Лабораторная работа №2

Markdawn

Румянцева Александра Сергеевна

30 сентября, 2022

Цели и задание на лабораторную работу

Цель работы: научиться оформлять отчёты с помощью легковесного языка разметки Markdown.

Задание: сделать отчёт по предыдущей лабораторной работе в формате Markdown. В качестве отчёта предоставить отчёты в 3 форматах: pdf, docx и md (в архиве, поскольку он должен содержать скриншоты, Makefile и т.д.).

Выполнение лабораторной работы

Для данной работы я создавала отчёт по лабораторной работе по дисциплине “Математические основы защиты и нформации и информационной безопасности”. Разберём основные моменты, которые были мною написаны с помощью Markdawn для создания отчета. На рис. 1 показано оформление титульного листа, а именно: заголовка, подзаголовка, указание автора и его харакетистик, указание даты выполнения работы.

```
---
# Front matter
lang: ru-RU
title: 'Отчёт по лабораторной работе 2'
subtitle: 'Тема лабораторной работы: Шифры перестановки'
author:
- "Студент: Румянцева Александра Сергеевна, 1132223493"
- "Группа: НПМмд-02-22"
- "Преподаватель: Кулябов Дмитрий Сергеевич,"
- "д-р.ф.-м.н., проф."
date: "Москва 2022"
```

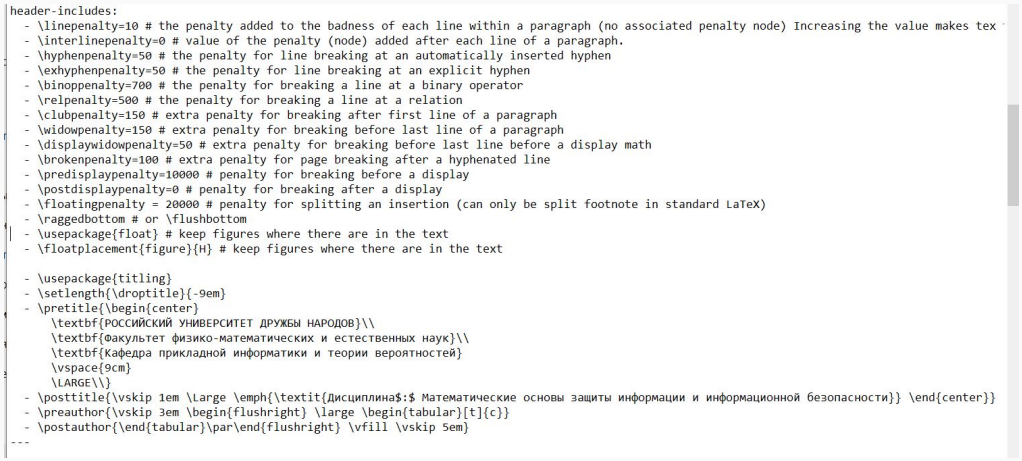
Figure 1: Рис. 1. Оформление титульного листа отчета.

На рисунке 2 видим автоматическое создание раздела содержаниеи и списков рисунков и таблиц (для пдф), а также указание к оформлению текста (шрифт, отступ, шрифты и тп), указаны используемые языки в тексте отчета, и способ конвентаризации в пдф (через lualatex).

```
# Formatting
toc-title: 'Содержание'
toc: true # Table of contents
toc_depth: 2
lof: true # List of figures
lot: true # List of tables
fontsize: 12pt
linestretch: 1.5
papersize: a4paper
documentclass: scrreprt
polyglossia-lang: russian
polyglossia-otherlangs: english
mainfont: PT Serif
romanfont: PT Serif
sansfont: PT Sans
monofont: PT Mono
mainfontoptions: Ligatures=TeX
romanfontoptions: Ligatures=TeX
sansfontoptions: Ligatures=TeX,Scale=MatchLowercase
monofontoptions: Scale=MatchLowercase
indent: true
pdf-engine: lualatex
```

Figure 2: Рис. 2. Указания к оформлению файлов и форматированию текста.

