВГДЕЖЗИКЛМНОПРСТУФХЦЧШЩЪЫЬЭЮЯ
ВГДЕЖЗИКЛМНОПРСТУФХЦЧШЩЪЫЬЭЮЯАБ
ЕЖЗИКЛМНОПРСТУФХЦЧШЩЪЫЬЭЮЯАБВГД
НОПРСТУФХЦЧШЩЪЫЬЭЮЯАБВГДЕЖЗИКЛМ
СТУФХЦЧШЩЪЫЬЭЮЯАБВГДЕЖЗИКЛМНОПР

Во время применения алгоритма шифрования (рис.2) под каждой буквой первичного сообщения фиксируют символы секретного состояния (в данном случае набор букв «весна»), число повторений написания ключа фиксируется нужное число раз, соответствующее количеству символов первичного алфавита, затем первичный текст по таблице шифрования изменяют буквами, находящимися на пересечениях линий столбцов и строк, связывающий последующую букву первичного текста (рассматривается по столбцу) и последующую букву ключа шифрования (рассматривается по строке). Из этого следует, первая буква первичного текста «м», ей соответствует буква ключа шифрования «в», далее ищем указанные буквы по столбцам и строкам соответственно, и на их соединении находим букву зашифрованного текстового сообщения, в данном месте буква «о» и так далее [**Ошибка! Источник ссылки не найден.**].

Изучим обратный алгоритм расшифрования той же системой. Первичными данными являются секретный ключ «весна» и шифрованное сообщение «кекхтвоэцотссвил» (при шифровании

пробелы не использовались). Расшифрование сообщения выполняется методом, представленным ниже:

- в строку над буквами шифрованного сообщения поочередно вносят буквы ключа, число повторений написания ключа записывается нужное количество раз, равное числу символов шифрованного сообщения;

- в строке подматрицы шифрования таблицы Виженера для каждой буквы ключа находиться буква, равная знаку шифрованного сообщения. Расположенная над ней буква первой строки и будет тем знаком расшифрованного текста; выведенный набор символов группируется в слова.

Механизм расшифрования

КЛЮЧ	ВЕСНАВЕСНАВЕСНАВ
ЗАШИФРОВАННЫЙ ТЕКСТ	КЕКХТВОЭЦОТССВИЛ
РАСШИФРОВАННЫЙ ТЕКСТ	ЗАЩИТАИНФОРМАЦИИ
ИСХОДНЫЙ ТЕКСТ	ЗАЩИТА ИНФОРМАЦИИ

Найти криптографический алгоритм шифрования, составленный на таблице Виженера, методом схожим, что и одноалфавитной подстановки, нельзя, из-за того, что одни и те же символы открытого текста могут быть заменены различными символами зашифрованного текста. Но в то же время, разные буквы открытого текста могут быть изменены равными знаками зашифрованного текста.

Преимуществом представленного метода многоалфавитной подстановки способствует способ применение символов первичного текста по отношению к символам ключа. Любой из символов секретного ключа применяется для шифрования одного символа первичного сообщения. После применения всех символов

секретного ключа, они повторяются в том же порядке требуемое число раз, равные количеству символов исходного алфавита. Когда используется ключ число букв, которого равно десяти, то каждая десятая буква сообщения шифруется одинаковым символом ключа. Данный характеристика называется периодом шифра. При условии того что ключ шифрования состоит из одного символа, то при шифровании будет применяться одна строка таблицы Виженера, из этого следует что, в данном примере мы получим моноалфавитную подстановку, а именуется шифр Цезаря.

Для обеспечения увеличения надежности шифрования текста имеется возможность применить два или более шифрования по методу Виженера с разными ключами.

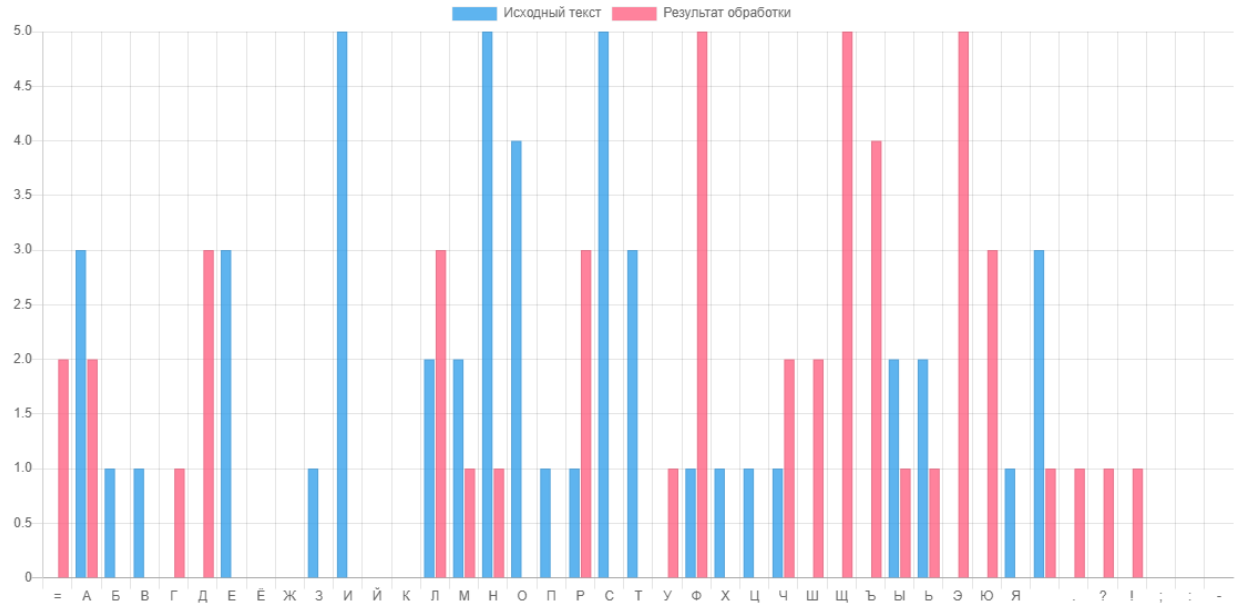


Рисунок 7 - Гистограмма распределения частот с применением шифра Цезаря

Рассмотрим применение метода Виженера для шифрования текста введения данного учебного пособия. При использовании алфавита, содержащего русские буквы и пробелы получилась выборка из 1400 символов, содержащая 162 слова. В качестве ключа возьмем слово «Криптография» и воспользуемся программной реализацией метода на базе web-технологий.

