МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ

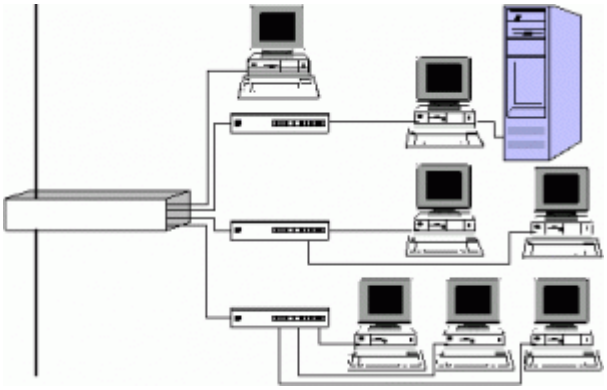
Федеральное государственное бюджетное образовательное
учреждение высшего образования
«Воронежский государственный технический университет»

Кафедра автоматизированных и вычислительных систем

ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

МЕТОДИЧЕСКИЕ УКАЗАНИЯ

к выполнению лабораторных работ
по дисциплине «Информационная безопасность и защита информации»
для студентов направления 38.03.05 «Бизнес-информатика»
(профиль «Информационные системы в бизнесе»)
очной и заочной форм обучения



Воронеж 2022

УДК 681.3.06(07)
ББК 32.973

Составители:
канд. техн. наук Т. И. Сергеева,
канд. техн. наук М. Ю. Сергеев

Обеспечение информационной безопасности: методические указания к выполнению лабораторных работ по дисциплине «Информационная безопасность и защита информации» для студентов направления 38.03.05 «Бизнес-информатика» (профиль «Информационные системы в бизнесе») очной и заочной форм обучения / ФГБОУ ВО «Воронежский государственный технический университет»; сост.: Т. И. Сергеева, М. Ю. Сергеев. Воронеж: Изд-во ВГТУ, 2022. 37 с.

Цель методических указаний - освоение различных методов и средств защиты информации и обеспечение информационной безопасности, выработка умений и навыков написания программ генерации паролей и шифрования сообщений с применением методов перестановки и замены.

Методические указания содержат теоретические сведения и практические задания для выполнения лабораторных работ.

Предназначены для проведения лабораторных работ по дисциплине «Информационная безопасность и защита информации» для студентов 4 и 5 курсов очной и заочной форм обучения.

Методические указания подготовлены в электронном виде и содержатся в файле IB_ZI_LR.pdf.

Ил. 5. Табл. 9. Библиогр.: 4 назв.

УДК 681.3.06(07)
ББК 32.973

Рецензент – П. Ю. Гусев, канд. техн. наук, доцент кафедры компьютерных интеллектуальных технологий проектирования ВГТУ

Издается по решению редакционно-издательского совета Воронежского государственного технического университета

1. ЛАБОРАТОРНАЯ РАБОТА № 1
РАЗРАБОТКА ПЛАНА МЕРОПРИЯТИЙ ПО ЗАЩИТЕ ИНФОРМАЦИИ С ИСПОЛЬЗОВАНИЕМ ОРГАНИЗАЦИОННЫХ СРЕДСТВ ЗАЩИТЫ

1.1. Общие сведения

Цель работы – изучение функционального назначения организационных средств защиты и их применения для обеспечения информационной безопасности.

Организационные средства защиты должны обеспечить:

- полное или частичное перекрытие значительной части каналов утечки информации;
- объединение всех используемых в КС средств защиты в целостный механизм защиты информации.

В процессе эксплуатации компьютерной системы (КС) должны осуществляться следующие организационные меры защиты информации:

- организация пропускного режима;
- определение технологии автоматизированной обработки документов;
- организация работы обслуживающего персонала;
- распределение реквизитов разграничения доступа пользователей к элементам КС (паролей, ключей, карт и т.п.);
- организация ведения протоколов работы КС;
- контроль выполнения требований служебных инструкций и т.п.

Мероприятия общего характера:

- подбор и подготовка кадров;
- организация плановых и предупреждающих проверок средств защиты информации;
- планирование мероприятий по защите информации;
- обучение персонала, участие в семинарах, конференциях и выставках по проблемам защиты безопасности информации и т.п.

1.2. Мероприятия по защите информации с применением организационных и физических средств защиты

Организация пропускного режима. Необходимо указать, сколько смен работы предусмотрено в фирме; указать время работы смен и перерывов; указать, какие будут пропуска (электронные или удостоверения). Определить, какое подразделение будет заниматься выдачей пропусков и организацией пропускного режима.

Определение технологии автоматизированной обработки документов. Задачи, реализующие обработку информации ограниченного доступа, как правило, состоят из следующих типовых действий: ввод данных, обработка, выда-

ча результата. Предположим, в фирме решаются следующие задачи по обработке информации:

- ввод и редактирование данных об объемах продаж за день, данные вводятся ежедневно в начале следующего дня;
- формирование отчета о продаже за день; отчет предоставляется в службу продаж к 10 часам следующего дня;
- расчет суммарных продаж за десять дней; расчет производят в каждый 11 день;
- формирование отчета о продажах за десять дней; отчет предоставляется в службу продаж к 10 часам каждый 11 день;
- расчет суммарных продаж за месяц и формирование отчета о продажах за месяц; отчет предоставляется к 11 часам в первый день следующего месяца.

Составить график обработки данных для каждой задачи (указать задачу, время выполнения, ответственного).

Организация работы обслуживающего персонала. Обслуживающий персонал, занимающийся автоматизированной обработкой информации, как правило, состоит из:

- инженеров по эксплуатации и ремонту вычислительной техники; осуществляют посменное дежурство и ремонтируют технику по мере появления неисправностей;
- инженеров-программистов, осуществляющих разработку и отладку программ;
- техников-операторов, осуществляющих запуск программ из стандартного набора.

Предположим, что вычислительный центр фирмы работает в две смены:

- с 8 часов до 15 часов;
- с 15 часов до 22 часов.

Определить график работы всех категорий работников на неделю. Количество работников определить самостоятельно.

Распределение реквизитов разграничения доступа пользователей к элементам КС (паролей, ключей, карт и т.п.).

Предположим, что вычислительный центр занимает следующие помещения:

- помещение для программистов;
- помещение для инженеров по обслуживанию вычислительной техники;
- помещение для техников;
- помещение, где имеется изолированная локальная сеть и осуществляется обработка информации ограниченного доступа;
- помещение для выхода в интернет.

Определить, какие замки будет иметь каждое помещение (электронный кодовый замок; вход с помощью специальных средств идентификации работников; свободный вход).

Для системного администратора определить размер имени пользователя и пароля, срок действия паролей на вход в операционную систему.

Организация ведения протоколов работы компьютерной системы.

Работы, проводимые в помещении с изолированной локальной сетью, должны фиксироваться в специальном журнале. Определить, какие реквизиты должны фиксироваться в журнале.

Мероприятия общего характера. Составить график проведения занятий по проблемам защиты безопасности информации. Предусмотреть изучение следующих тем: обзор устройств для ввода идентифицирующей пользователя информации; обзор устройств для воспрепятствования несанкционированному включению рабочих станций и серверов (электронные замки и блокираторы); программы разграничения доступа пользователей к ресурсам компьютерной системы; обзор современных программно-аппаратных средств по защите информации в сети.

К **физическим средствам** защиты информации относят механические, электронно-механические, электромеханические, оптические, акустические, лазерные, радио и радиационные и другие устройства, системы и сооружения, предназначенные для создания физических препятствий на пути к защищаемой информации и способные выполнять самостоятельно или в комплексе с другими средствами функции защиты информации.

Физические средства защиты выполняют следующие основные задачи:

1) охрана территории и зданий;
2) охрана внутренних помещений;
3) охрана оборудования и наблюдение за ним;
4) контроль доступа в защищаемые зоны;
5) нейтрализация излучений и наводок;
6) создание препятствий визуальному наблюдению и подслушиванию;
7) противопожарная защита;
8) блокировка действий нарушителя и т.п.

Охрана внутренних помещений, оборудования и наблюдения за ним. Датчики различного типа необходимы для предотвращения проникновения нарушителей на охраняемые объекты.

Сверхвысокочастотные (СВЧ), ультразвуковые (УЗ) и инфракрасные (ИК) системы

Предназначены для обнаружения движущихся объектов, определения их размеров, скорости и направления перемещения. Принцип их действия основан на изменении частоты отраженного от движущегося объекта сигнала.

