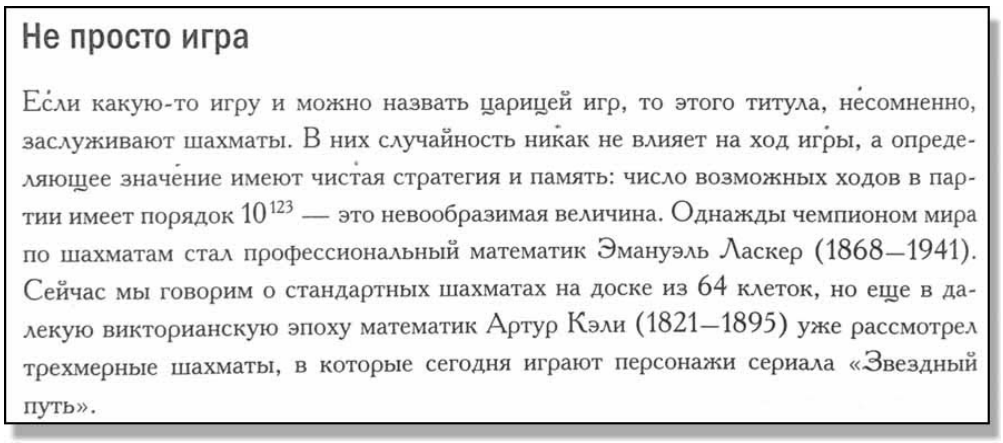
Practical work No. 1
Steganography

1. Description of the steganographic method.
2. Task for the implementation of practical work.

1. Description of the steganographic method

Steganographic methods, both independently and in conjunction with cryptography, have become widespread in order to protect confidential information. In practical work, steganographic hiding of secret messages in text documents of the Microsoft Word editor is considered due to the specific formatting of text characters. The principles of concealment are based on other known steganographic methods.

1. Microdots. The use of microdots to transmit secret messages was described by the Greek scientist Aeneas Tactics in his essay “On the Defense of Fortified Places”. The essence of the so-called "book cipher" proposed by him was to pierce inconspicuous holes in a book or in another document above the letters of a secret message. During the First World War, German spies used a similar cipher, replacing holes with dots, applied with sympathetic ink to the letters of newspaper text.



Не просто игра

Е́сли какую-то игру и можно назвать царицей игр, то этого титула, не́сомненно, заслуживают шахматы. В них случайность ни́как не влияет на ход игры́, а определяющее значе́ние имеют чи́стая стратегия и память: число возможных ходов в партии имеет порядок 10^{123} — это невообразимая величина. Однажды чемпионом мира по шахматам стал профессиональный математик Эмануэль Ласкер (1868–1941). Сейчас мы говорим о стандартных шахматах на доске из 64 клеток, но еще в далекую викторианскую эпоху математик Артур Кэли (1821–1895) уже рассмотрел трехмерные шахматы, в которые сегодня играют персонажи сериала «Звездный путь».

Fig.1. Hiding the message "secret" in the text due to inconspicuous dots
(Joaquin Navarro. The Secret Life of Numbers. The World of Mathematics - Volume 31)

By analogy with microdots, secret information hidden in the text is marked (formatted) in a special way.

2. Using the features of human vision. Such methods are widely used to hide information in multimedia files (in particular, the LSB method, Least Significant Bit - the least significant bit) due to their redundancy. By analogy with them, in ordinary text, the characters that make up the secret message can be formatted in such a way that it will not be noticeable to the eye of an inexperienced reader of the text. In particular, the symbols of the secret message can be highlighted in a different color, slightly different from the color of other symbols.

By analogy with microdots, secret information hidden in the text is marked (formatted) in a special way.

2. Using the features of human vision. Such methods are widely used to hide information in multimedia files (in particular, the LSB method, Least Significant Bit - the least significant bit) due to their redundancy. By analogy with them, in ordinary text, the characters that make up the secret message can be formatted in such a way that it will not be noticeable to the eye of an inexperienced reader of the text. In particular, the symbols of the secret message can be highlighted in a different color, slightly different from the color of other symbols.