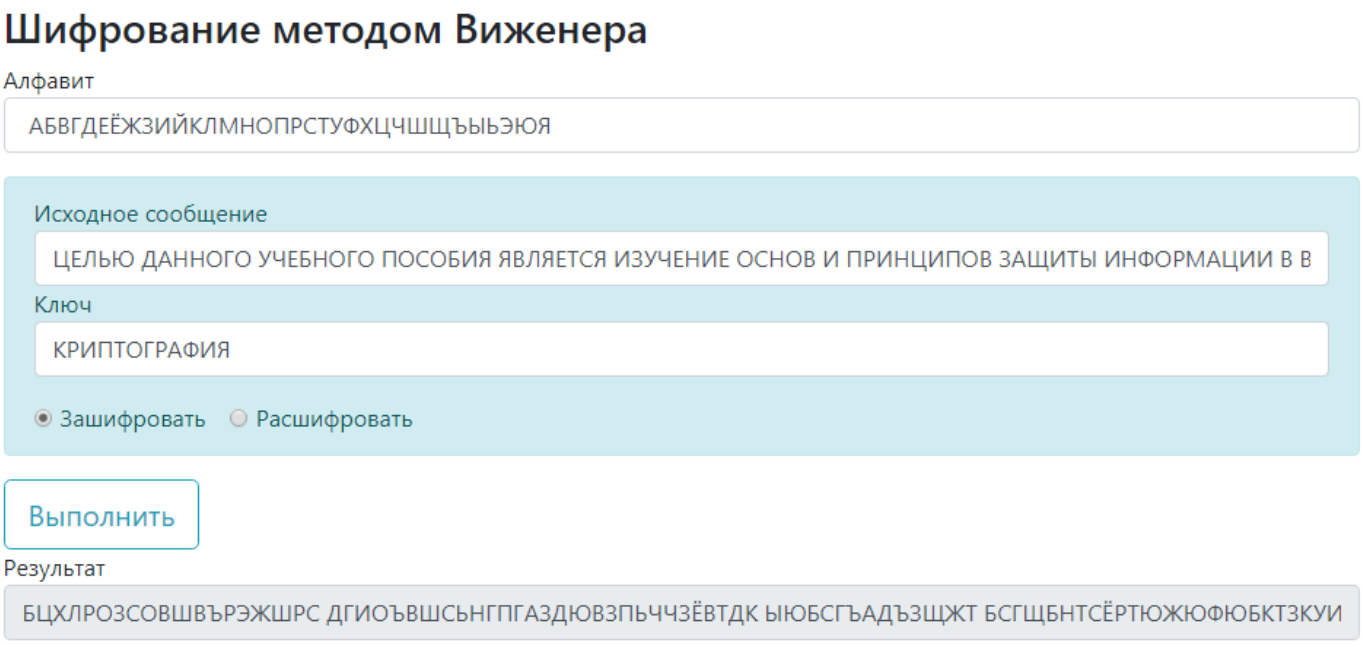


Рисунок 8 – Пример шифрования с использованием ключа

Для оценки распределения символов целесообразно применить метод частотного анализа исходного и результирующего текстов в виде радиальной и столбчатой диаграммы. Из графика следует, что применение даже небольшого по длине ключа позволило изменить статистику встречаемости символов. Радиальная диаграмма показывает равномерное распределение символов выходной последовательности с частотой, не превышающей 70 символов, в то время как исходный текст имеет большой разброс. Наиболее встречаемые символы – разделитель слов, буквы А, Е, И, Н, О.