ИК системы бывают активными и пассивными. Активные системы содержат источник излучения и его приемник. Функционирование пассивных систем основано на фиксации теплового излучения ИК-датчиками.

УЗ и ИК системы применяются, главным образом, внутри помещений. СВЧ системы могут применяться как внутри помещений, так и для охраны зданий и территории.

Лазерные и оптические системы, работающие в видимой части спектра, реагируют на пересечение нарушителями светового луча и применяются, в основном, внутри помещений.

Телевизионные системы применяются для наблюдения как за территорией охраняемого объекта, так и за обстановкой внутри помещений.

Кабельные системы используются для охраны небольших объектов, обычно временно находящихся на территории, а также оборудования внутри помещений. Они состоят из заглубленного кабеля, окружающего защищаемый объект и излучающего радиоволны. Приемник излучения реагирует на изменение поля, создаваемого нарушителем.

Системы защиты окон и дверей предназначены для препятствия механическому проникновению, а также для защиты от наблюдения и подслушивания.

Контроль доступа в защищаемые зоны. Контроль доступа в защищаемые зоны может осуществляться с помощью у**стройств идентификации** пользователей:

- ***пластиковые карты с магнитной полосой***, на которой помимо ключевой информации могут размещаться и дополнительные реквизиты пользователя (его фамилия, имя, отчество, фотография, название организации и ее подразделения и т.п.); подобные карты наиболее дешевы, но и наименее защищены от копирования и подделки;

- ***карты со штрихкодом***, покрытым непрозрачным составом, считывание информации с которых происходит в инфракрасных лучах; эти карты также относительно дешевы, но уязвимы для подделки;

- ***смарт-карты***, носителем ключевой информации в которых является специальная бескорпусная микросхема, включающая в себя только память для хранения ключевой информации (простые смарт-карты) или микропроцессор (интеллектуальные карты), позволяющий реализовывать достаточно сложные процедуры идентификации и аутентификации;

- ***элементы Touch Memory*** (аналогичные изделия других производителей именуются iButton), включающие в себя энергонезависимую память в виде постоянного запоминающего устройства с уникальным для каждого изделия серийным номером и (в более дорогих вариантах) оперативного запоминающего устройства для хранения идентифицирующей пользователя информации, а также встроенный элемент питания со сроком службы до 10 лет (элемент Touch Memory напоминает миниатюрную батарейку диаметром 16 мм и толщиной 3...6 мм, он имеет один сигнальный контакт и один контакт заземления, а для контакта элемента с Устройством чтения достаточно простого касания);

- ***маркеры eToken (USB-брелки)***, представляющие собой подключаемое к USB-порту компьютера устройство, которое включает в себя аналогичную

смарт-карте микросхему с процессором защищенной от несанкционированного доступа памятью (в отличие от пластиковых карт не требуется установка устройства их чтения с кабелем для подключения этого устройства к компьютеру).

1.3. Задания для лабораторной работы № 1

Задание:

- разработать план мероприятий по организационной защите информации ограниченного доступа;
- план мероприятий должен включать разделы: организация пропускного режима, определение технологии автоматизированной обработки документов, организация работы обслуживающего персонала, распределение реквизитов разграничения доступа пользователей к элементам КС (паролей, ключей, карт и т.п.;
- дополните план мероприятий по защите информации средствами охраны внутренних помещений, оборудования и наблюдения за ним; для каждого вида помещения предложите конкретные датчики;
- дополните план мероприятий по защите информации средствами идентификации пользователей; данные средства будут использованы для входа в помещение, в котором обрабатывается информация ограниченного доступа.

Отчет

Отчет должен содержать титульный лист и план мероприятий, состоящий из указанных выше разделов.

2. ЛАБОРАТОРНАЯ РАБОТА № 2
РАЗРАБОТКА ПРЕЗЕНТАЦИИ ПО СРЕДСТВАМ ЗАЩИТЫ

2.1. Общие сведения

Цель работы – структуризация информации о группе средств защиты и представление ее в виде презентации.

Презентация должна описать:

- назначение предложенной группы средств защиты информации;
- функциональные возможности данного средства защиты;
- примеры средств защиты из предложенной группы и их технические характеристики.

Презентация должна содержать иллюстративный материал.

Вариант текста для оформления презентации необходимо получить у преподавателя.

2.2. Задания для лабораторной работы № 2

Задание

Разработать презентацию по предложенной теме.

Отчет

Отчет – это разработанная презентация.

3. ЛАБОРАТОРНАЯ РАБОТА № 3
РАЗРАБОТКА ПРОГРАММЫ «ГЕНЕРАТОР ПАРОЛЯ»

3.1. Общие сведения

Цель работы – изучение назначения парольной защиты информации, программная реализация генератора паролей.

Подсистемы идентификации (отличие одного пользователя от другого) и аутентификации (проверка подлинности) пользователя играют очень важную роль в системах защиты информации.

Парольные системы идентификации / аутентификации являются одними из основных и наиболее распространенных методов пользовательской аутентификации. В данном случае, информацией, аутентифицирующей пользователя, является некоторый секретный пароль, известный только легальному пользователю.

Основными минимальными требованиями к выбору пароля и к подсистеме парольной аутентификации пользователя являются следующие:

- минимальная длина пароля должна быть не менее 6 символов;
- пароль должен состоять из различных групп символов (малые и большие латинские или русские буквы, цифры, специальные символы '(\, ')', '#' и т.д.);
- в качестве пароля не должны использоваться реальные слова, имена, фамилии и т.д.

3.2. Реализация генератора паролей в Visual Studio на языке C#

Необходимо осуществить следующие действия.

1. Создать папку для сохранения проекта.
2. Запустить Visual Stidio. Выбрать Create Project, на дереве выбрать Visual C#, Windows, в правом окне Windows Forms Application, в поле Name ввести имя программы, выбрать (создать) папку для сохранения проекта в окне Location, ОК.
3. Создать интерфейс пользователя (окно формы программы представлено на рис. 1).

Интерфейс пользователя включает:

- кнопки выхода и запуска программы генерации пароля;
- поясняющие надписи;
- окно для ввода имени (идентификатора) пользователя;
- окно для вывода сформированного пароля.

Компонент Label используется для создания надписи, компонент Button – для создания кнопки, компонент textBox – для создания поля для ввода или вывода данных.

4. Написание и отладка программы, проверка работы программы.