На рис. 3 интересен второй абзац, который добавляет оформление к титульному листу для конвертированного в пдф файла.



```
header-includes:
  - \linepenalty=10 # the penalty added to the badness of each line within a paragraph (no associated penalty node) Increasing the value makes tex
  - \interlinepenalty=0 # value of the penalty (node) added after each line of a paragraph.
  - \hyphenpenalty=50 # the penalty for line breaking at an automatically inserted hyphen
  - \exhyphenpenalty=50 # the penalty for line breaking at an explicit hyphen
  - \binoppenalty=700 # the penalty for breaking a line at a binary operator
  - \relpenalty=500 # the penalty for breaking a line at a relation
  - \clubpenalty=150 # extra penalty for breaking after first line of a paragraph
  - \widowpenalty=150 # extra penalty for breaking before last line of a paragraph
  - \displaywidowpenalty=50 # extra penalty for breaking before last line before a display math
  - \brokenpenalty=100 # extra penalty for page breaking after a hyphenated line
  - \predisplaypenalty=10000 # penalty for breaking before a display
  - \postdisplaypenalty=0 # penalty for breaking after a display
  - \floatingpenalty = 20000 # penalty for splitting an insertion (can only be split footnote in standard LaTeX)
  - \raggedbottom # or \flushbottom
  - \usepackage{float} # keep figures where there are in the text
  - \floatplacement{figure}{H} # keep figures where there are in the text

  - \usepackage{titling}
  - \setlength{\droptitle}{-9em}
  - \pretitle{\begin{center}
      \textbf{РОССИЙСКИЙ УНИВЕРСИТЕТ ДРУЖБЫ НАРОДОВ}\\
      \textbf{Факультет физико-математических и естественных наук}\\
      \textbf{Кафедра прикладной информатики и теории вероятностей}
      \vspace{9cm}
      \LARGE\\}
  - \posttitle{\vskip 1em \Large \emph{\textit{Дисциплина$:$ Математические основы защиты информации и информационной безопасности}} \end{center}}
  - \preauthor{\vskip 3em \begin{flushright} \large \begin{tabular}[t]{c}}
  - \postauthor{\end{tabular}\par\end{flushright} \vfill \vskip 5em}
---
```

Figure 3: Рис. 3. Техническая информация и указания к оформлению.

На рис. 4 начинается описание самой работы. Видно применение создания заголовков для глав работы, которые обозначения знаком “#”. Применено полужирное начертание текста с помощью двайных звёздочек в начале и в конце фраз. А в главах задач и в теоретической части видно оформление пронумерованного списка.