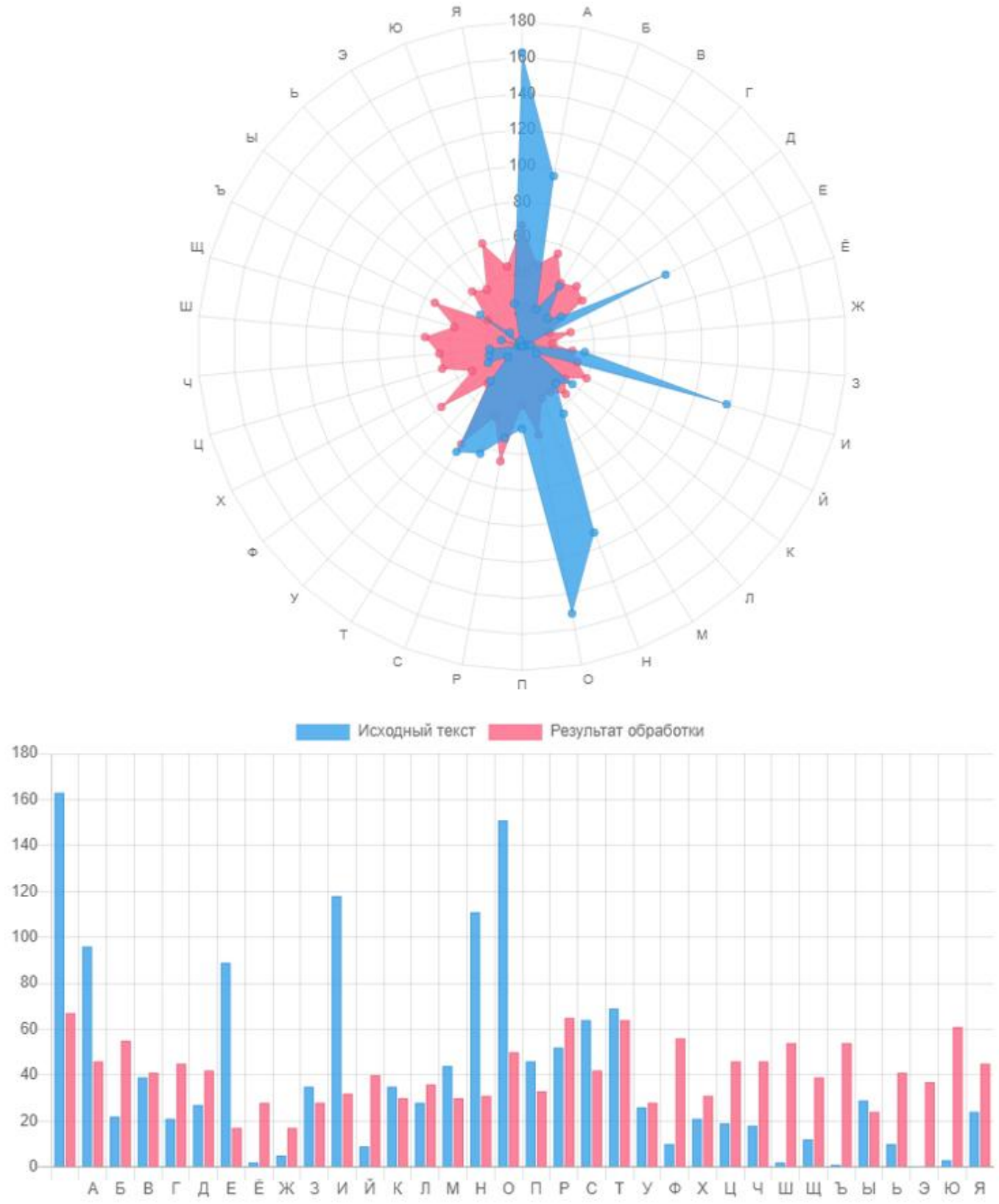


Рисунок 9 - Частотный анализ текста в виде радиальной и столбчатой диаграммы

В действительности, кроме метода Виженера применяются также разные модификации данного метода. К примеру, шифр Виженера с перемешанным один раз алфавитом. В данном примере для расшифрования сообщения адресату нужно знать порядок следования символов в таблице шифрования.

Шифр Виженера не сохраняет параметр частот возникновение символов в тексте, но определенные свойства образования символов в тексте остаются. Главный минус шифра Виженера это то что его ключ повторяется. Из этого следует что простой криптоанализ шифра может быть составлен в два этапа:

1. Поиск длины ключа. Анализ распределение частот в зашифрованном тексте с различным периодом. Нужно выбирать текст, в составе которого каждая 2-я буква зашифрованного текста, далее каждая 3-я и т.д. С момента когда распределение частот букв начнет сильно различаться от равномерного, то можно сделать вывод что нужная длинна ключа найдена.

2.Криптоанализ. Совокупность l шифров Цезаря (где l — найденная длина ключа), данный шифр ,по отдельности легко поддается взлому. В этом случае зашифрованный текст делится на m отличающийся друг от друга частей и используется метод, применяемый в криптоанализе аддитивного шифра, используя атаку частоты. Любая часть зашифрованного текста может быть расшифрована и соединена с другими, для того чтобы создать целый первичный текст. В полном объеме зашифрованный текст не сохраняет частоту отдельной буквы первоначального текста, но любая часть делает это. Один из вариантов повышения криптостойкости метода - сначала зашифровать исходное сообщение другим способом (например, перестановочным шифром) и только после этого применить метод Виженера. В этом случае, подбор ключа не даст осмысленную фразу поставит злоумышленника в тупик т.к. на выходе получится лишь бессмысленный набор букв. Идеальный вариант шифрования – использование одноразового ключа, сопоставимого по длине с исходным сообщением. В этом случае злоумышленник не сможет установить периодичность зацикливания [**Ошибка! Источник ссылки не найден.**].

Выполнение практических заданий предполагает навык

программирования и алгоритмизации. Приведем программный код функций, позволяющих осуществить шифрование методом Виженера на языке javaScript с использованием Bootstrap, jQuery, ChartJS. Преимуществом данной реализации является кроссплатформенность и свободное программное обеспечение. Структура проекта показано на рисунке 3.6 в левой части.