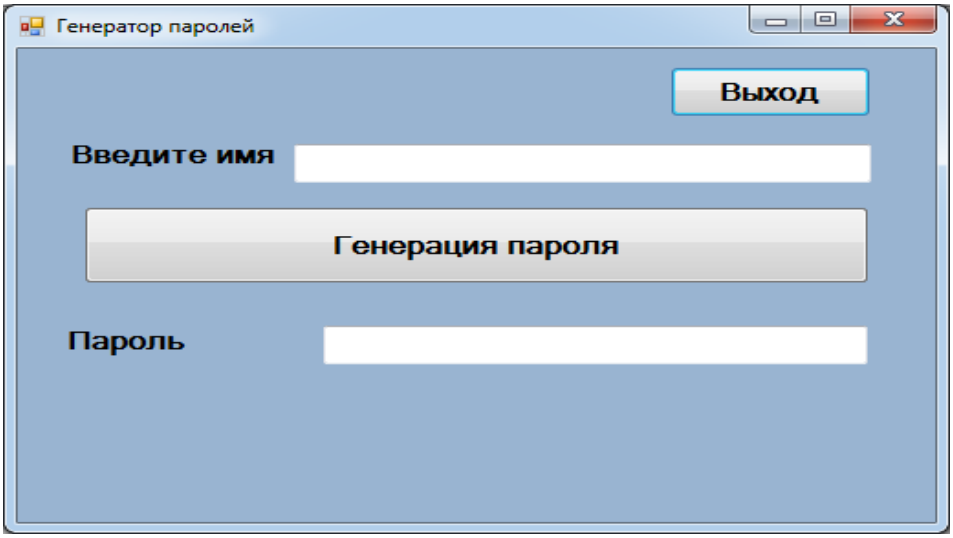


Рис. 1. Возможный вид оконной формы программы

Текст программы на кнопке «Выход»

```
  Close();
```

Примеры фрагментов программы на кнопке «Генерация пароля»

```
// описание строковых переменных
 String imp;
 String parol;

// проверка, что имя пользователя не пусто
if (textBox1.Text == "") textBox1.Text = "Не введено имя пользователя";

 // определение двух строковых переменных
String rbb = "АБВГДЕЁЖЗИЙКЛМНОПРСТУФХЦЧШЩЪЫЬЭЮЯ";
String mss = "$%^&*()";

// чтение (ввод) содержимого компонента textBox1
// (имени пользователя) в переменную imp
 imp = textBox1.Text;

// определение длины имени (идентификатора) пользователя
int dimp = imp.Length;
```

```
        // очистка пароль
        parol = "";
        // запуск датчика случайных чисел
        Random a = new Random();
          // случайный выбор числа в интервале от 0 до 9 и добавление его в
пароль
        int nn = a.Next(9);
        parol = parol + Convert.ToString(nn);
        // случайный выбор буквы из имени пользователя и добавление в пароль
         int q = dimp - 1;
         int mm = a.Next(q);
        parol = parol + imp[mm];
        // случайный выбор двух больших русских букв и добавление их в пароль
        int drbb = rbb.Length;
        q = drbb - 1;
        for (int i = 0; i < 2; i++)
                    {
              mm = a.Next(q);
              parol = parol + rbb[mm];
                    }
        // случайный  выбор специального символа из множества
        int dmss = mss.Length;
        q = dmss - 1;
        mm = a.Next(q);
        parol = parol + mss[mm];
       // добавление в пароль к-й буквы из имени пользователя,
       //где k есть остаток от деления на 10 длины имени
       // пользователя. Если к больше количества букв в имени,
       // то выбирается последняя буква
        int k = dimp % 10;
        if (k > dimp) k = dimp - 1;
        parol = parol + imp[k-1];

        // вывод сформированного пароля в компонент textBox2
        textBox2.Text = parol;
```

3.3. Задания для лабораторной работы № 3

Задание

Выполнить следующие действия:

- создать оконную форму для реализации задания, вариант задания выбрать из табл. 1; номер варианта совпадает с порядковым номером студента в списке группы;

- написать и отладить программу генерации пароля в соответствии с вариантом задания;
- продемонстрировать преподавателю работу программы;
- оформить отчет.

Отчет

Отчет должен содержать:
- титульный лист;
- задание;
- текст программы генерации пароля с комментариями, поясняющими группы операторов;
- скриншот оконной формы с результатами генерации пароля.

Таблица 1

Варианты заданий на формирование программы - генератора паролей

Вариант	Количество символов пароля	Перечень требований
1	6	1. b_1,Ь$_2$ - случайные цифры от 0 до 9. 2. b_3, b_4 - случайные символы из идентификатора (имени) пользователя. 4. b_5 - случайный символ из множества {!,",#,$,%,&,',(,),*}. 5. b_6 - случайная малая буква английского алфавита.
2	6	1. b_1 – случайный символ из идентификатора (имени) пользователя. 2. b_2– случайная малая буква английского алфавита. 3. b_3, b_4 _ случайные цифры от 0 до 9. 4. b_5, b_6 - случайный символ из множества {!,",#,$,%,&,',(,),*}.
3	7	1. b_1, b_2 - случайные малые буквы английского алфавита. 2. b_3, b_4 – случайные символы из идентификатора (имени) пользователя. 2. b_5, b_6 - случайные заглавные буквы английского алфавита. 3. b_7 - случайное число от 0 до 9.

Продолжение табл. 1

4	7	1. b_1, b_2 – случайные числа от 0 до 9. 2. b_3, b_4 – случайные малые буквы английского алфавита. 3. b_5 – случайный символ из множества {&, %, $, #, !} 4. b_6, b_7 - - случайные буквы из идентификатора (имя) пользователя.
5	8	1. b_1, b_2, b_3 - случайные цифры. 2. b_4, b_5 - случайные символы из множества {!,",#,$,%,&,',(,),*}. 3. b_6, b_7 - случайные буквы из идентификатора (имя) пользователя. 4. b_8 – случайная малая буква английского алфавита
6	8	1. b_1, b_2, b_3 - случайные малые буквы английского алфавита. 2. b_4, b_5, b_6 – случайные цифры от 0 до 9. 3. b_7 – случайная заглавная буква английского алфавита 4. b_8 – случайный символ из идентификатора (имя) пользователя
7	9	1. b_1,…, b_3 - случайные символы из множества {!,",#,$,%,&,',(,),*} 2. b_4,…,b_6 случайные малые буквы английского алфавита. 3. b_7, b_8 – случайные числа от 0 до 9 4. b_9 - случайный символ из идентификатора пользователя
8	9	1. b_1 – случайная цифра от 0 до 9. 2. b_2,b_3 – случайные буквы из идентификатора пользователя. 3. b_4, …, b_7 – случайные заглавные буквы английского алфавита. 4. b_8, b_9 – случайные малые буквы русского алфавита

Продолжение табл. 1

9	10	1. b_1, b_2 - случайные большие буквы английского алфавита. 2. b_3 ,…, b_5 - случайные символы из идентификатора пользователя. 3. b_6,…, b_{10} - случайные цифры от 0 до 9.
10	10	1. b_1, b_2 – случайные цифры от 0 до 9. 2. b_3,…, b_5 - случайные большие буквы английского алфавита. 3. b_6, …, b_8 - случайные символы из идентификатора пользователя. 4. b_9, b_{10} – случайные символы из множества {!,",#,$,%,&,',(,),*}.
11	8	1. b_1, b_2 - случайные символы из идентификатора пользователя. 2. b_3 ,…, b_5 - случайные большие буквы английского алфавита. 3. b_6, …, b_8 - случайные символы из множества {!,%"&,#,$+*',(,)}.
12	8	1. b_1, b_2 - случайные цифры. 2. b_3,…, b_5 - случайные малые буквы русского алфавита. 3. b_6 - случайный символ из множества {!,",#,$,%,&,',(,),*}. 4. b_7,b_8 – случайные символы из идентификатора пользователя.
13	8	1. b_1,Ь$_2$ - случайные символы из идентификатора пользователя. 2. b_3, b_4, b_5 - случайная цифра. 4. b_6 - случайный символ из множества {!,",#,$,%,&,',(,),*,[,]}. 5. b_7,b_8 - случайная малая буква английского алфавита.
14	9	1. b_1,b_2 – случайные цифры. 2. b_3,b_4,– случайные буквы английского алфавита. 3. b_5, b_6 – случайный символ из идентификатора пользователя. 4. b_7, b_8, b_9 - случайные символы из множества {!,",#,$,%,&,',(,),*}.

Продолжение табл. 1

15	8	1. b_1, b_2 - случайные малые буквы английского алфавита. 2. b_3,b_4,b_5 – случайные символы из идентификатора пользователя. 2. b_6, b_7 - случайные заглавные буквы английского алфавита. 3. b_8 – случайное число от 0 до 9.
16	6	1. b_1, b_2 – случайные числа от 0 до 6. 2. b_3, b_4 – случайные малые буквы английского алфавита 3. b_5, b_6 - случайные символы из идентификатора пользователя.
17	7	1. b_1, b_2 - случайные цифры. 2. b_3, b_4 - случайные символы из множества {",#,$,%,&,',(,),*}. 3. b_5, b_6 – случайные символы из идентификатора пользователя. 4. b7 – случайная малая буква английского алфавита.
18	8	1. b_1, b_2, b_3 - случайные малые буквы английского алфавита. 2. b_4, b_5 – случайные цифры от 0 до 9. 3. b_6 – случайная заглавная буква английского алфавита. 4. b_7,b_8 – случайные символы из идентификатора пользователя.
19	7	1. b_1,…, b_3 - случайные символы из множества {!,",#,$,%,&,',(,),*}, 2. b_4, …, b_6, - случайные малые буквы английского алфавита. 3. b_7 - случайный символ из идентификатора пользователя.
20	8	1. b_1, b_2 – случайные цифры от 0 до 9. 2. b_3 – случайный символ из идентификатора пользователя. 3. b_4 – случайная малая буква английского алфавита. 4. b_5,…, b_8 - случайные заглавные буквы английского алфавита.

Окончание табл. 1

21	7	1. b_1, b_2 – случайные буквы из имени пользователя. 2. b_3, b_4 – случайные числа от 0 до 9. 3. b_5, b_6 - случайные заглавные буквы русского алфавита 4. b_7 – случайная маленькая буква английского алфавита.
22	8	1. b_1, b_2 – случайные числа от 0 до 9. 2. b_3, b_4 – случайные буквы из имени пользователя. 3. b_5 , b_6 – случайные маленькие буквы английского алфавита. 4. b_7, b_8 - случайные заглавные буквы русского алфавита.
23	7	1. b_1, b_2 – случайные малые буквы русского алфавита. 2. b_3, b_4 – случайные заглавные буквы английского алфавита. 3. b_5, b_6 - случайные символы из имени пользователя. 4. b_7 – случайное число от 0 до 9.
24	8	1. b_1, b_2 – случайные символы из имени пользователя. 2. b_3, b_4 – случайные числа от 0 до 9. 3. b_5 , b_6 – случайная символы из множества {(*#^@+-%} 4. b_7, b_8 - случайные малые буквы русского алфавита.
25	7	1. $b_1, \ldots, b_3$ - случайные символы из имени пользователя. 2. $b_4, \ldots, b_6$, - случайные заглавные буквы английского алфавита. 3. b_7 - случайный символ из имени пользователя.