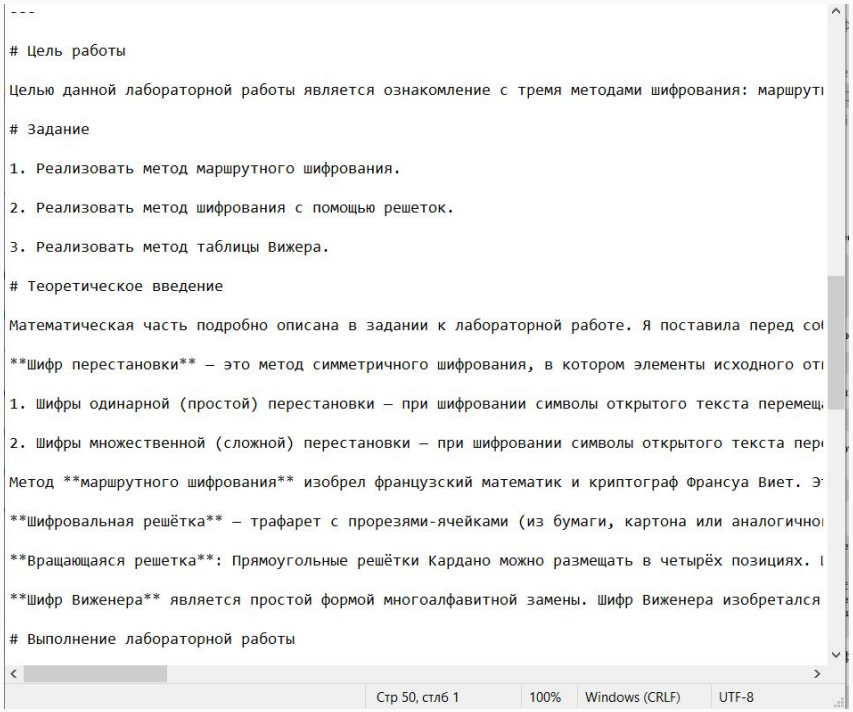
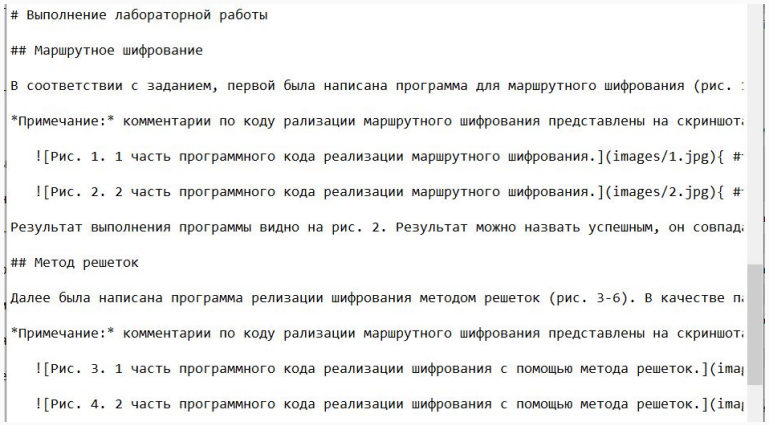


Figure 4: Рис. 4. Оформнение основной части работы с применением заголовков глав текста, полужирного шрифта, нумерационного списка.

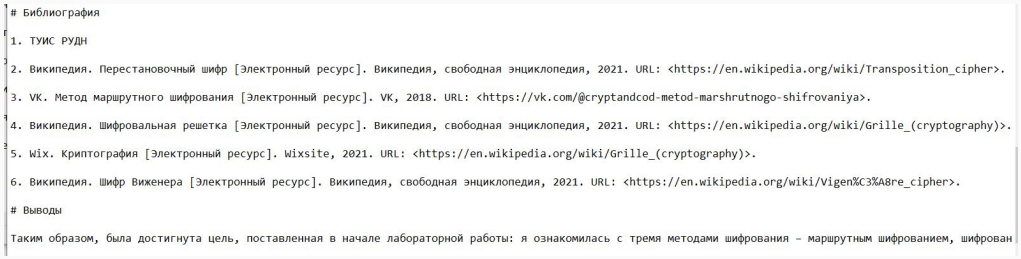
На рис. 5 начинается описание практической части работы. Видно применение создания заголовков разных уровней, то есть глав, обозначенных “#” и их подглав, обозначенных “##”. Далее применено курсивное начертание текста с помощью одинарной звёздочки в начале и в конце фраз. Показано как добавлять рисунок/картинку в отчет: через название рисунка{#fig: порядковый номер рисунка в отчете width=размер/разрешение рисунка%}



```
# Выполнение лабораторной работы

## Маршрутное шифрование

В соответствии с заданием, первой была написана программа для маршрутного шифрования (рис. 1

*Примечание:* комментарии по коду рализации маршрутного шифрования представлены на скриншот

   ![Рис. 1. 1 часть программного кода реализации маршрутного шифрования.](images/1.jpg){ #

   ![Рис. 2. 2 часть программного кода реализации маршрутного шифрования.](images/2.jpg){ #

Результат выполнения программы видно на рис. 2. Результат можно назвать успешным, он совпад

## Метод решеток

Далее была написана программа релизации шифрования методом решеток (рис. 3-6). В качестве п

*Примечание:* комментарии по коду рализации маршрутного шифрования представлены на скриншот

   ![Рис. 3. 1 часть программного кода реализации шифрования с помощью метода решеток.](ima

   ![Рис. 4. 2 часть программного кода реализации шифрования с помощью метода решеток.](ima
```

Figure 5: Рис. 5. Оформление практической работы с использованием заголовков разных уровнений, курсивного текста, добавлления рисунков.