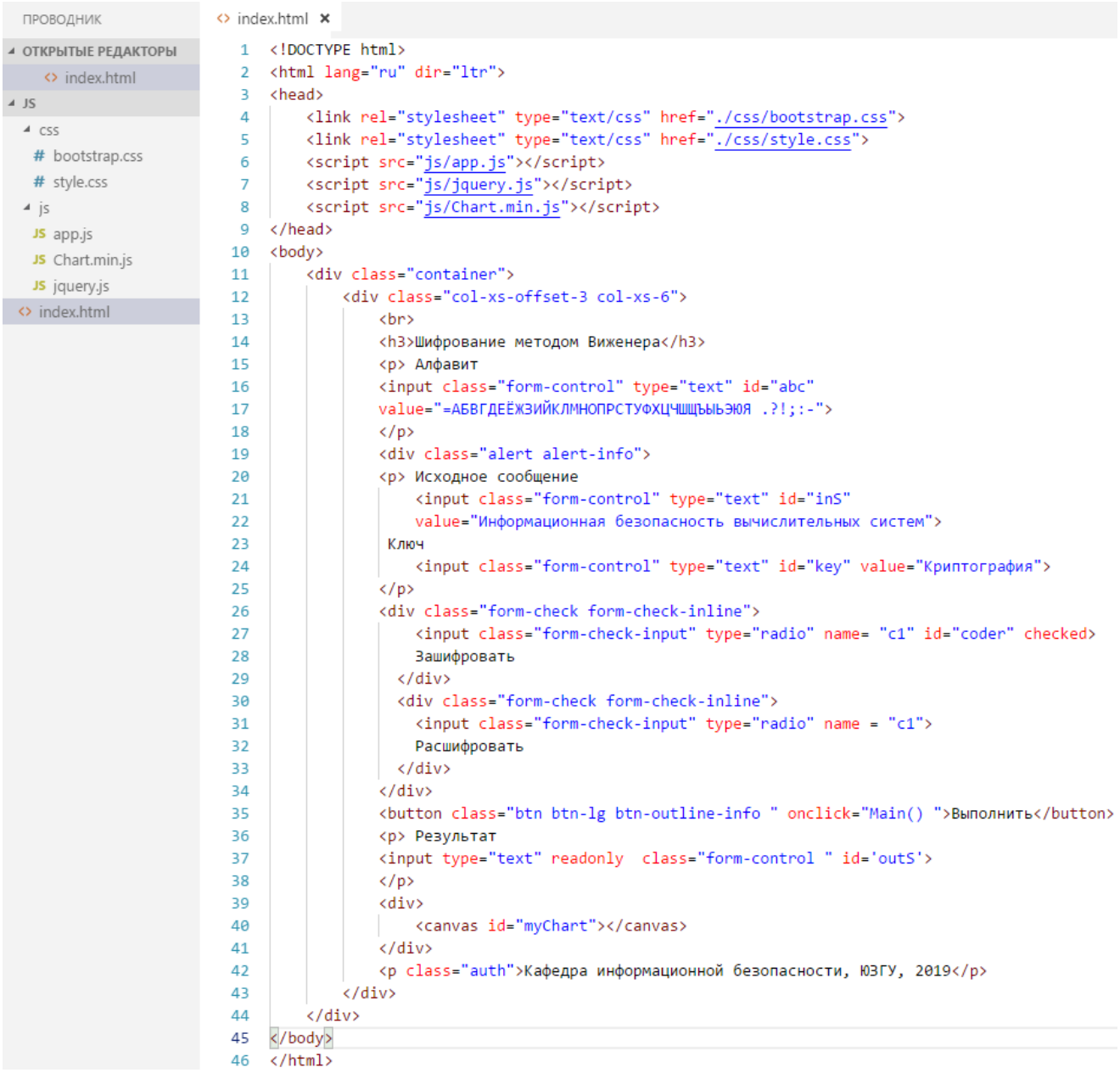


Рисунок 10 – Содержание интерфейсной части модуля

Логика обработки прописана в файле app.js, содержащего функцию приведения входных данных к алфавиту (StringToAbc),

непосредственное шифрование (Vig) и вызывающую функцию Main, в которой происходит построение гистограмм распределения символов [**Ошибка! Источник ссылки не найден.**].

```
function StringToAbc(v,abc){
 r='';
 for (i = 0; i < v.length; i++)
 if (abc.indexOf(v[i])>-1)
 r+=v[i];
 return r;
}

function Vig(v,key,abc,isCoder){
 while (key.length<v.length)
 key+=key;
 r='';
 for (i = 0; i < v.length; i++)
 {
 if (isCoder)
 x=(abc.indexOf(v[i])+abc.indexOf(key[i])) % abc.length
 else
 x=(abc.indexOf(v[i])-abc.indexOf(key[i])+abc.length) %
abc.length;
 r+=abc[x];
 }
 return r;
}

function Main() {
 abc = $('#abc').val().toUpperCase();
 inS = StringToAbc($('#inS').val().toUpperCase(),abc);
 $('#inS').val(inS);
 key = StringToAbc($('#key').val().toUpperCase(),abc);
 $('#key').val(key);
 outS = Vig(inS,key,abc,$('#coder').is(':checked'));
 $('#outS').val(outS);
 var ctx = $('#abc').getContext('2d');
 Horz = [];VIn = [];VOut = [];
 for(i=0;i<abc.length;i++){
 Horz.push(abc[i]);
 VIn.push(inS.split(abc[i]).length-1);
 VOut.push(outS.split(abc[i]).length-1);
 }
```

```
 myChart = new Chart(ctx, {
 type: 'bar',
 data: {
 labels:Horz,
 datasets: [{
 label: 'Исходный текст',
 data: VIn
 }, {
 label: 'Результат обработки',
 data: VOut
 }]
 },
 });
}
```

3. ВЫПОЛНЕНИЕ РАБОТЫ

В рамках практической работы необходимо расшифровать секретное сообщение (соответствует номеру индивидуального варианта) с использованием ключа. Известно, что алфавит мощностью 34 (содержит 34 символа) – для разделения слов используется знак равенства (имеет код ноль) и заглавные русские буквы А [1], Б [2]… Я [33]. Шифровка составлена путем сложения кодов исходного сообщения с соответствующими кодами ключа.

Порядок выполнения работы:

1. В соответствии с номером индивидуального варианта (порядковый номер студента по списку), в котором указан ключ и зашифрованное сообщение, необходимо произвести его расшифровку.
2. Сопоставить гистограммы распределения символов в открытом и зашифрованном тексте.
3. Зашифровать свой исходный текст (секретный вопрос или утверждение).

