

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ  
ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ  
ВЫСШЕГО ОБРАЗОВАНИЯ  
«НОВОСИБИРСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»

---

Кафедра защиты информации



Новосибирский  
государственный  
технический университет  
**НЭТИ**

**РАСЧЕТНО-ГРАФИЧЕСКАЯ РАБОТА**  
по дисциплине: «Программирование»

Выполнил(а):  
Студент(ка) гр. « *название* », « *факультет* »  
« *ФИО* »  
« \_\_\_ » \_\_\_\_\_ 20\_\_ г.

\_\_\_\_\_  
(подпись)

Проверил:  
*доцент кафедры ЗИ*  
*Архипова А. Б.*  
« \_\_\_ » \_\_\_\_\_ 20\_\_ г.

\_\_\_\_\_  
(подпись)

Новосибирск 2025

## СОДЕРЖАНИЕ

*(содержание до второго уровня заголовков, содержание только  
автособираемое)*

**ОБРАТИТЕ ВНИМАНИЕ НА РЕГИСТР ТЕКСТА В СОДЕРЖАНИИ:**

Введение .....	3
1. Теоретические аспекты реализации методов шифрования .....	4
1.1 Математическое обоснование алгоритма работы шифра Гронсфельда .....	4
1.2 Алгоритм работы шифра с помощью квадрата Полибия .....	4
1.3 Алгоритм работы шифра Атбаша .....	4
1.4 Алгоритм работы шифра Виженера .....	4
1.5 Алгоритм работы шифра «Тарабарская грамота» .....	4
2. Практическая часть .....	6
2.1 Техническое задание .....	6
2.2 Характеристика задачи .....	7
2.3 Алгоритм решения .....	7
2.4 Руководство пользователя .....	8
2.5 Руководство системного программиста .....	10
2.6 Контрольный пример .....	12
Заключение .....	13
Список использованных источников .....	14
Приложение А .....	15
Приложение В .....	16

## ВВЕДЕНИЕ

В общем случае, во введении следует:

- показать сущность и значимость вопросов, рассмотренных в работе (то есть суть проблемы и актуальность, «значимость» ее решения);
- охарактеризовать проблему, к которой относится тема работы (изложить историю вопроса, дать оценку современного состояния);
- указать цель выполнения работы;
- изложить задачи, которые необходимо решить в процессе выполнения работы;
- изложить ожидаемые результаты, отметить эффективность и новизну работы.

*Обязательно должны быть строки:*

Теоретической основой написания расчетно-графической работы явились .... следующих авторов С. И. Петрова [1], С. И. Иванова [2-4].

Практической основой написания расчетно-графической работы явились учебные материалы по языку программирования .... [1-15], среде разработки .... [2-5].

## **1. Теоретические аспекты реализации методов шифрования**

В программе используется 5 методов шифрования: Гронсфельда, квадрата Полибия, Атбаша, Виженера и «Тарабарская грамота». Шифр Гронсфельда и Виженера реализуют с помощью ключей шифрования.

### **1.1 Математическое обоснование алгоритма работы шифра Гронсфельда**

*(анализ литературы (минимум 1,5 страницы) по рассматриваемому виду шифра, с указанием ссылок на использованные источники, например [1] или [1-3]).*

### **1.2 Алгоритм работы шифра с помощью квадрата Полибия**

*(анализ литературы (минимум 1,5 страницы) по рассматриваемому виду шифра, с указанием ссылок на использованные источники, например [1] или [1-3]).*

### **1.3 Алгоритм работы шифра Атбаша**

*(анализ литературы (минимум 1,5 страницы) по рассматриваемому виду шифра, с указанием ссылок на использованные источники, например [1] или [1-3]).*

### **1.4 Алгоритм работы шифра Виженера**

*(анализ литературы (минимум 1,5 страницы) по рассматриваемому виду шифра, с указанием ссылок на использованные источники, например [1] или [1-3]).*

### **1.5 Алгоритм работы шифра «Тарабарская грамота»**

*(анализ литературы (минимум 1,5 страницы) по рассматриваемому виду шифра, с указанием ссылок на использованные источники, например [1] или [1-3]).*

*В Приложении А помещается скрин страницы антиплагиата.  
Оригинальность текста от 75%.*

## **2. Практическая часть**

### **2.1 Техническое задание**

#### **2.1.1 Постановка задачи**

Необходимо разработать программу, которая должна шифровать и расшифровать исходные данные одним из представленных алгоритмов. Программа должна выполнять следующие основные действия:

- обеспечить процедуру проверки пользовательских данных путем авторизации в системе;
- предусмотреть ввод исходного текста с клавиатуры или загрузку данных из файла;
- реализовать шифрование данных и демонстрацию полученных результатов;
- реализовать дешифрование (расшифрование) данных и демонстрацию полученных результатов (консоль, файл).

Методы шифрования реализовать в виде отдельных функций/модулей.

ДАЛЕЕ СТАРОСТЫ СОСТАВЯТ ДОКУМЕНТ ПО ПУНКТУ 2.1

## 2.2 Характеристика задачи

2.2.1 Программа «*Название программы*» предназначена для автоматизации шифрования и расшифрования исходных данных авторизованного в системе пользователя.