Оформление ссылок показано на рис 6, а именно это возможно через < ссылка >



```
# Библиография

1. ТУИС РУДН

2. Википедия. Перестановочный шифр [Электронный ресурс]. Википедия, свободная энциклопедия, 2021. URL: <https://en.wikipedia.org/wiki/Transposition_cipher>.

3. VK. Метод маршрутного шифрования [Электронный ресурс]. VK, 2018. URL: <https://vk.com/@cryptandcod-metod-marshrutnogo-shifrovaniya>.

4. Википедия. Шифровальная решетка [Электронный ресурс]. Википедия, свободная энциклопедия, 2021. URL: <https://en.wikipedia.org/wiki/Grille_(cryptography)>.

5. Wix. Криптография [Электронный ресурс]. Wixsite, 2021. URL: <https://en.wikipedia.org/wiki/Grille_(cryptography)>.

6. Википедия. Шифр Виженера [Электронный ресурс]. Википедия, свободная энциклопедия, 2021. URL: <https://en.wikipedia.org/wiki/Vigen%C3%A8re_cipher>.

# Выводы

Таким образом, была достигнута цель, поставленная в начале лабораторной работы: я ознакомилась с тремя методами шифрования – маршрутным шифрованием, шифрован
```

Figure 6: Рис. 6. Оформление активных ссылок в тексте.

3. Конвертирование

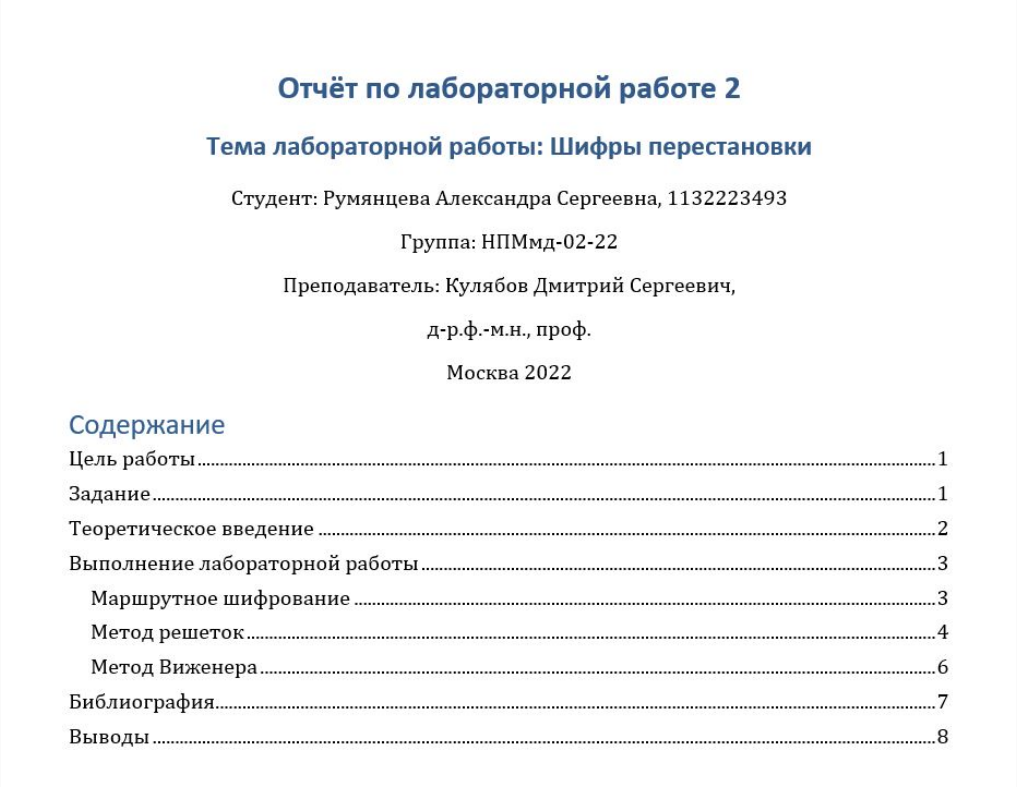
Конвертировала текст с помощью командной строки используя:

pandoc –filter pandoc-crossref -o report.docx report.md

pandoc –filter pandoc-crossref -o report.pdf report.md

В папке заранее находился Makefile, файл пандок, папка с фотографиями, которые добавлялись в отчет.

Рассмотрим ворд файл. Титульный лист и содержание.



Отчёт по лабораторной работе 2

Тема лабораторной работы: Шифры перестановки

Студент: Румянцева Александра Сергеевна, 1132223493

Группа: НПМмд-02-22

Преподаватель: Кулябов Дмитрий Сергеевич,

д-р.ф.-м.н., проф.

Москва 2022

Содержание

Figure 7: Рис. 7. Docx файл. Титульный лист и содержание.

Рассмотрим пдф файл. Титульный лист.

РОССИЙСКИЙ УНИВЕРСИТЕТ ДРУЖБЫ НАРОДОВ
Факультет физико-математических и естественных наук
Кафедра прикладной информатики и теории вероятностей

Отчёт по лабораторной работе 2

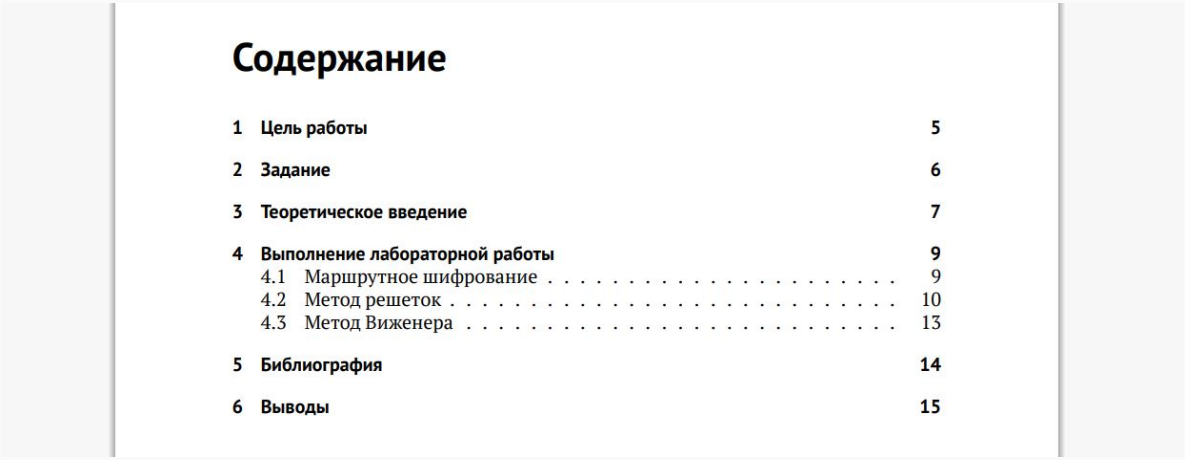
Дисциплина: Математические основы защиты информации и информационной безопасности

Студент: Румянцева Александра Сергеевна, 1132223493
Группа: НПМмд-02-22
Преподаватель: Кулябов Дмитрий Сергеевич,
д-р.ф.-м.н., проф.

Москва 2022

Figure 8: Рис. 8. Pdf файл. Титульный лист.

Рассмотрим пдф файл. Содержание.



Содержание

Figure 9: Рис. 9. Pdf файл. Содержание.