Список индивидуальных вариантов:

1) АНАПА
   ИТПАПГИКППВЯБШАЗЧИЮЙАЭУЮПТЧУХТЭНЛПТГЭЁ

ЭФААЁЬФААБЫАЛОЛПВФТУЯАГИАБПВЧСРЁУУТЛАЙ=РЯМ
ЭЦПТБУЙАХДПНЕЯАТАБПМЁА

2) АРБАТ

ОСЛЕЬУЦБМРЕЦЛАЮПГРСННЪБНБЗЯРАХПВЧЙЛБГЮТ
САЪБТЕББВКЕЁВЮАЬЦРССШГЩРКЕЙ

3) БИТВА

ПТЮСДЁЙТРЁБЭЦГЕВОКЯАМЬБВЕРЫЕСЙПИЧСГЖЪЬБА
УЙ=ЮЁБКЯЛИМТШВРРЪБМАСЪШЖБ=ЬТФБОДШВШХРЬЗАП
ОБЙЙЁЙАРПБЩБППЕЙРХ

4) ВИТОК

РОАПНЛЫЕККФШТСЬЗЦШЭРПИЁБФШЙШБКСКЬУЛВЩГ
ЮАСНЬБККХБАЮЯИЁТЛФЙШБКГИГПУСАУ=ЪЕЙАШРВЧУС
ЭЗМЧПКСЬЧПЧБОЕОЧАНШЩКЖЪЁТКСЬТУЬЦМУ

5) ДЕКАН

ТККВЯУЧЛКАЙЕ=СОМАКТСУЦЙШОДКЭУЙДЧЧПРЕЕЭЙ
ЪАУРЁНШЦЛДОТЁКИОЛОНБЛЧЕЬБЬ=ЕЪУНТФТБНЕЕЪУНЦС
ЪГНТККИОЛОНБЛЧЕЬБЬ=

6) ДОБРО

ППМРЧЕАФССНБЮРЁЙЫРУФППБВЪЕЧВГКДЯТССИВББ
ПМЮЙЭШЧФБЦТУОДРНХЮУГШДВБЭМИФЛРЭЙББУ=ЙЬЖЯ
ШДЯТЪУШЬЭУПЧКБЭЮЛК

7) ДЫМКА

ЙМ=ЖАЧЬШЛ=ДОСФГННТЧЭТЬЛКЛЕНТОПХДЛКМВ=ТХ
АПЙ=ЪС=АМПФСЬКЮАЬНЬКНУВЫЪАПЙРЪУУЫЭЬЁИЬ=ЖА
МЬ=РНДКЬППЛ=НЮЭДИТЦПЧЙЮЪЁДЮЮРНГЫЦКТТЙПЛАФ
ЙЭЁУЕНИЭ=ДЮЬУПЁИЬНЙЧЧМЪВЮАЫФЁДЁНЦАТДМНАЬБ
ЪКОЙЫОЁГЕЖЬКРУЛНУЙЧАЩЖО=АМЧЯИД

8) ЗАКОН

ЦЁКРИКБРБНЩБУЭЧЯЬКСНКПУ=ОЪУРОПГГЛФАЗСЛЧЬ
СЧЛОРЗФШФНЧНЛ=НЮБХНЫ

9) ЗЕФИР

ЦЁЩШРЬТЪЬМЗНХФБГЗХЬМЗЧ=ЭЗЦЩТИЬЦОШЭРЬЫГН
ЪЫБФЫРШСГЯ=ЛФФФЪЦФФЭУЧСРЧПЫБЁЗРЪЕДХ=ЮФЯИБ
ИЖГЬЛЗОФЪСЪЧЖЙУИШРЫПЗЧФХОМББТРУФЖШБГКФЬ=Й
ФЯИЯНЕЩШБЧМХЬ

10) ИДЕАЛ

ЩРГО=ЛДЗАГЭЛЩЯЛНШЮФЛЫРКЕХЬЙЕИМИЖКУЭШС

11) ИСКРА

ФАОХБИИРЭПЛЧЦРЕОЮЛЦУИ=ЛЮАКАЧМОШСЮ=АЫЭ
ЪБЁОСНВЁМАКВБЦСЪЯАМЮЯТПФАКЯЁЫИЛВУО=КВШЙГ
ЮЭЙЛМРРМЖЦФРООСАСНЗДКУАШИРБЁНРАРООСЬДДЙПЮ
В=ИФКГСЙ=ЭАПЪДРРООСЭАМОДЩЪШЙПЮРПИЭЪЭМОХЛЁ
АЫИЛВУХЫНЛЁИЮИХЙИФКХСЭХЪЫАЪЧЛЭЭЧАЭГЙИЫШР
ЮЬАКЯЙИЭКЗЁЦЕ

12) ИСТОК

ЭС=ФЩЗСДЫФБЭБЬКЯАГЮГОЧТЭЛЫДБНДОЧТШКЩАЕ
=ЙЫТРЗРОСФВПЭКШФКАДБРЁИББЬЩТДООЪКЫЧЙКЩВБЖЧ
ШХБ

13) КАЗУС

ЪТЦВФЩПНУБЬБКЭЮЪАПЭЪЩЙЗУ=РАМФФЛУДУГЧПХ
ЭДЖАЪЩУЙАЦЭСЧЯМТЯКОСУАМТЫВРЮЁФПГЮГИА

14) КИВОК

ЦШЁУЛКНСЫОЪИОММФБЯОЗЮШВЯРЬОФБЛИЬВЧЛШО
ЪПЮЖИНЮООПЙВУЪЧМСОЫЬШЬПРГЕВЛЮФЦВЭЛВТРПИЮ
ИТЮЧЖССЛЮЕФНКЦШЁУЛКМСБЪНИРПКНЫЗОЫЬШФБЪК
ЩЗ=РЭЬГМЮК=ЗЭФЮЕВШКЮШОКЦЪИНЮОПЙВВАЪНЛЖЖ
КЧГЁФЩЙАБКЫШРШШЛЬЯОЦЛФВУЪЬШЁОМЁХВЁРЧШЕФЦ
КФСБЪЬШЁЮКНОУЭЯЮЕВВТРИТЮУПЧС

