

Документ подписан простой электронной подписью
Информация о владельце: **1**
ФИО: Локтионова Оксана Геннадьевна
Должность: проректор по учебной работе
Дата подписания: 16.06.2021 10:19:39
Уникальный программный ключ:
0b817ca911e6668abb13a5d426d39e5f1c11eabbf73e943df4a4851fda56d089

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

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. *625* 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 $M \times M$, 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 первоначального 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 «кекхтвоэцотсвил» (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 находится 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	ВЕСНАВЕСНАВЕСН
	АВ
ЗАШИФРОВАННЫЙ ТЕКСТ	КЕКХТВОЭЦОТССВ
	ИЛ
РАСШИФРОВАННЫЙ ТЕКСТ	ЗАЩИТАИНФОРМА ЦИИ
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. Данная 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.

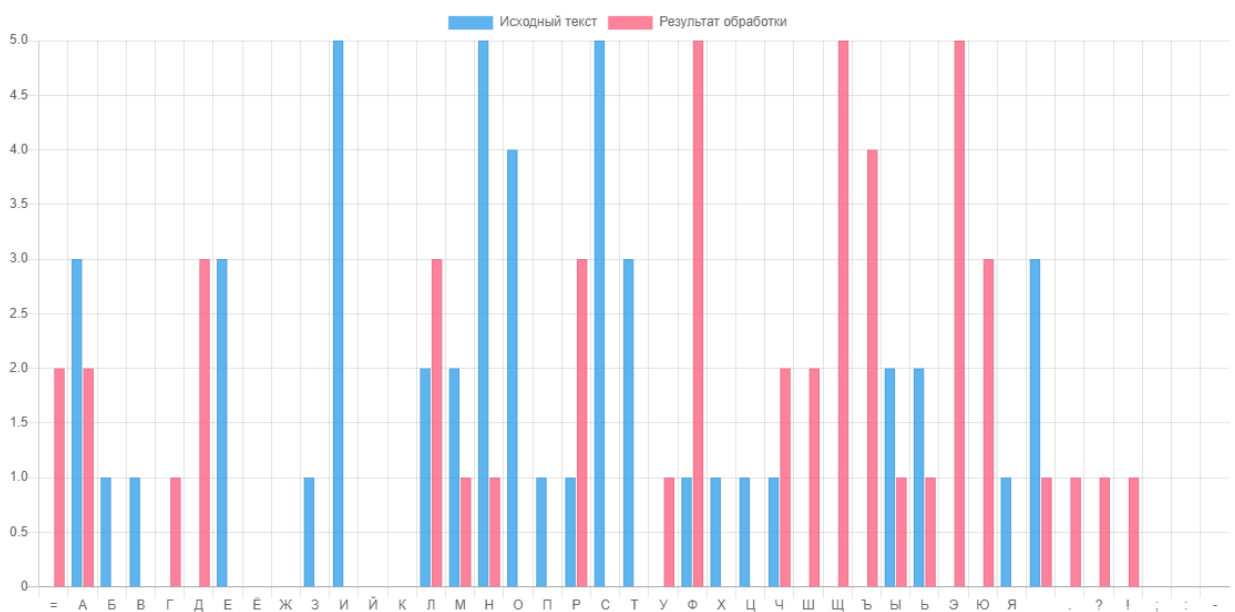


Рисунок 7 - Гистограмма распределения частот с применением шифра Цезаря

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.

Шифрование методом Виженера

Алфавит

АБВГДЕЁЖЗИЙКЛМНОПРСТУФХЦЧШЩЪЫЬЭЮЯ

Исходное сообщение

ЦЕЛЬЮ ДАННОГО УЧЕБНОГО ПОСОБИЯ ЯВЛЯЕТСЯ ИЗУЧЕНИЕ ОСНОВ И ПРИНЦИПОВ ЗАЩИТЫ ИНФОРМАЦИИ В В

Ключ

КРИПТОГРАФИЯ

Зашифровать Расшифровать

Выполнить

Результат

БЦХЛПРОЗСОВШВЪРЭЖШРС ДГИОЪВШСЪНГПГАЗДЮВЗПЪЧЗЁВТДК ЫЮБСГЪАДЪЗЩЖТ БСГЩБНТСЁРТЮЖЮФЮБКТЗКУИ

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.