4. ЛАБОРАТОРНАЯ РАБОТА № 4
ШИФРОВАНИЕ СООБЩЕНИЙ МЕТОДОМ ПЕРЕСТАНОВКИ

4.1. Общие методические указания по выполнению лабораторной работы № 4

Цель работы - реализация простейших алгоритмов шифрования сообщений методом перестановки.

При использовании для шифрования методов перестановки символы открытого текста переставляются в соответствии с некоторыми правилами.

Пример 1. Открытый текст: "ШИФРОВАНИЕ_ПЕРЕСТАНОВКОИ". Ключ (правило перестановки): группы из 8 букв с порядковыми номерами 1.2.....8 переставить в порядок 3-8-1-5-2-7-6-4.

Шифротекст: "ФНШОИАВР_СИЕЕЕРПННТВАОКО".

Можно использовать более усложненную перестановку. Для этого открытый текст записывается в матрицу по определенному ключу k1. Шифротекст образуется при считывании из этой матрицы по ключу k2.

Пример 2. Открытый текст: "ШИФРОВАНИЕ_ПЕРЕСТАНОВКОЙ" зашифровать, используя два ключа перестановки. Ключи для перестановки: k1 3-4-2-5-1-6; k2 4-2-3-1.

В матрицу, состоящую из шести строк и четырех столбцов, записывают исходный текст. Затем строки перемешивают согласно ключу k1.

Исходная матрица

1	ш	и	ф	р
2	о	в	а	н
3	и	е	_	п
4	е	р	е	с
5	т	а	н	о
6	в	к	о	й

Запись по строкам в соответствии с ключом k1.

1	и	е	_	п
2	е	р	е	с
3	о	в	а	н
4	т	а	н	о
5	ш	и	ф	р
6	в	к	о	й

Чтение по столбцам осуществляют в соответствии с ключом k2 (4, 2, 3, 1). Шифротекст: "пснорйерваик_еанфоиеотшв".

4.2. Методические указания к написанию программы в Visual Studio (C#)

1 этап. Разработка интерфейса пользователя

Интерфейс пользователя может состоять из одного окна. Возможный вид окна представлен на рис. 2.

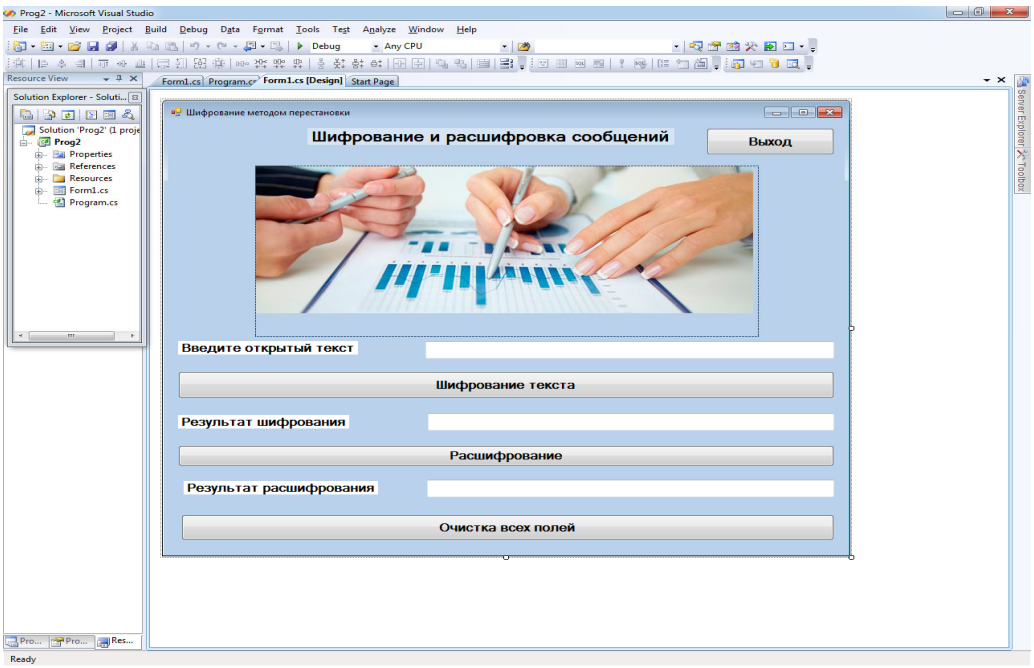


Рис. 2. Вид Интерфейс пользователя в программе на C#

Интерфейс может состоять из трех окон:
- главное окно программы (рис. 3);
- окно для реализации шифрования (рис. 4);
- окно для реализации расшифрования (рис. 5).

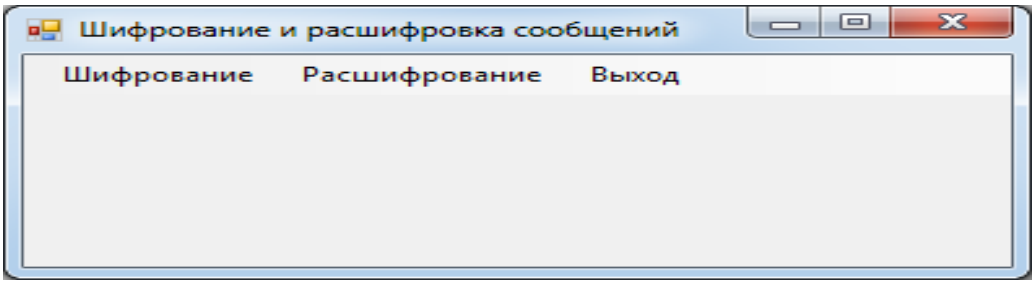


Рис. 3. Вид главного окна программы

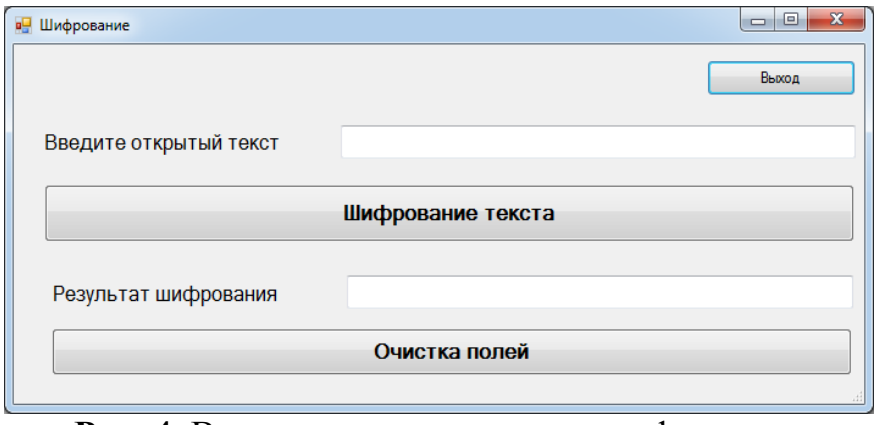


Рис. 4. Вид окна для реализации шифрования

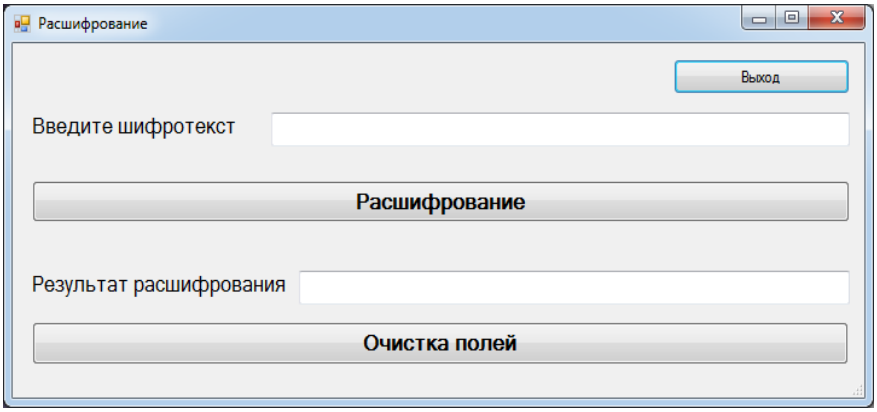


Рис. 5. Вид окна для реализации расшифрования

2 этап. Создание меню и настройка пунктов меню.