15) КИСТЬ

ФЧАЦАЛИДШСКФАЦККЦМТНЯЦЧЯЕКЩВБНЮТДОЬЯРЧ
ТЙРИЖБУРЬГСЬЪК=ЬИЛЬН

16) МЕСЯЦ

ФКГСЕШФГСТМЭЧПИНЕЖ=ЖНРДДЖНЕЫРБЩГИЗИТСН
МЕМЙААЖЗЫСКФСКЬЯЕЫЁСОЕЛЗЮЮЬ=ЧРЯИЬИЦ=ЦШФХГ
ЧМФСМ=ВЕ==НЦУТЭИМЗМС=ЮЁДЫЦЫФХЗ

17) НУЖДА

ЭХРЛБАПЩГАЧУХЙДЭШЦЖБАПЖБУЭУЙЦЁНДЗЖОЭУЯ
ЧПНЦВФЙАПЖГЕНЦЖТБТЩОИЁНКЪУАЭБЖШВЙЩЪДУРВР
ЪАРДЗЗПРУ

18) ПАДЕЖ

ЫБПЕУХДПФЖЯВНЙМВЭДЭМЫПЖКТРАЖНЁЬАНЕИАПЦ
ОУПХХЁПГАМСМХАФКШЁБДЁЖ=ПЧФФПРУЦЦЪАТКЖЕГЕ
ШРВАЖКТРАЬШЦСАЖКШЮФЧБЖЯВНММЮОУКЖБЁХЙЮХ

19) ПАСТА

ЗБЯНАЫУАГЬХАГЕГЩМЫТВЬЙЪЮЙПМПЧЙПОСЫМЖЙДТОЩЛДБАЮЙСЫОЬЙСЮЕПВНРУ

20) ПОБЕДА

БЫЖХУНГОПКДРЯЪВМЙЩЛОЕСШЦЯЬХЕТЁП=ВЧЦЛРЦЖЮААУЫХХУНГОПКДЕЯЪВМЙЩЛ

21) ПОЛКА

ТАСКОРЖХКТХБЫНБЮШККРЯОЬЪГЯУ=КУЯТЫКШХТЫКНКОШФЩХЭЖКРАЮХЭУХЪМИУПЮЯКОХУЫЭУРБЧЛАСЫМОПФПЭЩПББХКИРОЯЪАЖБЫКНКОХШЁХЬЛПБЮШСЧЭПУС=П

22) ПРЕСС

ЖЦШМВХРЗЧКЩРУЧФЯЩТАЩЮ=ЕФЧАЯЩДНПЬЁЯЧЮМЕЧГЬЪЕА=ПТЦАЙХЯЕГЮЯУФСЧБЭОСАЮ=ЕГЭРЩЁ=АПВСЕИРЫЕЧГЬЪЕА=ПДХЕКХЯЕЫСТБКЯРПЬФДАА=КСБА=ЮЮА

23) РАЗУМ

ЬПЛШНРГЗКТЭПКЩШСАУЭССЁЫЩМФСЖЬИОАШВЪЯЙЫЩМЗУЧУС=АЦЩР=АЧБНРНЧЫТГАЦЩМХПФЩ=ЦУДУНРОИУПСЩСИМБФУФВРФПУ==ШЦВМ=ТЫФЫЦУЪТ

24) СТОЛБ

=ШООРЪХ=МЫТЭБСУНТЪЛНПЧНЩБЭББЫТМШООВГТЯЭЖЦУЫХБААШЛПЧТЬСПРРБЮА

25) ТИСКИ

АОСЭЬУЪТХЬШЫНКТДЩВЛЛЬЬНКХРНЧХИЬВЫЮОТЬЧАИЮЬАКОЛОСЩОТТГЫШГАЧЩ

26) ТРАВА

АЦАТЬЕСКХЁДМАЛТВББЕЙЕМАТСБИМСЁТЭФЪЩШРРУЙЯ=ЗЛУШРГФЁТДТЛМЬПАЪУБТЬВОШРЙФРББУЛУОРВЦЕЁЙЁЗ

27) ТЫКВА

ДЬШСЁТЭЪОЭКЙРВТБВЛОЁАДРВВШМЭПЬДЖРРОУЪКХСШЮЪЁБ

28) УТРОМ

ББЬЮРШУРЭТУВДБНЮЕЦОЪВЭРДНДУЬБТДТВОЪВЬЮООЬЁА=ЖТБЬЦЬМЯТУПЪУ==ЩМИУБПШЁШБОХФХЪАЦЁТ=БМАШЯНМФТЮЮТУБГЭЬЛШЯШТУБГОПФКЦТЬУВ=СТШШЯШЛ

29) ХОЛОД

ШЙНШХЦНЛЬЙЭУ=ОЧЁПЯЮООХУСЭЙЩОЪПДШФЕШДЯ ЫХОЖЕФГПЧБФЪШГХСЖРНЁПЦБЙХСЬФЫЦБШФТЯНЛ=ЕЪЮ ЮБАХЮЯОЖЕФГПЧБФЪШОХШЛСУЖЯЫЬНГПЪШОХСЖЖЙ

4. ПРИМЕР ВЫПОЛНЕНИЯ РАБОТЫ

Ключ: ПРИМЕР;

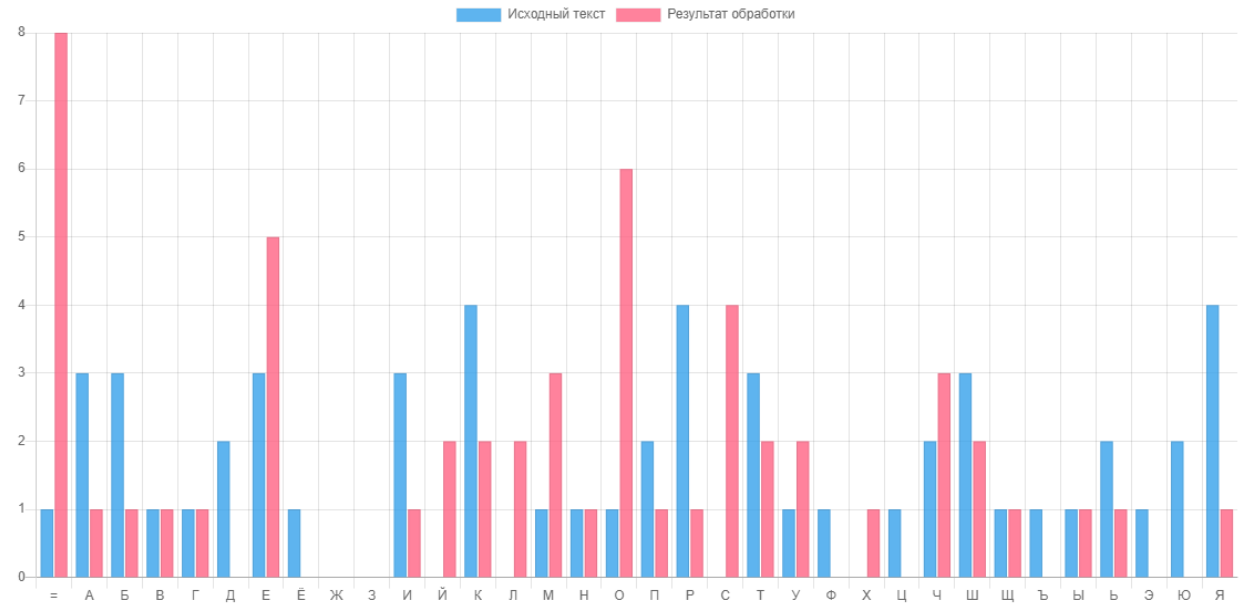
Сообщение:

ЬДАЕКРЯТВНШМБПИЯЕЁЯБШЕКЫПЬЧЦИ=ЪРАТТРБРЩАЧГКЮ ИДКЭЯУОШФЮ

1) Расшифровка.

01) Ь[30]-П[17] -> Л[13]
02) Д[05]-Р[18] -> У[21]
03) А[01]-И[10] -> Ч[25]
04) Е[06]-М[14] -> Ш[26]
05) К[12]-Е[06] -> Е[06]
06) Р[18]-Р[18] -> =[00]
07) Я[33]-П[17] -> О[16]
08) Т[20]-Р[18] -> Б[02]
09) В[03]-И[10] -> Щ[27]
10) Н[15]-М[14] -> А[01]
11) Ш[26]-Е[06] -> Т[20]
12) М[14]-Р[18] -> Ь[30]
13) Б[02]-П[17] -> С[19]
14) П[17]-Р[18] -> Я[33]
15) И[10]-И[10] -> =[00]
16) Я[33]-М[14] -> С[19]
17) Е[06]-Е[06] -> =[00]
18) Ё[07]-Р[18] -> Х[23]
19) Я[33]-П[17] -> О[16]
20) Б[02]-Р[18] -> Р[18]
21) Ш[26]-И[10] -> О[16]
22) Е[06]-М[14] -> Ш[26]
23) К[12]-Е[06] -> Е[06]
24) Ы[29]-Р[18] -> Й[11]
25) П[17]-П[17] -> =[00]
26) Ь[30]-Р[18] -> К[12]
27) Ч[25]-И[10] -> Н[15]
28) Ц[24]-М[14] -> И[10]
29) И[10]-Е[06] -> Г[04]
30) =[00]-Р[18] -> О[16]
31) Ъ[28]-П[17] -> Й[11]
32) Р[18]-Р[18] -> =[00]
33) А[01]-И[10] -> Ч[25]
34) Т[20]-М[14] -> Е[06]
35) Т[20]-Е[06] -> М[14]
36) Р[18]-Р[18] -> =[00]
37) Б[02]-П[17] -> С[19]
38) Р[18]-Р[18] -> =[00]
39) Щ[27]-И[10] -> П[17]
40) А[01]-М[14] -> У[21]
41) Ч[25]-Е[06] -> С[19]
42) Г[04]-Р[18] -> Т[20]
43) К[12]-П[17] -> Ы[29]
44) Ю[32]-Р[18] -> М[14]
45) И[10]-И[10] -> =[00]
46) Д[05]-М[14] -> Ч[25]
47) К[12]-Е[06] -> Е[06]
48) Э[31]-Р[18] -> Л[13]
49) Я[33]-П[17] -> О[16]
50) У[21]-Р[18] -> В[03]
51) О[16]-И[10] -> Е[06]
52) Ш[26]-М[14] -> К[12]
53) Ф[22]-Е[06] -> О[16]
54) Ю[32]-Р[18] -> М[14]

ЛУЧШЕ=ОБЩАТЬСЯ=С=ХОРОШЕЙ=КНИГОЙ=ЧЕМ=С=ПУСТЫМ=ЧЕЛОВЕКОМ



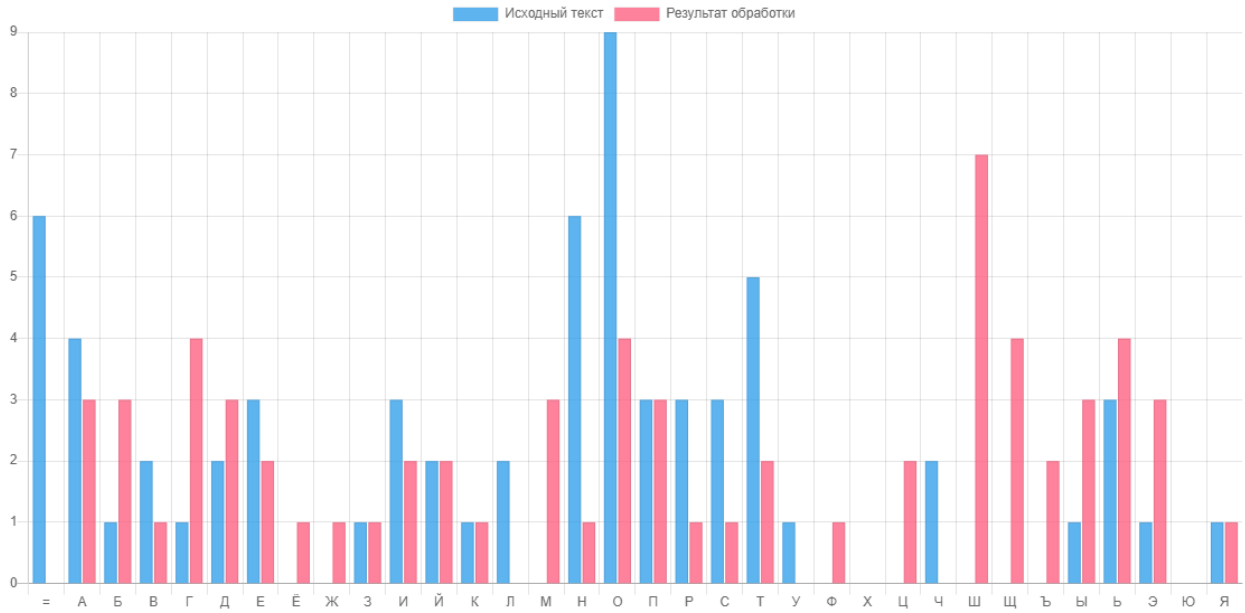
2) Частотный анализ показывает несоответствие распределений встречаемости символов исходного сообщения и шифрованного текста за счет использования составного ключа.