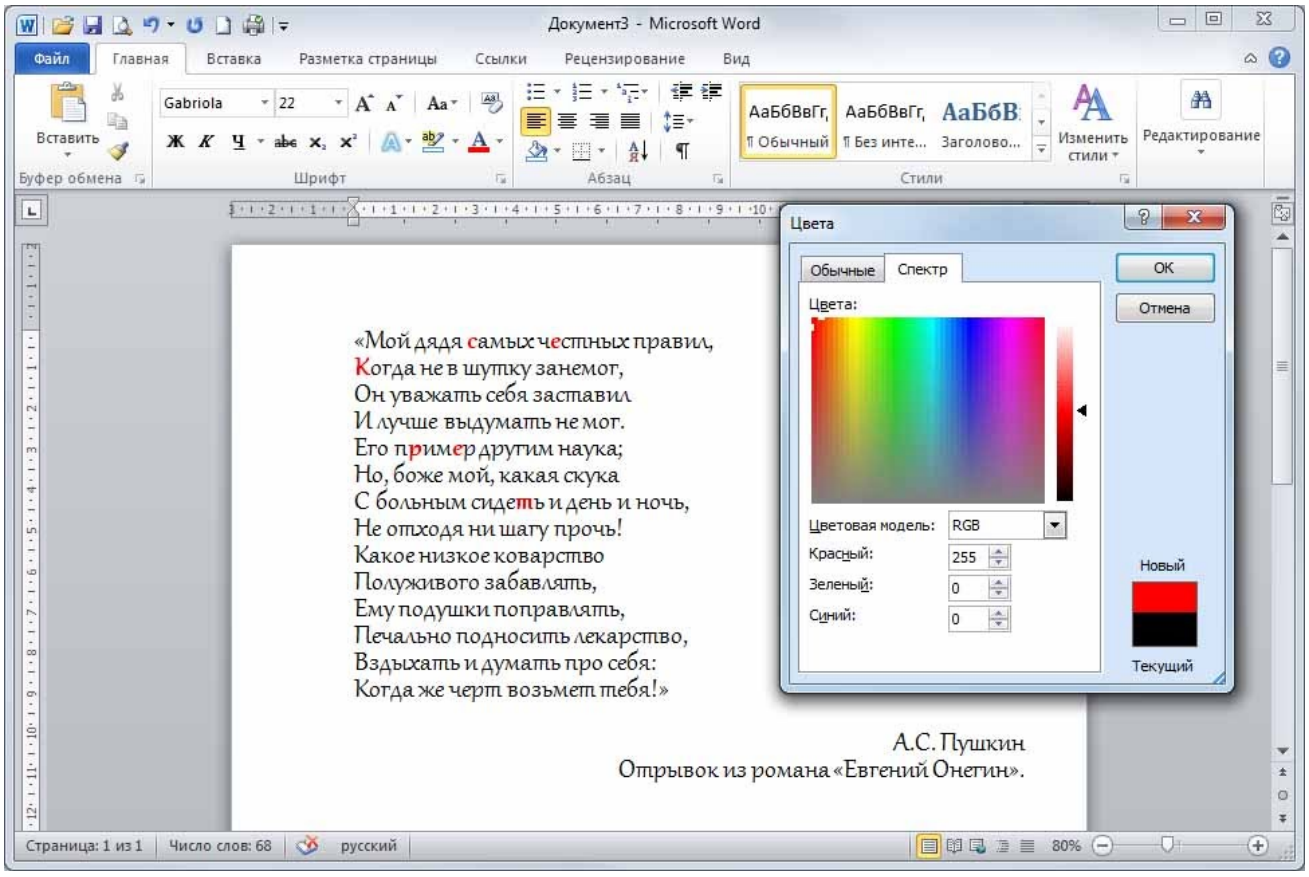


Fig.2. The principle of formatting the characters of the secret message "secret" (character color is red - RGB(255, 0, 0))