Формирование меню реализуют следующим образом:

- на главное окно ставят компонент MenuStrip;
- в поле ввода записывают название пункта меню и нажимают клавишу Enter;
- затем заполняют следующее поле ввода.

Добавление новых форм реализуют с помощью меню программы Visual Studio: Проект (Project), Добавить новую форму (Add Windows Form).

Привязку пункта меню «Шифрование» к вызову второй формы выполняют так:

- дважды щелкают по данному пункту меню;
- в тексте процедуры набирают

```
form f2 = new Form2();
f2.ShowDialog();
```

Вариант вызова формы означает, что пока форма Form2 не будет закрыта, доступ к другим формам будет невозможен.

Привязку пункта меню «Расшифрование» к вызову третьей формы выполняют так:

- дважды щелкают по данному пункту меню;
- в тексте процедуры набирают

```
form f3 = new Form3();
f3.ShowDialog();
```

Привязка пункта меню «Выход» к процедуре закрытия формы реализуют следующим образом:

- дважды щелкают по пункту меню «Выход»;
- в тексте процедуры набирают Close();

Для позиционирования главной формы в центре экрана форму выделяют и в свойстве StartPosition выбирают из списка CenterScreen.

Для позиционирования вызываемых форм в центре экрана вызываемую форму выделяют и в свойстве StartPosition выбирают из списка CenterParent.

3 этап. Написание программ

Пример программы на кнопке «Шифрование текста» представлен ниже. Ключ 4 3 1 2.

```
            String otext;
        String shtext;
        if (textBox1.Text == “”) textBox1.Text = “Не введено сообщение”;
        else
        {
     // Ввести открытый текст и определить его длину
            otext = textBox1.Text;
            int ds = otext.Length;
     // Очистить шифротекст
            shtext = «»;
    // Проверить, что длина сообщения кратна 4. Если не так, то дописать *
            int k = ds%4;
            if (k > 0)
            {
               k = 4 – k;
               for (int i = 1; i <= k; i++) otext = otext + “*”;
               ds = ds + k;
            }
            int j = 0;
// Шифрование методом перестановки
            while (j < ds)
            {
               shtext = shtext + otext[j + 3];
               shtext = shtext + otext[j + 2];
               shtext = shtext + otext[j];
               shtext = shtext + otext[j + 1];
               j = j + 4;
            }
// Вывод шифротекста
            textBox2.Text = shtext;
        }
```

Пример программы на кнопке «Расшифрование» представлен ниже.

```
String otext;
        String shtext;
        if (textBox2.Text == “”) textBox2.Text = “Нет шифротекста”;
        else
        {
// ввести шифротекст и определить его длину
            shtext = textBox2.Text;
            int ds = shtext.Length;
            otext = “”;
            int j = 0;
// Расшифрование
            while (j < ds)
            {
               otext = otext + shtext[j + 2];
               otext = otext + shtext[j + 3];
               otext = otext + shtext[j + 1];
               otext = otext + shtext[j];
               j = j + 4;
            }
// Вывод открытого текста
            textBox3.Text = otext;
        }
    }
```

Пример программа на кнопке «Очистка полей» представлен ниже.

```
    Private void button4_Click(object sender, EventArgs e)
    {
       textBox1.Text = “”;
       textBox2.Text = “”;        textBox3.Text = “”;
    }
```

4.3. Задания для лабораторной работы № 4

Задание

Выполнить следующие действия:

- создать оконные формы для реализации задания, вариант задания выбрать из табл. 2; номер варианта совпадает с порядковым номером студента в списке группы;

- первая оконная форма должна содержать меню: Шифрование, Расшифрование, Выход;

- вторая оконная форма содержит поле для ввода открытого текста; кнопку для вызова программы шифрования, поле для вывода зашифрованного текста;

- третья оконная форма содержит поле для ввода зашифрованного текста; кнопку для вызова программы расшифрования, поле для вывода открытого текста;

- написать и отладить программу шифрования открытого сообщения в соответствии с вариантом задания;

- написать и отладить программу расшифрования открытого сообщения в соответствии с вариантом задания;

- продемонстрировать преподавателю работу программ шифрования и расшифрования.

Отчет

Отчет должен содержать:

- титульный лист;
- задание;
- текст программы шифрования;
- текст программы расшифрования;
- скриншоты оконных форм с результатами шифрования и расшифрования сообщений.

Таблица 2

Варианты заданий к лабораторной работе № 4

Вариант	Задание на программирование
1	Реализовать шифрование и расшифровку методом перестановки. Ключ 5 4 2 1 3.
2	Реализовать шифрование и расшифровку методом перестановки. Ключ 3 4 2 1 5.
3	Реализовать шифрование и расшифровку методом перестановки. Ключ 4 2 3 1.
4	Реализовать шифрование и расшифровку методом перестановки. Ключ 2 1 4 3.
5	Реализовать шифрование и расшифровку методом перестановки. Ключ 3 1 5 2 4 7 6.
6	Реализовать шифрование и расшифровку методом перестановки. Ключ 3 7 2 5 4 1 6.
7	Реализовать шифрование и расшифровку методом перестановки. Ключ 5 4 2 1 3 6.
8	Реализовать шифрование и расшифровку методом перестановки. Ключ 6 5 4 2 1 3.
9	Реализовать шифрование и расшифровку методом перестановки. Ключ 5 6 4 2 1 3.
10	Реализовать шифрование и расшифровку методом перестановки. Ключ 3 4 6 5 4 2.
11	Реализовать шифрование и расшифровку методом перестановки. Ключ 2 1 6 5 4 3.

Окончание табл. 2

12	Реализовать шифрование и расшифровку методом перестановки. Ключ 2 1 5 4 3.
13	Реализовать шифрование и расшифровку методом перестановки. Ключ 4 5 3 1 2.
14	Реализовать шифрование и расшифровку методом перестановки. Ключ 3 1 5 2 4.
15	Реализовать шифрование и расшифровку методом перестановки. Ключ 3 4 2 1.
16	Реализовать шифрование и расшифровку методом перестановки. Ключ 3 1 2 4.
17	Реализовать шифрование и расшифровку методом перестановки. Ключ 3 2 1 4.
18	Реализовать шифрование и расшифровку методом перестановки. Ключ 1 4 3 2.
19	Реализовать шифрование и расшифровку методом перестановки. Ключ 1 3 5 8 2 4 7 6.
20	Реализовать шифрование и расшифровку методом перестановки. Ключ 8 3 1 5 2 6 7 4.
21	Реализовать шифрование и расшифровку методом перестановки. Ключ 5 1 3 7 2 4 8 6.
22	Реализовать шифрование и расшифровку методом перестановки. Ключ 4 5 1 8 2 3 6 7.
23	Реализовать шифрование и расшифровку методом перестановки. Ключ 3 1 5 6 2 4 7 8.
24	Реализовать шифрование и расшифровку методом перестановки. Ключ 7 8 5 1 2 4 3 6.
25	Реализовать шифрование и расшифровку методом перестановки. Ключ 8 5 1 2 4 3 6 7.

5. ЛАБОРАТОРНАЯ РАБОТА № 5 ШИФРОВАНИЕ СООБЩЕНИЙ МЕТОДОМ МОНОАЛФАВИТНОЙ ЗАМЕНЫ

5.1. Общие методические указания по выполнению лабораторной работы № 5

Цель работы – реализация алгоритмов шифрования сообщений методом моноалфавитной замены (подстановки).

Методы замены. Шифрование методом замены (подстановки) основано на алгебраической операции, называемой подстановкой.

Подстановка – это взаимно – однозначное отображение некоторого конечного множества M на себя.

Число N элементов этого множества называется степенью подстановки. Природа множества M роли не играет, поэтому можно считать, что M={1,2,…,N}.

В криптографии рассматриваются **четыре типа подстановки (замены)**: - моноалфавитная, - гомофоническая, - полиалфавитная; - полиграммная.

При **моноалфавитной** замене каждой букве алфавита открытого текста ставится в соответствие одна буква шифротекста из этого же алфавита.