2.2.2 Программа используется пользователем для защиты персональной информации.

2.2.3 Периодичность решения задачи по запросу пользователя.

2.2.4 Прекращение автоматизированного решения задачи происходит при отключении источника электропитания ЭВМ.

2.2.5 Связь с другими задачами отсутствует.

2.2.6 Специальных ограничений на временные характеристики решения задачи не налагается.

2.2.7 Специальных требований на уровень подготовки пользователя не налагается. Но лицо, работающее с программой, должно иметь минимальное представление о компьютере (знание необходимых операций).

## 2.3 Алгоритм решения

1. Запустить приложение «*Название программы*»;

2. Вывод: "Пароль:";

3. Ввод пароля;

4. Вывод меню:

"Выберите шифр: "

"Нажмите 1 для выбора шифра Гронсфельда"

"Нажмите 2 для выбора шифра с помощью квадрата Полибия"

"Нажмите 3 для выбора шифра Атбаша"

"Нажмите 4 для выбора шифра Виженера"

"Нажмите 5 для выбора шифра 'Тарабарская грамота'";

- 4.1 Если выбран пункт – "Нажмите 1 для выбора шифра Гронсфельда";
  - 4.1.1 Вывод: " Введите сообщение: ";
  - 4.1.2 Ввод сообщения;
  - 4.1.3 Вывод подменю: " Введите ключ: ";
  - 4.1.4 Ввод ключа;
  - 4.1.5 Шифрование текста шифром Гронсфельда;
  - 4.1.6 Вывод зашифрованного сообщения на консоль и в файл 1.txt;
  - 4.1.7. Дешифровка текста шифром Гронсфельда;
  - 4.1.8. Вывод дешифрованного сообщения на консоль и в файл 2.txt;
  - 4.1.9 Вывод: " Нажмите Enter для выбора другого шифра";
  - 4.1.10 Если нажата клавиша Enter, переход на п. 4;
- (фрагмент пропущен)

## **2.4 Руководство пользователя**

### **2.4.1 Введение**

2.4.1.1 Программа «*Название программы*» предназначена для .....

2.4.1.2 Программа предоставляет пользователю следующие возможности:

- полный доступ в систему;
- ввод, изменение, удаление данных .....
- .
- выдача документов в формате .....

2.4.1.3 Программа реализована на алгоритмическом языке ..... Работает в любой среде совместимой с «*указать ОС*». Дискковой памяти для запуска программы требуется не менее.... Мб. Оперативной памяти для нормальной работы программы требуется не менее ..... Мб.



### 2.4.2 Описание операций

Основные функции программы «*Название программы*» соответствуют ..... Для удобства пользователя и более легкого изучения системы большинство форм и диалогов имеют идентичный интерфейс. Далее описаны все функции системы, а также формы и диалоги для ввода и вывода информации. Для каждой формы приведены основные компоненты и их назначение.

После входа в систему на экран выводится главное окно программы. Вид окна приведен на рисунке 2.1. Для начала работы с программой необходимо ввести правильный пароль (в данном случае «6230»)



Рисунок 2.1 - Главное окно программы

В случае неверного ввода пароля ....

Далее программа предлагает пользователю на выбор один из пяти алгоритмов шифрования (рисунок 2.2)

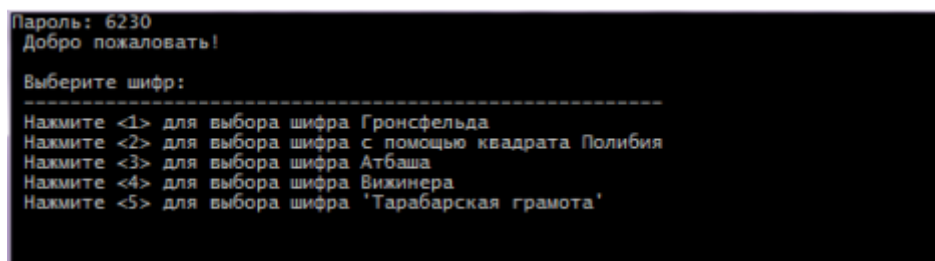


Рисунок 2.2 – Вывод меню и выбор пункта

(фрагмент пропущен)

### 2.4.3 Сообщения пользователю

При работе с программой могут появиться следующие сообщения, представленные в таблице 2.1.

Таблица 2.1 – Сообщения пользователю

Текст сообщения программы	Ответ пользователя
Нет записей для редактирования.	В таблице нет записей.
Запись уже существует.	При добавлении или редактировании данных продублировали уже существующую запись.
Не все поля введены.	Заполнить не введенные поля.
Отсутствует база данных!	Проверить наличие базы данных в каталоге с программой.

#### 2.4.4 Аварийные ситуации

К аварийным ситуациям относятся: нехватка оперативной памяти для создания окна программы. Если исполняемый модуль программы не запускается, либо не выполнены требования условия работы программы, либо один из файлов поврежден, необходимо обратиться к разработчику программы.