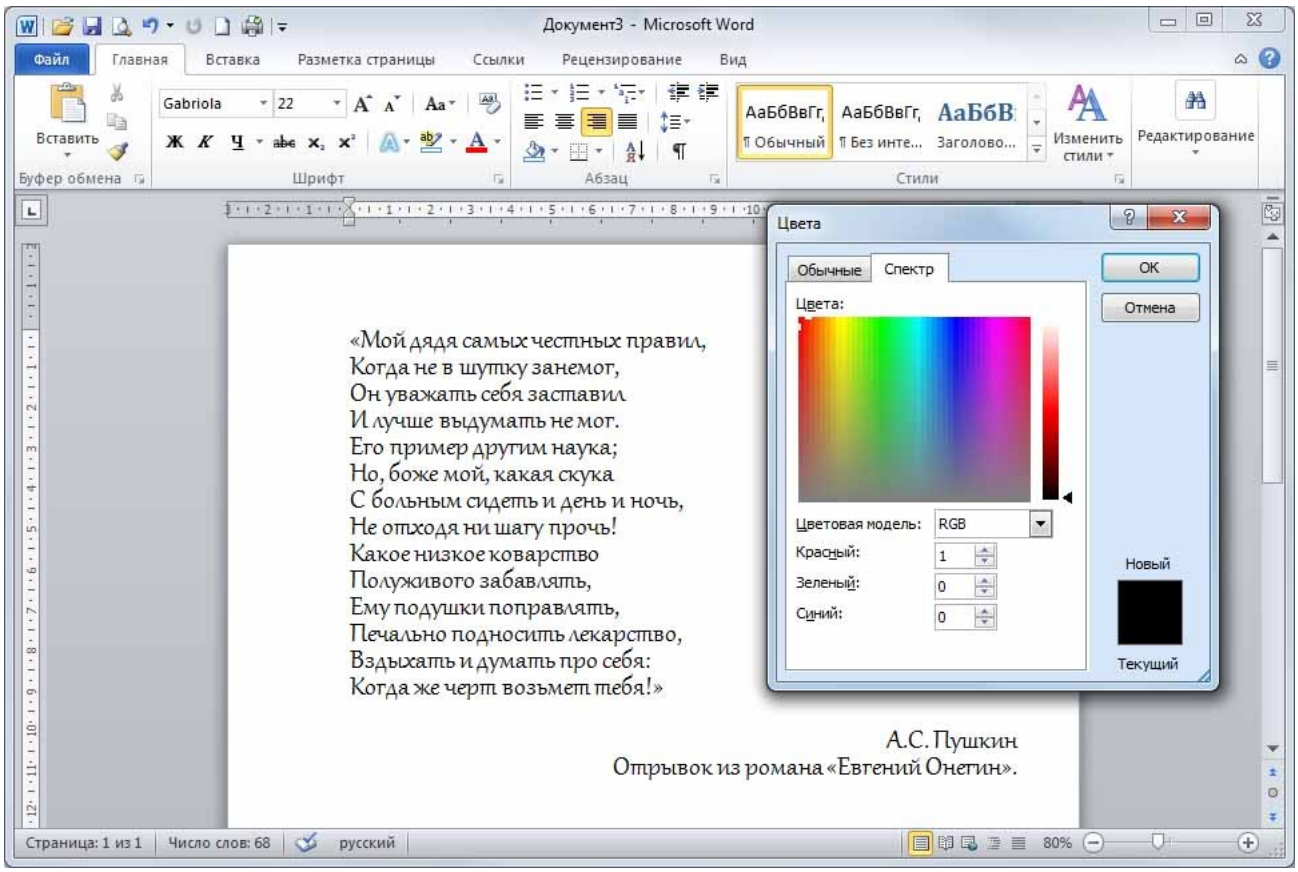


Fig.3. Steganographic hiding of secret message characters "secret"
(character color is "almost black" - RGB(1, 0, 0))

In Fig. 3, the color of the symbols of the secret message RGB(1, 0, 0) practically does not differ from the color of the symbols of the rest of the RGB(0, 0, 0) text.

3. Coding. The previous method can be enhanced by using pre-encoded secret message characters (eg Morse code or Windows 1251). Before formatting, the symbols of the secret message are first encoded with bit strings of length n according to the accepted encoding. In the source text, the first n characters are selected, which will correspond to the bit representation of the first character of the secret message. For zeros of the bit string, the original formatting is left, for ones, they are slightly changed (see Fig. 3). The procedure is repeated sequentially for the remaining symbols of the secret message. For example, the word "secret" according to Windows encoding 1251 in bit representation will look like 11110001 11100101 11101010 11110000 11100101 11110010_2.