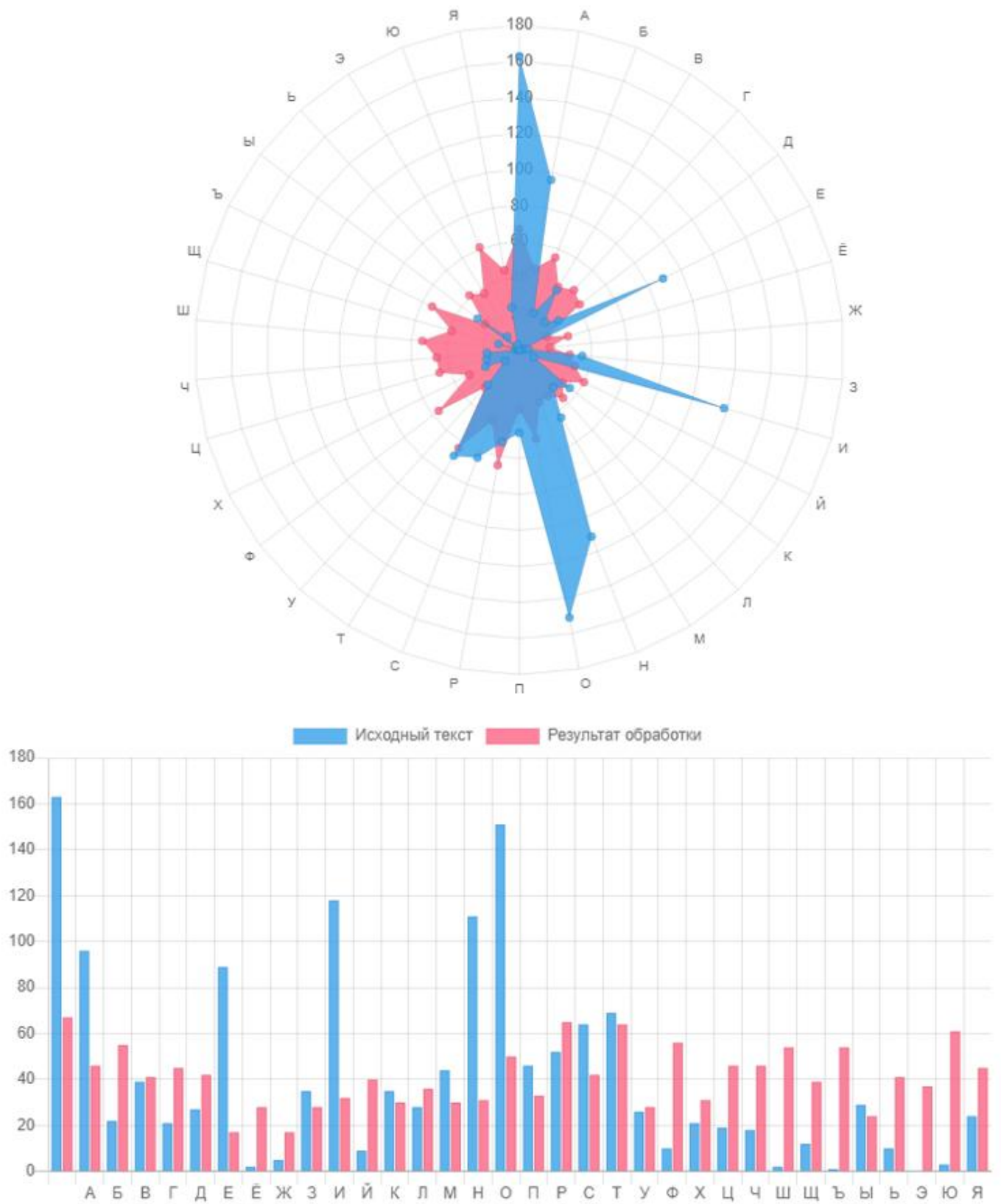


Рисунок 9 - Частотный анализ текста в виде радиальной и столбчатой диаграммы

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 возникновения 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 длина ключа найдена.