Общая формула моноалфавитной замены имеет следующий вид:

$$Yi=(k1*Xi + k2),$$

где Yi – i-й символ алфавита шифротекста; k1 и k2 – константы; Xi – i-й символ открытого текста (номер буквы в алфавите); N – длина используемого алфавита.

Пример 1. Дан открытый текст: «шифрование_заменой». Зашифровать текст, используя алфавиты, приведенные в табл. 4.

Таблица 4

Алфавиты исходного текста и шифротекста

Алфавит исходного текста	а	б	в	г	д	е	ё	ж	з	и	й	к	л	м
Алфавит шифротекста	_	я	ю	э	ъ	ь	щ	ш	ы	ч	ц	х	ф	у
Алфавит исходного текста	н	о	п	р	с	т	у	ф	х	ц	ч	ы	ш	щ
Алфавит шифротекста	т	с	р	п	о	н	м	л	к	й	и	з	ж	ё
Алфавит исходного текста	ь	ъ	э	ю	я	_								
Алфавит шифротекста	е	д	г	в	б	а								

Открытый текст: «шифрование_заменой»

Шифротекст: «жчлпсю_тчьаы_уьтсц».

Пример 2. Задан шифр, определяемый формулой (**шифр Вижинера)**:

$$yi=(xi+ki),$$

где ki – i-ая буква ключа, в качестве которого используются слово или фраза**.**

Зашифровать открытый текст «ЗАМЕНА» шифром Вижинера. Ключ: слово «КЛЮЧ».

Каждой букве открытого текста ставится в соответствии цифра, начиная с 0 (табл. 5).

Таблица 5

Соответствие алфавита и цифр

Алфавит исходного текста	а	б	в	г	д	е	ё	ж	з	и	й	к	л	м	н	о	п	р	с
Цифра	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18

Окончание табл. 5

Алфавит исходного текста	т	у	ф	х	ц	ч	ы	ш	щ	ь	ъ	э	ю	я	_
Цифра	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33

Наложение ключа «КЛЮЧ» на открытый текст реализуется следующим образом:

З А М Е Н А
К Л Ю Ч К Л

Вычисление цифр для шифротекста:

y1= (x1 + k1) = (8+11) = 19 -> Т
y2= (x2 + k2) = (0+12) = 12 -> Л
y3= (x3 + k3) = (13+31) = 44 = 10-> Й
(если $y_i > 34$, то $y_i = y_i - 34$)
y4= (x4 + k4) = (5+24) = 29 -> Ъ
y5=(x5 + k5) = (14+11 = 25 -> Ы
y6=(x6 + k6) = (0+12) = 12 -> Л.

Шифртекст: "ТЛЙЪЫЛ".

Расшифрование реализуется по формуле:

$$x_i = (y_i - k_i)$$

Если $(y_i - k_i) < 0$, то прибавляется N (размер алфавита).

Наложение ключа на шифротекст:

ТЛЙЪЫЛ
КЛЮЧКЛ

Вычисление цифр для открытого текста:

x1 = (y1 - k1) = 19 – 11 = 8 -> З
x2 = (y2 - k2) = 12 – 12 = 0 -> А
x3 = (y3 – k3) = 10 – 31= -21 (+ 34) = 13 -> М

Если число меньше нуля, значит надо прибавить 34, получают 13, это буква М.

x4 = (y4 – k4) = 29 – 24 = 5 -> Е

x5 = (y5 – k5) = 25 – 11 = 14 -> Н

x6 = (y6 – k6) = 12 – 12 = 0 -> А

Результат расшифрования: «ЗАМЕНА»

Существуют и другие шифры, реализующие моноалфавитную замену. Например, **шифры Бофора**, которые используют формулы:

yi = (ki – xi) и yi = (xi – ki) .

Пример 3. Задан шифр, определяемый формулой (**шифр Бофора)**:

yi=(xi - ki),

где ki - i-ая буква ключа, в качестве которого используются слово или фраза**.**

Зашифровать открытый текст "шифрование" шифром Бофора. Ключ: "Бофор".

Каждой букве открытого текста ставится в соответствии цифра, начиная с 0 (табл. 5).

Наложение ключа «Бофор» на открытый текст реализуется следующим образом:

шифрование

бофорбофор

Реализация шифрования

Вычисление цифр для шифротекста:

y1= (x1 - k1) = (26 - 1) = 25 -> ы

y2 = (x2 - k2) = (9 - 15) = -6 + 34 = 28 -> ь

Если $(x_i - k_i) < 0$, то прибавляется N (размер алфавита).

y3 = (x3 - k3) = (21 - 21) = 0 -> а

y4 = (x4 - k4) = (17+15) = 2 -> в

y5 = (x5 - k5) = (15 – 17) = -2 + 34 = 32 -> я

Если $(x_i - k_i) < 0$, то прибавляется N (размер алфавита).

y6 = (x6 - k6) = (2 - 1) = 1 -> б.

y7 = (x7 - k7) = (0 - 15) = -15 + 34 = 19 -> т

Если $(x_i - k_i) < 0$, то прибавляется N (размер алфавита).

y8 = (x8 - k8) = (14 - 21) = -7 + 34 = 27 -> щ

y9 = (x9 - k9) = (9 - 15) = -6 + 34 = 28 -> ь

y10 = (x10 – k10) = (5 - 17) = -12 + 34 = 22 -> х

Шифротекст - ыьавябтщьх

Расшифрование осуществляют с использованием формулы:

$$xi = yi + ki$$

Наложение ключа на шифротекст
ыьавябтщьх
бофорбофор

Реализация расшифрования
Вычисление цифр для открытого текста:
x1 = (y1 = k1) = 25 + 1 = 26 -> ш
x2 = (y2 + k2) = 28 + 15 = 43 – 34 = 9 -> и
Если число больше или равно 34, то вычитается 34.
x3 = (y3 + k3) = 0 + 21= 21 -> ф
x4 = (y4 + k4) = 2 + 15= 17 -> р
x5 = (y5 + k5) = 32+ 17= 49 -34 = 15 -> о
Если число больше или равно 34, то вычитается 34.
x6 = (y6 + k6) = 1 + 1= 2 -> в
x7 = (y7 + k7) = 19 + 15= 34 – 34 = 0 -> а
Если число больше или равно 34, то вычитается 34.
x8 = (y8 + k8) = 27 + 21= 48 – 34 = 14 -> н
Если число больше или равно 34, то вычитается 34.
x9 = (y9 + k9) = 28 + 15= 43 – 34 = 9 -> и
Если число больше или равно 34, то вычитается 34.
x10 = (y10 + k10) = 22 + 17= 39 – 34 = 5 -> е
Если число больше или равно 34, то вычитается 34.
Результат расшифровки – слово «шифрование».

Основным недостатком моноалфавитного метода является то, что статистические свойства открытого текста (частоты повторения букв) сохраняются в шифротексте.

5.2. Задание для лабораторной работы № 5

Задание

Выполнить следующие действия:

- создать оконные формы для реализации задания, вариант задания выбрать из табл. 6;
- первая оконная форма должна содержать меню: Шифрование, Расшифрование, Выход;
- вторая оконная форма содержит исходные данные для реализации шифрования и выводит результат шифрования;
- третья оконная форма содержит исходные данные для реализации расшифрования и выводит результат расшифрования;

- написать и отладить программу шифрования открытого сообщения в соответствии с вариантом задания;

- написать и отладить программу расшифрования открытого сообщения в соответствии с вариантом задания;

- продемонстрировать преподавателю работу программ шифрования и расшифрования сообщений;

- оформить отчет.

Отчет

Отчет должен содержать:

- титульный лист;

- задание;

- текст программы шифрования;

- текст программы расшифрования;

- скриншоты оконных форм с результатами шифрования и расшифрования сообщений.

Таблица 6

Варианты задания для лабораторной работы № 5

Вариант	Задание на программирование
1	Реализовать шифрование и расшифровку сообщения методом моноалфавитной замены. Задать алфавит шифротекста со смещением символов исходного текста на 5 символов вправо.
2	Реализовать шифрование и расшифровку сообщения методом моноалфавитной замены. Задать алфавит шифротекста со смещением символов исходного текста на 10 символов вправо.
3	Реализовать шифрование и расшифровку сообщения методом моноалфавитной замены. Задать алфавит шифротекста со смещением символов исходного текста на 7 символов влево.
4	Реализовать шифрование и расшифровку сообщения методом моноалфавитной замены. Задать алфавит шифротекста со смещением символов исходного текста на 10 символов влево.
5	Реализовать шифрование и расшифровку сообщения методом моноалфавитной замены. Задать алфавит шифротекста со смещением символов исходного текста на 6 символов влево.
6	Реализовать шифрование и расшифровку сообщения методом моноалфавитной замены. Задать алфавит шифротекста со смещением символов исходного текста на 8 символов влево.