Наличие в пдф файле списков фигур и таблиц

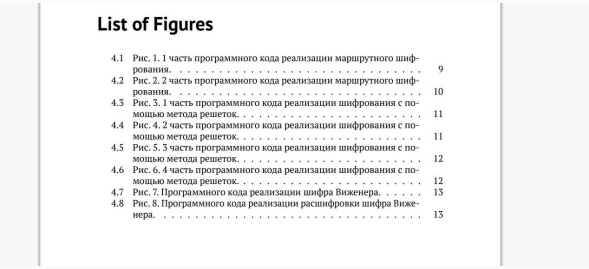


Figure 10: Рис. 10. Pdf файл. Список рисунков (фигур).

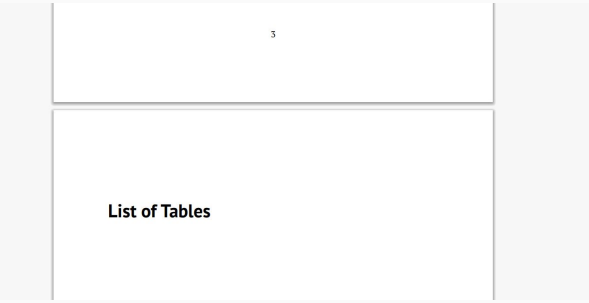
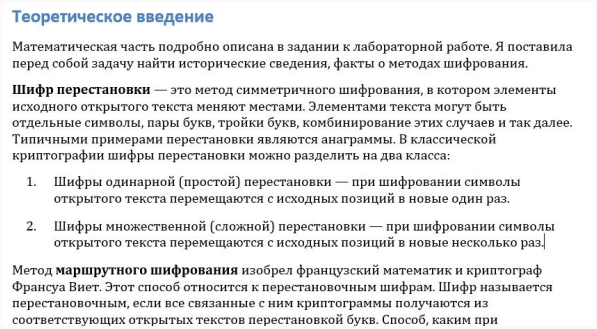


Figure 11: Рис. 11. Pdf файл. Список таблиц



Теоретическое введение

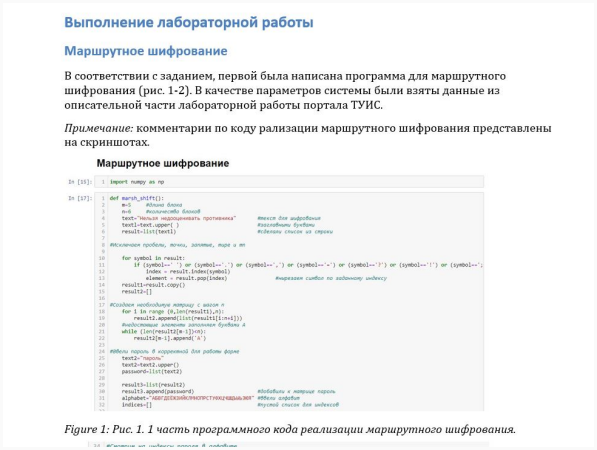
Математическая часть подробно описана в задании к лабораторной работе. Я поставила перед собой задачу найти исторические сведения, факты о методах шифрования.

Шифр перестановки — это метод симметричного шифрования, в котором элементы исходного открытого текста меняют местами. Элементами текста могут быть отдельные символы, пары букв, тройки букв, комбинирование этих случаев и так далее. Типичными примерами перестановки являются анаграммы. В классической криптографии шифры перестановки можно разделить на два класса:

1. Шифры одинарной (простой) перестановки — при шифровании символы открытого текста перемещаются с исходных позиций в новые один раз.
2. Шифры множественной (сложной) перестановки — при шифровании символы открытого текста перемещаются с исходных позиций в новые несколько раз.

Метод **маршрутного шифрования** изобрел французский математик и криптограф Франсуа Виет. Этот способ относится к перестановочным шифрам. Шифр называется перестановочным, если все связанные с ним криптограммы получаются из соответствующих открытых текстов перестановкой букв. Способ, каким при

Figure 12: Рис. 12. Docx файл. Заголовок главы, полужирный шрифт, пронумерованный список.



Выполнение лабораторной работы

Маршрутное шифрование

В соответствии с заданием, первой была написана программа для маршрутного шифрования (рис. 1-2). В качестве параметров системы были взяты данные из описательной части лабораторной работы портала ТУИС.