2. Криптоанализ. Совокупность 1 шифров Цезаря (где 1 — 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.

```

1 <!DOCTYPE html>
2 <html lang="ru" dir="ltr">
3 <head>
4 <link rel="stylesheet" type="text/css" href="./css/bootstrap.css">
5 <link rel="stylesheet" type="text/css" href="./css/style.css">
6 <script src="js/app.js"></script>
7 <script src="js/jquery.js"></script>
8 <script src="js/Chart.min.js"></script>
9 </head>
10 <body>
11 <div class="container">
12 <div class="col-xs-offset-3 col-xs-6">
13 <br>
14 <h3>Шифрование методом Виженера</h3>
15 <p> Алфавит
16 <input class="form-control" type="text" id="abc"
17 value="АБВГДЕЖЗИЙКЛМНОПРСТУФХЦШЩЪЫЬЭЮЯ .?!;:-">
18 </p>
19 <div class="alert alert-info">
20 <p> Исходное сообщение
21 <input class="form-control" type="text" id="inS"
22 value="Информационная безопасность вычислительных систем">
23 Ключ
24 <input class="form-control" type="text" id="key" value="Криптография">
25 </p>
26 <div class="form-check form-check-inline">
27 <input class="form-check-input" type="radio" name="c1" id="coder" checked>
28 Зашифровать
29 </div>
30 <div class="form-check form-check-inline">
31 <input class="form-check-input" type="radio" name="c1">
32 Расшифровать
33 </div>
34 </div>
35 <button class="btn btn-lg btn-outline-info" onclick="Main()" >Выполнить</button>
36 <p> Результат
37 <input type="text" readonly class="form-control" id='outS'>
38 </p>
39 <div>
40 <canvas id="myChart"></canvas>
41 </div>
42 <p class="auth">Кафедра информационной безопасности, ЮЗГУ, 2019</p>
43 </div>
44 </div>
45 </body>
46 </html>

```

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

ПТЮСДЁЙТРЕБЭЦГЕВОКЯАМЪБВЕРЫЕСЙПИЧСГЖЪББА
УЙ=ЮЁБКЯЛИМТШВРРЪБМАСЪШЖБ=ЪТФБОДШВШХРЪЗАП
ОБЙЙЁЙАРПЫЩБППЕЙРХ

4) ВИТОК

РОАПНЛЫЕККФШТСЪЗЦШЭРПИЁБФШЙШБКСКЪУЛВЦГ
ЮАСНЪБККХБАЮЯИЁТЛФЙШБКГИГПУСАУ=ЪЕЙАШРВЧУС
ЭЗМЧПКСЪЧПЧБОЕОЧАНШЩКЖЪЁТКСЪТУЫЦМУ

5) ДЕКАН

ТККВЯУЧЛКАЙЕ=СОМАКТСУЦЙШОДКЭУЙДЧЧПРЕЕЭЙ
ЪАУРЁНШЦЛДОТЁКИОЛОНБЛЧЕЬБЪ=ЕЪУНТФТБНЕЕЪУНЦС
ЪГНТККИОЛОНБЛЧЕЬБЪ=

6) ДОБРО

ППМРЧЕАФССНБЮРЁЙЫРУФППВЪЕЧВГКДЯТССИВББ
ПМЮЙЭШЧФБЦТУОДРНХЮУГШДВБЭМИФЛРЭЙББУ=ЙЪЖА
ШДЯТЬУШЬЭУПЧКБЭЮЛК

7) ДЫМКА

ЙМ=ЖАЧЬШЛ=ДОСФГННТЧЭТЬЛКЛЕНТОПХДЛКМВ=ТХ
АПЙ=ЪС=АМПФСЬКЮАЬНЬКНУВЫЪАПЙРЪУУЫЭЪЁИЬ=ЖА
МЪ=РНДКЪППЛ=НЮЭДИТЦПЧЙЮЪЁДЮЮРНГЫЩКТТЙПЛАФ
ЙЭЁУЕНИЭ=ДЮБУПЁИЙНЙЧМЪВЮАЫФЁДЁНЦАТДМНАББ
ЪКОЙЫОЁГЕЖЬКРУЛНУЙЧАЩЖО=АМЧЯИД

8) ЗАКОН

ЦЁКРИКБРЬНЩБУЭЧЯЬКСНКПУ=ОЪУРОПГГЛФАЗСЛЧЬ
СЧЛОРЗФШФНЧНЛ=НЮБХНЫ

9) ЗЕФИР

ЦЁЩШРЪТЬМЗНХФБГЗХЪМЗЧ=ЭЗЦЩТИЬЦОШЭРЬЫГН
ЪЫБФЫРШСГЯ=ЛФФФЪЦФФЭУЧСРЧПЫБЁЗРЪЕДХ=ЮФЯИБ
ИЖГЪЛЗОФЪСЪЧЖЙУИШРЬПЗЧФХОМББТРУФЖШБГКФЪ=Й
ФЯИЯНЕЩШБЧМХЪ