Продолжение табл. 6

7	Реализовать шифрование и расшифровку сообщения методом моноалфавитной замены. Задать алфавит шифротекста со смещением символов исходного текста на 6 символов вправо.
8	Реализовать шифрование и расшифровку сообщения методом моноалфавитной замены. Задать алфавит шифротекста со смещением символов исходного текста на 5 символов влево.
9	Реализовать шифрование и расшифровку сообщения методом моноалфавитной замены. Задать алфавит шифротекста со смещением символов исходного текста на 7 символов вправо.
10	Реализовать шифрование и расшифровку сообщения методом моноалфавитной замены. Задать алфавит шифротекста со смещением символов исходного текста на 8 символов вправо.
11	Реализовать шифрование и расшифровку сообщения методом моноалфавитной замены. Задать алфавит шифротекста со смещением символов исходного текста на 4 символа вправо.
12	Реализовать шифрование и расшифровку сообщения методом моноалфавитной замены. Задать алфавит шифротекста со смещением символов исходного текста на 4 символа влево.
13	Реализовать шифрование и расшифровку сообщения методом моноалфавитной замены. Задать алфавит шифротекста со смещением символов исходного текста на 9 символов вправо.
14	Реализовать шифрование и расшифровку сообщения методом моноалфавитной замены. Задать алфавит шифротекста со смещением символов исходного текста на 9 символов влево.
15	Реализовать шифрование с использованием шифра Бофора (yi=xi – ki). Ключом выбрать Ваше имя. Реализовать также расшифровку шифротекста.
16	Реализовать шифрование с использованием шифра Бофора (yi=xi – ki). Ключом выбрать слово «Экзамен». Реализовать также расшифровку шифротекста.

Окончание табл. 6

17	Реализовать шифрование с использованием шифра Вижинера. Ключом выбрать Вашу фамилию. Реализовать также расшифровку шифротекста.
18	Реализовать шифрование с использованием шифра Вижинера. Ключом выбрать слово «Зачет». Реализовать также расшифровку шифротекста.
19	Реализовать шифрование с использованием шифра Бофора (yi=ki – xi). Ключом выбрать Вашу фамилию. Реализовать также расшифровку шифротекста.
20	Реализовать шифрование с использованием шифра Бофора (yi=ki – xi). Ключом выбрать слово «совет». Реализовать также расшифровку шифротекста.
21	Реализовать шифрование с использованием шифра Бофора (yi=xi – ki). Ключом выбрать Вашу фамилию. Реализовать также расшифровку шифротекста.
22	Реализовать шифрование с использованием шифра Бофора (yi=xi – ki). Ключом выбрать слово «пятерка». Реализовать также расшифровку шифротекста.
23	Реализовать шифрование и расшифровку сообщения методом моноалфавитной замены. Задать алфавит шифротекста со смещением символов исходного текста на 9 символов влево.
24	Реализовать шифрование с использованием шифра Вижинера. Ключом выбрать Ваше имя. Реализовать также расшифровку шифротекста.
25	Реализовать шифрование с использованием шифра Вижинера. Ключом выбрать слово «Замена». Реализовать также расшифровку шифротекста.

6. ЛАБОРАТОРНАЯ РАБОТА № 6
ШИФРОВАНИЕ СООБЩЕНИЙ МЕТОДОМ ГОМОФОНИЧЕСКОЙ И ПОЛИАЛФАВИТНОЙ ЗАМЕНЫ

6.1. Общие методические указания по выполнению лабораторной работы № 6

Цель работы - реализация алгоритмов шифрования сообщений методом гомофонической или полиалфавитной замены (подстановки).

Гомофоническая замена означает, что одному символу открытого текста ставится в соответствие несколько символов шифротекста.

Этот метод применяется для искажения статистических свойств шифротекста.

Пример 3. Зашифровать открытый текст, используя гомофоническую замену. Открытый текст: "ЗАМЕНА".

Пример соответствия алфавита открытого текста трем шифротекстам представлен в табл. 7. Алфавит шифротекста задан, как числа, состоящие из трех цифр.

Таблица 7

Алфавиты открытого и шифротекста при гомофонической замене

Алфавит открытого текста	А Б ... Е Ж З ... М Н
Алфавиты шифротекста	117 123 197 147 176 132 155 131 144 151 167 119 128 184 148 163 115 133 159 161 134

Шифротекст: "176 117 132 197 155 131".

В данном шифротексте вторая буква А получила шифр 131, а не 117. Таким образом, при гомофонической замене каждая буква открытого текста заменяется по очереди цифрами столбца, соответствующими алфавиту шифротекста.

Полиалфавитная подстановка использует несколько алфавитов шифротекста. Пусть используется k алфавитов. Тогда открытый текст:

$X=X_1X_2...X_k\ X_{k+1}...X_{2k}\ X_{2k+1}...$

заменяется шифротекстом:

$Y=F1(X_1)\ F2(X_2)\ ...\ Fk(X_k)\ F1(X_{k+1})\ F2(X_{k+2})\ ...\ Fk(X_{2k})\ F1(X_{2k+1})\ F2(X_{2k+2})\ ...\ Fk(X_{3k})\ ...$

где Fi(Xj) означает символ шифротекста алфавита i для символа открытого текста Xj.

Пример 4. Зашифровать открытый текст, используя полиалфавитную подстановку. Открытый текст: "ЗАМЕНА", k=2. Подстановка задана в табл. 8.

Таблица 8

Алфавиты открытого текста и шифротекста при полиалфавитной замене

Алфавит открытого текста	А Б ... Е Ж З ... М Н
Алфавиты шифротекста	Л О Й С А Е Ф Г В И Ш Ъ У П

Y1=F1(x1)=F1(З)=А, Y2=F2(x2)=F2(А)=Г, Y3=F1(x3)=F1(М)=Е,
Y4=F2(x4)=F2(Е)=И,
Y4=F1(x5)=F1(Н)=Ф, Y6=F2(x6)=F2(А)=Г.

Шифротекст: "АГЕИФГ".

При расшифровке символы шифротекста, имеющие номера 1,3,5 и т.д., ищутся в первом алфавите шифротекста. Символы шифротекста, имеющие номера 2,4,6 и т.д. ищутся во втором алфавите шифротекста.

6.2. Задание для лабораторной работы № 6

Задание

Выполнить следующие действия:

- создать оконные формы для реализации задания, вариант задания выбрать из табл. 9;
- первая оконная форма должна содержать меню: Шифрование, Расшифрование, Выход;
- написать и отладить программу шифрования открытого сообщения в соответствии с вариантом задания;
- написать и отладить программу расшифрования открытого сообщения в соответствии с вариантом задания;
- продемонстрировать преподавателю работу программ шифрования и расшифрования;
- оформить отчет.

Отчет

Отчет должен содержать:

- титульный лист;
- задание;
- текст программы шифрования;
- текст программы расшифрования;
- скриншоты оконных форм с результатами шифрования и расшифрования сообщений.

Таблица 9

Варианты задания для лабораторной работы № 6

Вариант	Задание на программирование
1	Реализовать шифрование и расшифровку сообщения методом **полиалфавитной подстановки**. Использовать два алфавита шифротекста, которые задать самостоятельно. Первый символ шифруют из первого алфавита шифротекста, второй символ – из второго алфавита шифротекста, третий символ – снова из первого алфавита шифротекста.
2	Реализовать шифрование и расшифровку сообщения методом **полиалфавитной** подстановки. Использовать два алфавита шифротекста, которые задать самостоятельно. Если номер символа из открытого текста кратен трем, то для замены выбирают символ из первого алфавита шифротекста, в противном случае - для замены выбирают символ из второго алфавита шифротекста.
3	Реализовать шифрование и расшифровку сообщения методом **гомофонической** замены. Каждому символу открытого текста поставить в соответствие два символа шифротекста. Два алфавита шифротекста задать самостоятельно.
4	Реализовать шифрование и расшифровку сообщения методом **полиалфавитной** подстановки. Использовать два алфавита шифротекста, которые задать самостоятельно. Если номер символа из открытого текста кратен четырем, то для замены выбирают символ из первого алфавита шифротекста, в противном случае – для замены выбирают символ из второго алфавита шифротекста.
5	Реализовать шифрование и расшифровку сообщения методом **полиалфавитной** подстановки. Использовать два алфавита шифротекста, которые задать самостоятельно. Если номер символа из открытого текста кратен пяти, то для замены выбирают символ из первого алфавита шифротекста, в противном случае - для замены выбирают символ из второго алфавита шифротекста.