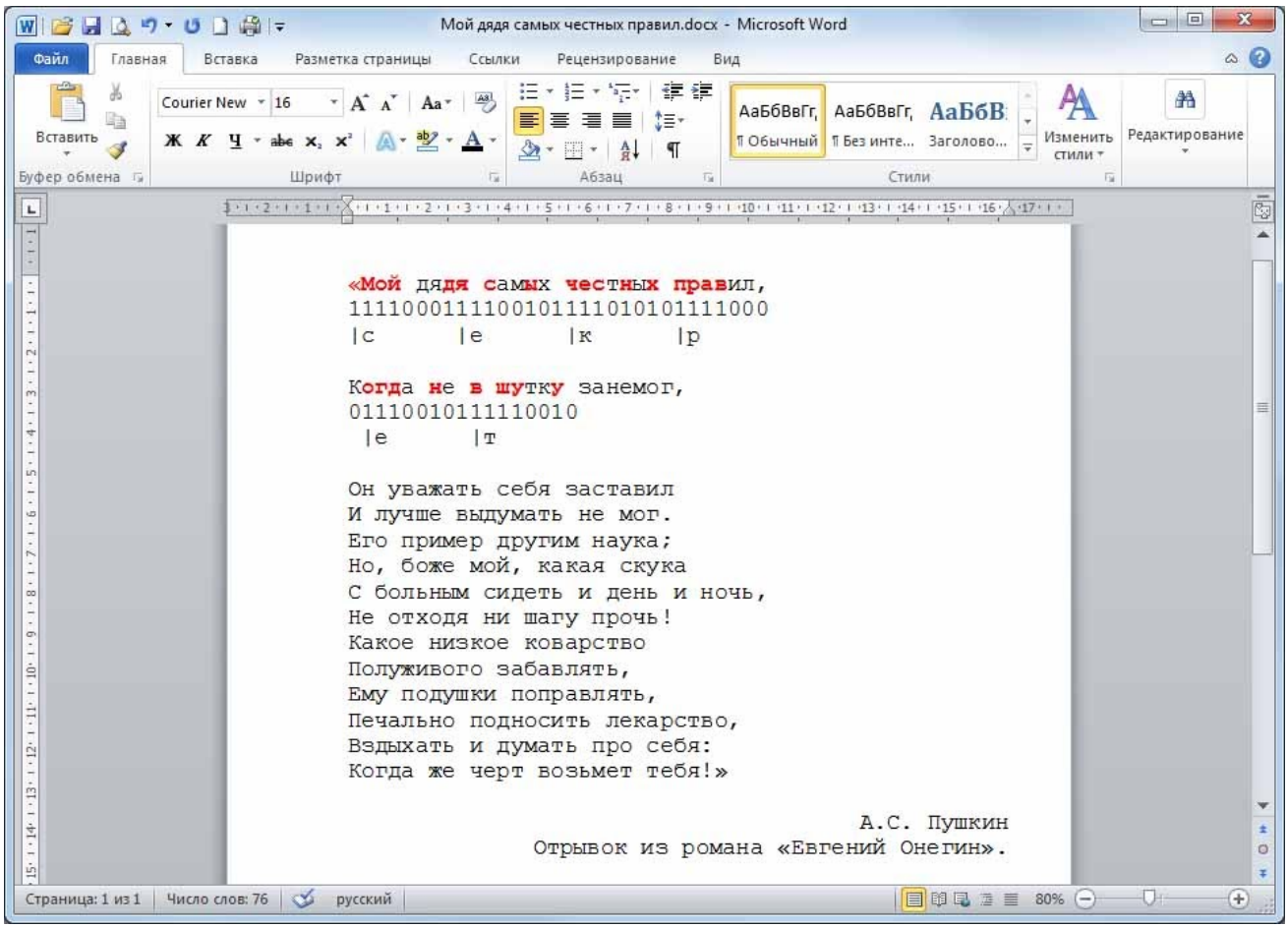


Fig.4.

The principle of encoding and formatting the symbols of the secret message "secret" (the color of zeros is black - RGB(0, 0, 0); the color of units is red - RGB(255, 0, 0))

2. Task for the implementation of practical work

1) For a given file, it is necessary to write a program for determining a hidden message, determine the encoding and the method used for its steganographic concealment.