10) ИДЕАЛ

ЩРГО=ЛДЗАГЭЛЩЯЛНШЮФЛЫРКЕХЪЙЕИМИЖКУЭШС

11) ИСКРА

ФАОХБИИРЭПЛЧЦРЕОЮЛЦУИ=ЛЮАКАЧМОШСЮ=АЫЭ
 ЪБЁОСНВЁМАКВБЦСЪЯАМЮЯТПФАКЯЁЫИЛВУО=КВШЙГ
 ЮЭЙЛМРРМЖЦФРООСАСНЗДКУАШИРБЁНРАРООСЪДДЙПЮ
 В=ИФКГСЙ=ЭАПЪДРРООСЭАМОДЦЪШЙПЮРПИЭЪЭМОХЛЁ
 АЫИЛВУХЫНЛЁИЮИХЙИФКХСЭХЪАЪЧЛЭЭЧАЭГЙИЫШР
 ЮБАКЯЙИЭКЗЁЦЕ

12) ИСТОК

ЭС=ФЩЗСДЫФБЭЪБЪКЯАГЮГОЧТЭЛЫДБНДОЧТШКЩАЕ
 =ЙЫТРЗРОСФВПЭКШФКАДБРЁИББЫЦТДООЪКЫЧЙКЩВБЖЧ
 ШХБ

13) КАЗУС

ЪТЦВФЩПНУБЪБКЭЮЪАПЭЪЩЙЗУ=РАМФФЛУДУГЧПХ
 ЭДЖАЪЩУЙАЦЭСЧЯМТЯКОСУАМТЫВРЮЁФПГЮГИА

14) КИВОК

ЦШЁУЛКНСЫОЪИОММФБЯОЗЮШВЯРЬОФБЛИВЧЛШО
 ЪПЮЖИНЮОПЙВУЪЧМСОЫЪШЬПРГЕВЛЮФЦВЭЛВТРПИЮ
 ИТЮЧЖСССЛЮЕФНКЦШЁУЛКМСБЪНИРПКНЫЗОЫЪШФБЪК
 ЩЗ=РЭЪГМЮК=ЗЭФЮЕВШКЮШОКЦЪИНЮОПЙВВАЪНЛЖЖ
 КЧГЁФЩЙАБКЫШРШШЛЬЯОЦЛФВУЪЪШЁОМЁХВЁРЧШЕФЦ
 КФСБЪЪШЁЮКНОУЭЯЮЕВВТРИТЮУПЧС

15) КИСТЬ

ФЧАЦАЛИДШСКФАЦККЦМТНЯЦЧЯЕКЩВБНЮТДОБЪЯРЧ
 ТЙРИЖБУРЫГСЪЪК=ЫИЛЬН

16) МЕСЯЦ

ФКГСЕСШФГСТМЭЧПИНЕЖ=ЖНРДДЖНЕЫРБЩГИЗИТСН
 МЕМЙААЖЗЫСКФСКЪЯЕЫЁСОЕЛЗЮЮЪ=ЧРЯИЫИЦ=ЦШФХГ
 ЧМФСМ=ВЕ==НЦУТЭИМЗМС=ЮЁДЫЦЫФХЗ

17) НУЖДА

ЭХРЛБАПЩГАЧУХЙДЭШЦЖБАПЖБУЭУЙЦЁНДЗЖОЭУЯ
 ЧПНЦВФЙАПЖГЕНЦЖТЪТЩОИЁНКЪУАЭБЖШВЙЩЪДУРВР
 ЪАРДЗЗПРУ

18) ПАДЕЖ

ЫБПЕУХДПФЖЯВНИМВЭДЭМЫПЖКТРАЖНЁБАНИЕИАПЦ
 ОУПХХЁПГАМСМХАФКШЁБДЁЖ=ПЧФФПРУЦЦЪАТКЖЕГЕ
 ШРВАЖКТРАЪЩЦСАЖКШЮФЧБЖЯВНММЮОУКЖБЁХЙЮХ

19) ПАСТА

ЗБЯНАБУАГЪХАГЕГЦМЫТВЪЙЪЮЙПМПЧЙПОСЫМЖЙ
ДТОЩЛДБАЮЙСЫОБЪСЮЕПВНРУ

20) ПОБЕДА

БЫЖХУНГОПКДРЯЪВМЙЩЛОЕСШЦЯЪХЕТЁП=ВЧЦЛРЦ
ЖЮААУЫХХУНГОПКДЕЯЪВМЙЩЛ

21) ПОЛКА

ТАСКОРЖХКТХБЫНБЮШККРЯОБЪГЯУ=КУЯТЫКШХТЫ
КНКОШФЦХЭЖКРАЮХЭУХЪМИУПЮЯКОХУЫЭУРБЧЛАСЫ
МОПФПЭЩПБХКИРОЯЪАЖБЫКНКОХШЁХЪЛПБЮШСЧЭПУ
С=П