3) Шифровка.

Ключ: ЗАЩИТА.

Сообщение:

СЧАСТЬЕ=ЭТО=ПОБОЧНЫЙ=ПРОДУКТ=ПРАВИЛЬНО=ОРГАНИЗОВАННОЙ=ДЕЯТЕЛЬНОСТИ



```
01) С[19]+З[09] -> Ъ[28]
02) Ч[25]+А[01] -> Ш[26]
03) А[01]+Щ[27] -> Ъ[28]
04) С[19]+И[10] -> Ы[29]
05) Т[20]+Т[20] -> Е[06]
06) Ь[30]+А[01] -> Э[31]
07) Е[06]+З[09] -> Н[15]
08) =[00]+А[01] -> А[01]
09) Э[31]+Щ[27] -> Ц[24]
10) Т[20]+И[10] -> Ь[30]
11) О[16]+Т[20] -> Б[02]
12) =[00]+А[01] -> А[01]
13) П[17]+З[09] -> Ш[26]
14) О[16]+А[01] -> П[17]
15) Б[02]+Щ[27] -> Ы[29]
16) О[16]+И[10] -> Ш[26]
17) Ч[25]+Т[20] -> Й[11]
18) Н[15]+А[01] -> О[16]
19) Ы[29]+З[09] -> Г[04]
20) Й[11]+А[01] -> К[12]
21) =[00]+Щ[27] -> Щ[27]
22) П[17]+И[10] -> Щ[27]
23) Р[18]+Т[20] -> Г[04]
24) О[16]+А[01] -> П[17]
25) Д[05]+З[09] -> М[14]
26) У[21]+А[01] -> Ф[22]
27) К[12]+Щ[27] -> Д[05]
28) Т[20]+И[10] -> Ь[30]
29) =[00]+Т[20] -> Т[20]
30) П[17]+А[01] -> Р[18]
31) Р[18]+З[09] -> Щ[27]
32) А[01]+А[01] -> Б[02]
33) В[03]+Щ[27] -> Ь[30]
34) И[10]+И[10] -> Т[20]
35) Л[13]+Т[20] -> Я[33]
36) Ь[30]+А[01] -> Э[31]
37) Н[15]+З[09] -> Ц[24]
38) О[16]+А[01] -> П[17]
39) =[00]+Щ[27] -> Щ[27]
40) О[16]+И[10] -> Ш[26]
41) Р[18]+Т[20] -> Г[04]
42) Г[04]+А[01] -> Д[05]
43) А[01]+З[09] -> И[10]
44) Н[15]+А[01] -> О[16]
45) И[10]+Щ[27] -> В[03]
46) З[09]+И[10] -> С[19]
47) О[16]+Т[20] -> Б[02]
48) В[03]+А[01] -> Г[04]
49) А[01]+З[09] -> И[10]
50) Н[15]+А[01] -> О[16]
51) Н[15]+Щ[27] -> Ж[08]
52) О[16]+И[10] -> Ш[26]
53) Й[11]+Т[20] -> Э[31]
54) =[00]+А[01] -> А[01]
55) Д[05]+З[09] -> М[14]
56) Е[06]+А[01] -> Ё[07]
57) Я[33]+Щ[27] -> Ш[26]
58) Т[20]+И[10] -> Ь[30]
59) Е[06]+Т[20] -> Ш[26]
60) Л[13]+А[01] -> М[14]
61) Ь[30]+З[09] -> Д[05]
62) Н[15]+А[01] -> О[16]
63) О[16]+Щ[27] -> З[09]
64) С[19]+И[10] -> Ы[29]
65) Т[20]+Т[20] -> Е[06]
66) И[10]+А[01] -> Й[11]
```

ЪШЪЫЕЭНАЦЬБАШПЫШЙОГКЩЩГПМФДЬТРЩБЬТЯЭЦПЩШГДИОВСБГИОЖШЭАМЁШЬШМДОЗЫЕЙ

5. КОНТРОЛЬНЫЕ ВОПРОСЫ.

1. Что такое шифр Цезаря?
2. В чем заключается метод Виженера?
3. Что такое частотный анализ?
4. Что такое мощность алфавита?
5. Как повысить криптостойкость метода Виженера?

СПИСОК ЛИТЕРАТУРЫ

1. Панасенко, С. Алгоритмы шифрования [Текст] / С. Панасенко. Спб: БХВ-Петербург, 2009, 576 стр.

2. Ростовцев А.Г., Маховенко Е.Б. Теоретическая криптография [Текст] / А.Г. Ростовцев, Е.Б. Маховенко. М: АНО НПО "Профессионал", 2005, 480 стр.

3. Рябко, Б. Я., Фионов, А. Н. Основы современной криптографии для специалистов в информационных технологиях [Текст] / Б. Я. Рябко, А. Н. Фионов. М: Научный мир, 2004, 179 стр.

4. Смарт, Н. Криптография [Текст] / Н. Смарт. М: Техносфера, 2006, 528 стр.