(programmatically implement all methods of steganographic hiding and all encodings presented)

2) Character formatting methods used for secret messages (whole characters, zeros or ones):

- color of symbols;
- background color;
- font size;
- font scale;
- intercharacter interval.

3) Used binary character encodings:

- Baudot code (MTK-2);
- KOI-8R;
- cp866;
- Windows 1251.

4) individual tasks

1. variant01.docx;
2. variant02.docx;
3. variant03.docx;
4. variant04.docx;
5. variant05.docx;
6. variant06.docx;
7. variant07.docx;
8. variant08.docx;
9. variant09.docx;
10. variant10.docx;
11. variant11.docx;
12. variant12.docx;
13. variant13.docx;
14. variant14.docx;
15. variant15.docx;
16. variant16.docx;
17. variant17.docx;
18. variant18.docx;
19. variant19.docx;
20. variant20.docx;
21. variant21.docx;
22. variant22.docx;
23. variant23.docx;
24. variant24.docx;
25. variant25.docx.

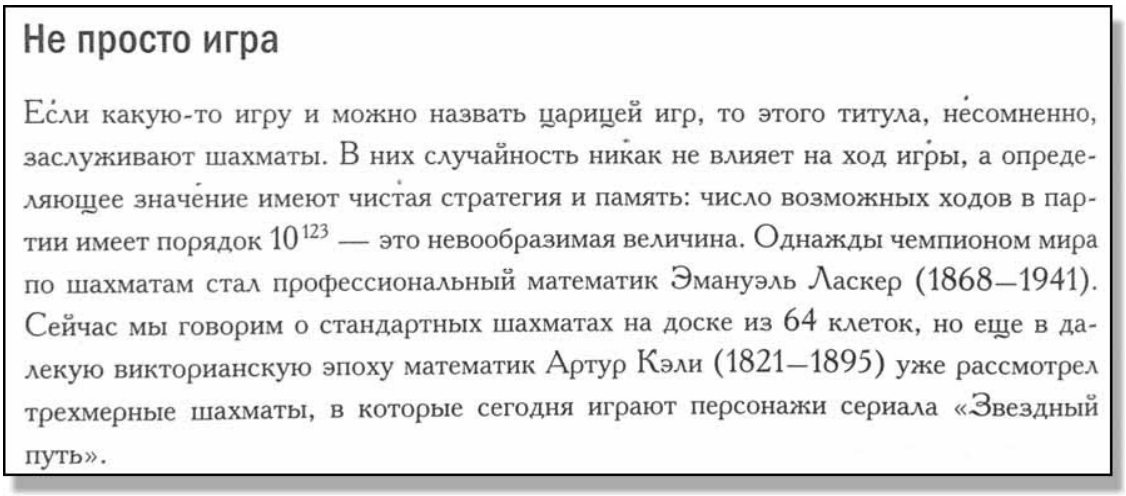
Практическая работа №1
Стеганография

1. Описание стеганографического метода.
2. Задание на выполнение практической работы.

1. Описание стеганографического метода

Стеганографические методы как самостоятельно, так и совместно с криптографией, получили широкое распространение в целях защиты конфиденциальной информации. В практической работе рассматривается стеганографическое сокрытие секретных сообщений в текстовых документах редактора Microsoft Word за счет специфического форматирования символов текста. Принципы сокрытия базируются на других известных стеганографических методах.

1. Микроточки. Использование микроточек для передачи секретных сообщений описал греческий ученый Эней Тактик в сочинении «Об обороне укреплённых мест». Суть предложенного им так называемого «книжного шифра» заключалась в прокалывании малозаметные дырок в книге или в другом документе над буквами секретного сообщения. Во время Первой мировой войны германские шпионы использовали аналогичный шифр, заменив дырки на точки, наносимые симпатическими чернилами на буквы газетного текста.