22) ПРЕСС

ЖЦШМВХРЗЧКЩРУЧФЯЩТАЩЮ=ЕФЧАЯЩДНПЬЁЯЧЮ
МЕЧГЪБЕА=ПТЦАЙХЯЕГЮЯУФСЧБЭОСАЮ=ЕГЭРЩЁ=АПВС
ЕИРЫЕЧГЪБЕА=ПДХЕКХЯЕЫСТБКЯРПЬФДАА=КСБА=ЮЮА

23) РАЗУМ

БПЛШНРГЗКТЭПКЩШСАУЭССЁЫЩМФСЖЬИОАШВЪЯ
ЙЫЩМЗУЧУС=АЦЩР=АЧБНРНЧЫТГАЦЩМХПФЩ=ЦУДУНР
ОИУПСЦСИМБФУФВРФПУ==ШЦВМ=ТЫФЫЦУЪТ

24) СТОЛБ

=ШООРЪХ=МЫТЭБСУНТЬЛНПЧНЩБЭБЫТМШООВГТЯЭЖЦ
УЫХБААШЛПЧТЬСПРРБЮА

25) ТИСКИ

АОСЭЪУЪТХЫШЫНКТДЦВЛЛЪНКХРНЧХИВЪЮОТЬЧ
АИЮБАКОЛОСЩОТТГЫШГАЧЦ

26) ТРАВА

АЦАТЬЕСКХЁДМАЛТВББЕЙЕМАТСБИМСЁТЭФЫЩШРУ
ЙЯ=ЗЛУШРГФЁТДТЛМЪПАЪУБТЬВОШРЙФРЪБУЛУОРВЦЕЙЙ
ЁЗ

27) ТЫКВА

ДЫШСЁТЭЪОЭКЙРВТВВЛОЁАДРВВШМЭПЪДЖРРОУЪКХ
СШЮЪЁБ

28) УТРОМ

БЪЮРШУРЭТУВДБНЮЕЦОЪВЭРДНДУЪБТДТВОЪВЪЮО
БЁА=ЖТЪЦЪМЯТУПЪУ==ЩМИУБПШЁШБОХФХЪАЦЁТ=БМ
АШЯНМФТЮЮТУБГЪЛШЯШТУБГОПФКЦТЬУВ=СТШШЯШ
Л

29) ХОЛОД

ШЙНШХЦНЛЬЙЭУ=ОЧЁПЯЮОХУСЭЙЩОЪПДШФЕШДЯ
 ЫХОЖЕФГПЧБФЪШГХСЖРНЁПЦБЙХСЬФЬЦБШФТЯНЛ=ЕЪЮ
 ЮБАХЮЯОЖЕФГПЧБФЪШОХШЛСУЖЯЬНГПЪШОХСЖЖЙ

4. ПРИМЕР ВЫПОЛНЕНИЯ РАБОТЫ

Ключ: ПРИМЕР;

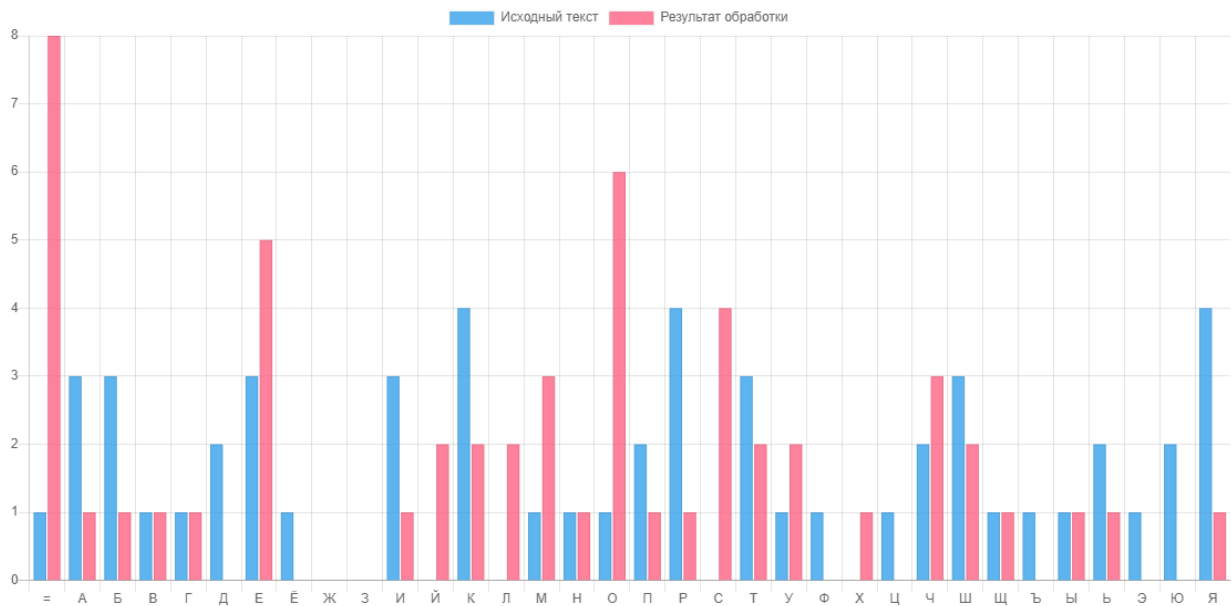
Сообщение:

БДАЕКРЯТВНШМБПИЯЕЁЯБШЕКЫПЬЦЦИ=ЪРАТТРБРЦАЧГКЮ
 ИДКЭЯУОШФЮ

1) Расшифровка.

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

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



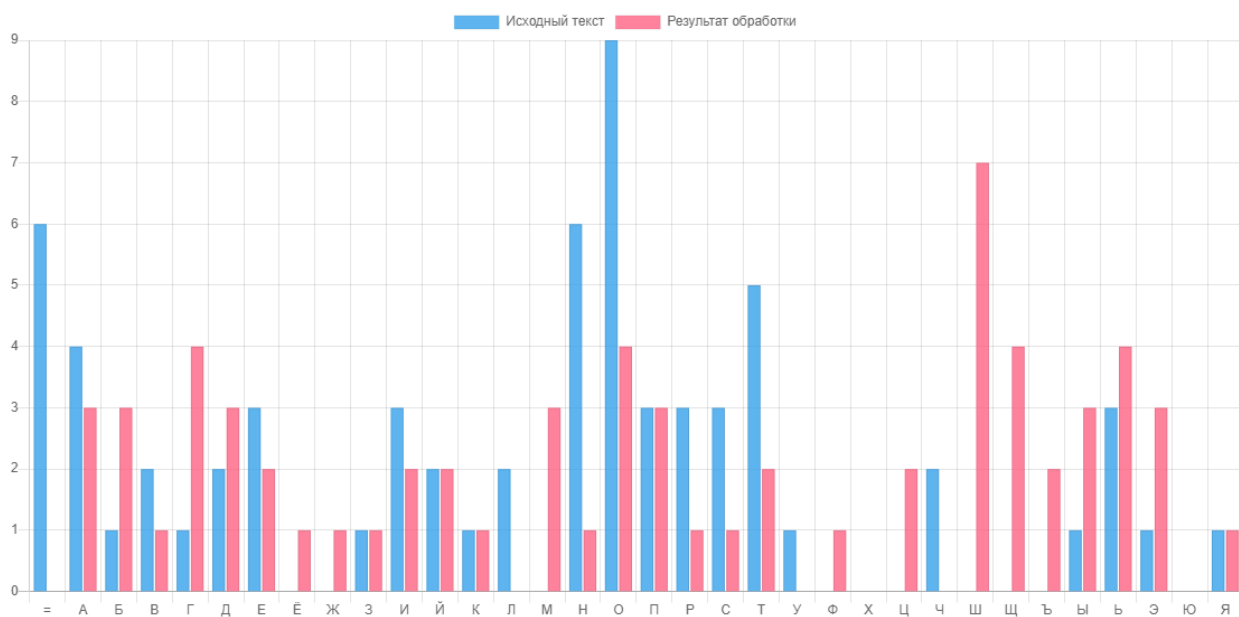
2) Частотный анализ показывает несоответствие распределений встречаемости символов исходного сообщения и зашифрованного текста за счет использования составного ключа.

3) Шифровка.

Ключ: ЗАЩИТА.

Сообщение:

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



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

ЪЫГЬЕЭНАЦЪБАШПЫШЙОГКЩЦГПМФДЪТРЩБЪТЯЭЦПЩГДИОВСВГИОЖШЭАМЁШЬМДОЗЫЙ

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.