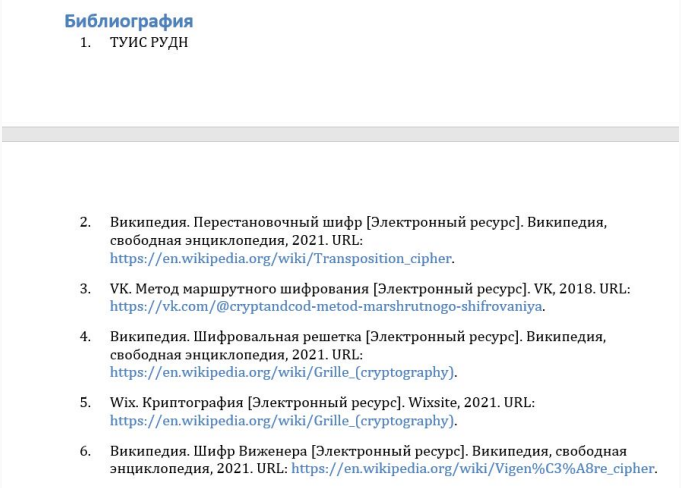
Примечание: комментарии по коду ралиазации маршрутного шифрования представлены на скриншотах.

Маршрутное шифрование

```
In [16]: import numpy as np

In [17]: def marsh_sh(ft):
             m=5     #длина блока
             n=6     #количество блоков
             text="Нельзя недооценивать противника"          #текст для шифровани
             text1=text.upper()                              #заглавные буквы
             result=list(text1)                              #делаем список из строки

         #исключаем пробелы, точки, запятые, тире и пт

             for symbol in result:
                 if (symbol==' ') or (symbol=='.') or (symbol==',') or (symbol=='-') or (symbol=='!') or (symbol=='!') or (symbol==':
                     index = result.index(symbol)
                     element = result.pop(index)             #выражаем символ по заданному индексу
             result1=result.copy()
             result2=[]

         #создаем необходимую матрицу с шагом n
             for i in range (0,len(result1),n):
                 result2.append(list(result1[i:n+i]))
             #print(result2)                                 #печатаем буквицу в
             while (len(result2[m-1])<n):
                 result2[m-1].append('A')

         #вводим пароль в корректной для работы форме
             text2="пароль"
             text2=text2.upper()
             password=list(text2)

             result3=list(result2)
             result3.append(password)                        #добавляем к матрице пароль
             alphabet="АБВГДЕЖЗИЙКЛМНОПРСТУФХЦЧШЩЬЫЭЮЯ"      #вводим алфавит
             indices=[]                                      #пустой список для индексов
```

Figure 1: Рис. 1. 1 часть программного кода реализации маршрутного шифрования.

Figure 13: Рис. 13. Docx файл. Заголовки разных уровней, курсивный шрифт, добавленный рисунок с подписью.



Библиография

1. ТУИС РУДН

2. Википедия. Перестановочный шифр [Электронный ресурс]. Википедия, свободная энциклопедия, 2021. URL: https://en.wikipedia.org/wiki/Transposition_cipher.
3. VK. Метод маршрутного шифрования [Электронный ресурс]. VK, 2018. URL: https://vk.com/@cryptandcod-metod-marshrutnogo-shifrovaniya.
4. Википедия. Шифровальная решетка [Электронный ресурс]. Википедия, свободная энциклопедия, 2021. URL: https://en.wikipedia.org/wiki/Grille_(cryptography).
5. Wix. Криптография [Электронный ресурс]. Wixsite, 2021. URL: https://en.wikipedia.org/wiki/Grille_(cryptography).
6. Википедия. Шифр Виженера [Электронный ресурс]. Википедия, свободная энциклопедия, 2021. URL: https://en.wikipedia.org/wiki/Vigen%C3%A8re_cipher.

Figure 14: Рис. 14. Docx файл. Активные ссылки в тексте.

Выводы

Я научилась оформлять отчёты с помощью легковесного языка разметки Markdown.