### 2.5 Руководство системного программиста

Программа реализована на языке C++ в среде Eclipse, основанном на визуальном построении приложений (помещение компонентов на формы и изменение их свойств и методов), поэтому некоторые функции формирования окон и отчетов невозможно описать в списке функций и листинге программы.

Модули программы:

Header.h - заголовочный файл, содержит объявления всех функций, использованных в данной программе;

Source.cpp – файл содержит определение функций, объявленных в заголовочном файле Header.h:

string gronsfeld(const string& text) - шифрование текста алгоритмом Гронсфельда;

main.cpp. Содержит функцию main, представляющую функционал по вводу пароля, выводу меню выбора шифров, с соответствующим вызовом функций, и вводом необходимых данных.

*(фрагмент пропущен – расписать все модули и назначение прототипов функций)*

Программа содержит ряд сообщений, предназначенных для сигнализации ошибок:

1. «Неверный пароль» – ошибка при введении неверного пароля; программа не выдаст меню выбора алгоритмов шифрования.

2. "Повторите попытку!!!" – ошибка при вводе пункта меню; программа предложит ввести другой (существующий) номер.

Связь модулей программы между собой представлена на рисунке 2.10.



Рисунок 2.10 – Связь модулей программы

Сообщения системному программисту приведены в таблице 2.2.

Таблица 2.2 – Сообщения системному программисту

Текст сообщения	Расшифровка
Missing Connection	Таблица не активна
Table 'work.[]' does not exist	Таблица не существует
Field [] not found	Табличное поле не найдено
Could not perform this operation because another user change this record	Невозможно выполнить эту операцию, потому что другой пользователь изменил эту запись
[] is not a valid integer value	[] не является корректным значением типа integer
Data too long	Строка или значение не соответствуют полю по длине
Can not perform this operation on a closed dataset	Невозможно выполнить эту операцию над закрытым источником данных
Invalid descriptor	Неправильный дескриптор окна

## 2.6 Контрольный пример

После запуска на экран выводится главное окно программы, вид которого представлен на рисунке 2.11.

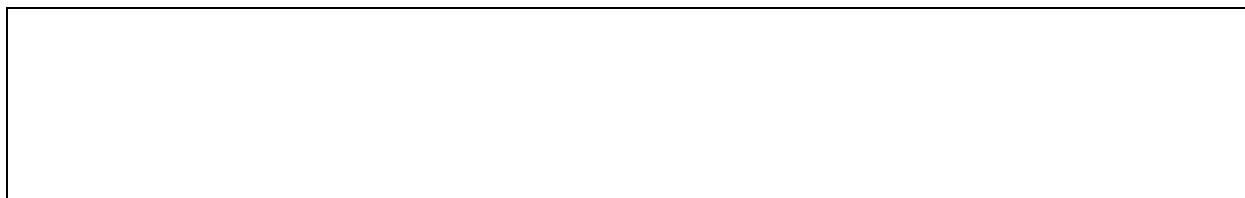


Рисунок 2.11 – Главное окно программы

*(Далее необходимо провести пользователя по всему функционалу программы последовательно, с демонстрацией всех модификаций визуального отображения экранных форм. В завершении представить ручной расчет по каждому примеру, представленному в данном подразделе. Результаты работы программы и результаты ручного расчета должны быть равны).*

## ЗАКЛЮЧЕНИЕ

В результате выполнения расчетно-графической работы были достигнуты основные цели:

1.

*(фрагмент пропущен)*

Для достижения поставленных целей были выполнены следующие задачи:

1. Изучен процесс ...

*(фрагмент пропущен)*

На сегодняшний день .... Данные об объекте внесены в журнал учета аттестованных объектов организации, проводившей аттестацию

2/3 листа

## СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

*(источники оформляются по ГОСТ. Год издания – не старше 5 лет (кроме математической литературы), нельзя ссылаться на habr, wiki..., allreferat и т.п.)*

1. Иванова Г.С. Средства процедурного программирования Microsoft Visual C++ 2008 [Электронный ресурс]: учебное пособие/ Г.С. Иванова, Т.Н. Ничушкина, Р.С. Самарев— Электрон. текстовые данные.— М.: Московский государственный технический университет имени Н.Э. Баумана, 2012.— 140 с.— Режим доступа: <http://www.iprbookshop.ru/31263.html>.— ЭБС «IPRbooks» (дата обращения 25.09.2025 г.).

2. Окулов С.М. Основы программирования [Электронный ресурс]/ Окулов С.М.— Электрон. текстовые данные.— Москва: Лаборатория знаний, 2020.— 337 с.— Режим доступа: <http://www.iprbookshop.ru/6449.html>.— ЭБС «IPRbooks» (дата обращения 25.09.2025 г.).

*Минимум 10 источников*

## **ПРИЛОЖЕНИЕ А**

### **Отчет антиплагиат**

(скриншот)

## ПРИЛОЖЕНИЕ В

### Текст программы

Mainform\_ – Главный модуль программы

*(текст программы – шрифт любой, цвет – любой (видимый), можно в две колонки размещать)*

```
#include <iostream>
```