Продолжение табл. 9

6	Реализовать шифрование и расшифровку сообщения методом **полиалфавитной** подстановки. Использовать два алфавита шифротекста, которые задать самостоятельно. Если номер символа из открытого текста кратен семи, то для замены выбирают символ из первого алфавита шифротекста, в противном случае - для замены выбирают символ из второго алфавита шифротекста.
7	Реализовать шифрование и расшифровку сообщения методом **полиалфавитной** подстановки. Использовать два алфавита шифротекста, которые задать самостоятельно. Если номер символа из открытого текста нечетный, то для замены выбирают символ из первого алфавита шифротекста, в противном случае - для замены выбирают символ из второго алфавита шифротекста.
8	Реализовать шифрование и расшифровку сообщения методом **гомофонической** замены. Каждому символу открытого текста поставить в соответствие два символа шифротекста. Два алфавита шифротекста задать самостоятельно.
9	Реализовать шифрование и расшифровку сообщения методом **полиалфавитной** подстановки. Использовать два алфавита шифротекста, которые задать самостоятельно. Если номер символа из открытого текста четный, то для замены выбирать символ из первого алфавита шифротекста, в противном случае для замены выбирать символ из второго алфавита шифротекста.
10	Реализовать шифрование и расшифровку сообщения методом **полиалфавитной** подстановки. Использовать три алфавита шифротекста, которые задать самостоятельно. Первый символ шифруют из первого алфавита шифротекста, второй символ – из второго алфавита шифротекста, третий символ – снова из первого алфавита шифротекста. Для четвертого символа снова выбирают первый алфавит, для пятого символа – второй алфавит и т.д.
11	Реализовать шифрование и расшифровку сообщения методом **полиалфавитной** подстановки. Использовать три алфавита шифротекста, которые задать самостоятельно. Если номер символа из открытого текста кратен трем, то для замены выбирают символ из первого алфавита шифротекста. Если номер символа из открытого текста четный, то для замены выбирают символ из второго алфавита шифротекста. Если номер символа из открытого текста нечетный и не кратен трем, то для замены выбирают символ из третьего алфавита шифротекста.

Продолжение табл. 9

12	Реализовать шифрование и расшифровку сообщения методом **полиалфавитной** подстановки. Использовать два алфавита шифротекста, которые задать самостоятельно. Если номер символа из открытого текста кратен шести, то для замены выбирают символ из первого алфавита шифротекста, в противном случае для замены выбирают символ из второго алфавита шифротекста.
13	Реализовать шифрование и расшифровку сообщения методом **гомофонической** замены. Каждому символу открытого текста поставить в соответствие три символа шифротекста. Три алфавита шифротекста задать самостоятельно.
14	Реализовать шифрование и расшифровку сообщения методом **полиалфавитной** подстановки. Использовать два алфавита шифротекста, которые задать самостоятельно. Если номер символа из открытого текста кратен четырем, то для замены выбирают символ из второго алфавита шифротекста, в противном случае – для замены выбирают символ из первого алфавита шифротекста.
15	Реализовать шифрование и расшифровку сообщения методом **полиалфавитной** подстановки. Использовать два алфавита шифротекста, которые задать самостоятельно. Если номер символа из открытого текста кратен пяти, то для замены выбирают символ из второго алфавита шифротекста, в противном случае - для замены выбирают символ из первого алфавита шифротекста.
16	Реализовать шифрование и расшифровку сообщения методом **полиалфавитной** подстановки. Использовать два алфавита шифротекста, которые задать самостоятельно. Если номер символа из открытого текста нечетный, то для замены выбирают символ из первого алфавита шифротекста, в противном случае - для замены выбирают символ из второго алфавита шифротекста.
17	Реализовать шифрование и расшифровку сообщения методом **гомофонической** замены. Каждому символу открытого текста поставить в соответствие три символа шифротекста. Три алфавита шифротекста задать самостоятельно.
18	Реализовать шифрование и расшифровку сообщения методом **гомофонической** замены. Каждому символу открытого текста поставить в соответствие два символа шифротекста. Два алфавита шифротекста задать самостоятельно.

Продолжение табл. 9

19	Реализовать шифрование и расшифровку сообщения методом **полиалфавитной подстановки**. Использовать два алфавита шифротекста, которые задать самостоятельно. Первый символ шифруют из первого алфавита шифротекста, второй символ – из второго алфавита шифротекста, третий символ – снова из первого алфавита шифротекста и т.д.
20	Реализовать шифрование и расшифровку сообщения методом **полиалфавитной подстановки**. Использовать два алфавита шифротекста, которые задать самостоятельно. Первый символ шифруют из второго алфавита шифротекста, второй символ – из первого алфавита шифротекста, третий символ – снова из второго алфавита шифротекста и т.д.
21	Реализовать шифрование и расшифровку сообщения методом **полиалфавитной** подстановки. Использовать два алфавита шифротекста, которые задать самостоятельно. Если номер символа из открытого текста кратен четырем, то для замены выбирают символ из второго алфавита шифротекста, в противном случае – для замены выбирают символ из первого алфавита шифротекста.
22	Реализовать шифрование и расшифровку сообщения методом **полиалфавитной** подстановки. Использовать два алфавита шифротекста, которые задать самостоятельно. Если номер символа из открытого текста кратен пяти, то для замены выбирают символ из второго алфавита шифротекста, в противном случае - для замены выбирают символ из первого алфавита шифротекста.
23	Реализовать шифрование и расшифровку сообщения методом **полиалфавитной** подстановки. Использовать два алфавита шифротекста, которые задать самостоятельно. Если номер символа из открытого текста кратен семи, то для замены выбирают символ из второго алфавита шифротекста, в противном случае - для замены выбирают символ из первого алфавита шифротекста.
24	Реализовать шифрование и расшифровку сообщения методом **полиалфавитной** подстановки. Использовать два алфавита шифротекста, которые задать самостоятельно. Если номер символа из открытого текста четный, то для замены выбирать символ из второго алфавита шифротекста, в противном случае для замены выбирать символ из первого алфавита шифротекста.

Окончание табл. 9

25	Реализовать шифрование и расшифровку сообщения методом **полиалфавитной** подстановки. Использовать три алфавита шифротекста, которые задать самостоятельно. Первый символ шифруют из первого алфавита шифротекста, второй символ – из второго алфавита шифротекста, третий символ – снова из первого алфавита шифротекста. Для четвертого символа снова выбирают первый алфавит, для пятого символа – второй алфавит и т.д.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Мельников В. П. Информационная безопасность : учебное пособие / под ред. С. А. Клейменова. - 8-е изд., испр. - М.: Академия, 2013.

2. Сергеева Т. И. Сергеев М.Ю. Методы и средства защиты компьютерной информации: учебное пособие/ Т. И. Сергеева, М. Ю. Сергеев – Воронеж: ВГТУ, 2011.

3. Алексеев В.А. Методы и средства криптографической защиты информации [Электронный ресурс]: методические указания к проведению лабораторных работ по курсу «Методы и средства защиты компьютерной информации»/ В. А. Алексеев— Электрон. текстовые данные.— Липецк: Липецкий государственный технический университет, ЭБС АСВ, 2009.— 16 с.— Режим доступа: http://www.iprbookshop.ru/17710.html.— ЭБС «IPRbooks»

4. Башлы, П. Н. Информационная безопасность и защита информации [Электронный ресурс]: учебное пособие/ П. Н. Башлы, А. В. Бабаш, Е. К. Баранова— Электрон. текстовые данные.— М.: Евразийский открытый институт, 2012.— 311 с.— Режим доступа: http://www.iprbookshop.ru/10677.html.— ЭБС «IPRbooks»

ОГЛАВЛЕНИЕ

ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

МЕТОДИЧЕСКИЕ УКАЗАНИЯ

к выполнению лабораторных работ
по дисциплине «Информационная безопасность и защита информации»
для студентов направления 38.03.05 «Бизнес-информатика»
(профиль «Информационные системы в бизнесе»)
очной и заочной форм обучения

Составители:
Сергеева Татьяна Ивановна
Сергеев Михаил Юрьевич

Компьютерный набор Т.И. Сергеевой

Подписано к изданию 26.01.2022.
Уч.-изд. л. 1,9.

ФГБОУ ВО «Воронежский государственный технический университет»
394026 Воронеж, Московский просп., 14