Не просто игра

Е́сли какую-то игру и можно назвать царицей игр, то этого титула, не́сомненно, заслуживают шахматы. В них случайность ни́как не влияет на ход игры́, а определяющее значе́ние имеют чиста́я стратегия и память: число возможных ходов в партии имеет порядок 10^{123} — это невообразимая величина. Однажды чемпионом мира по шахматам стал профессиональный математик Эмануэль Ласкер (1868–1941). Сейчас мы говорим о стандартных шахматах на доске из 64 клеток, но еще в далекую викторианскую эпоху математик Артур Кэли (1821–1895) уже рассмотрел трехмерные шахматы, в которые сегодня играют персонажи сериала «Звездный путь».

Рис.1. Сокрытие сообщения «секрет» в тексте за счет малозаметных точек
(Хоакин Наварро. Тайная жизнь чисел. Мир математики – том 31)

По аналогии с микроточками скрываемая в тексте секретная информация специальным образом помечается (форматируется).

2. Использование особенностей человеческого зрения. Подобные методы широко используются для сокрытия информации в мультимедийных файлах (в частности, метод LSB, Least Significant Bit - наименьший значащий бит) за счет их избыточности. По аналогии с ними, в обычном тексте символы, составляющие секретное сообщение, могут форматируются так, что это будет незаметно для глаза неискушенного читателя текста. В частности, символы

секретного сообщения могут выделяться другим цветом, незначительно отличающегося от цвета остальных символов.

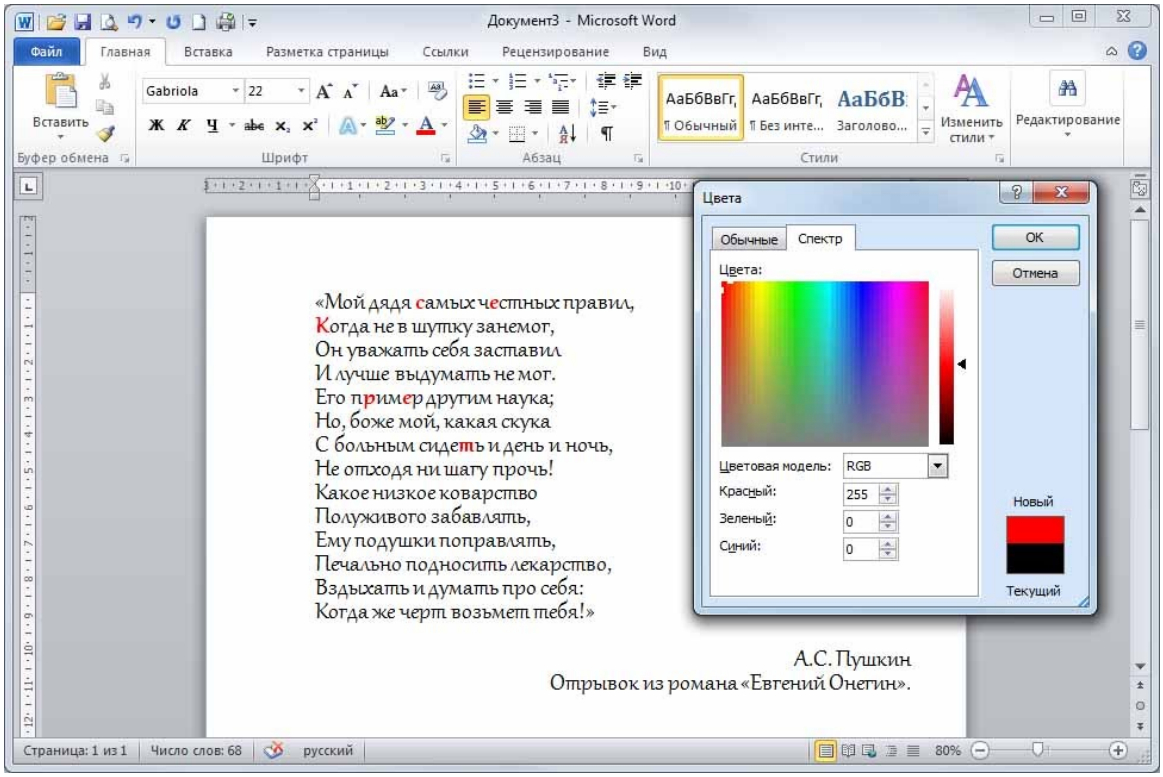


Рис.2. Принцип форматирования символов секретного сообщения «секрет» (цвет символов красный – RGB(255, 0, 0))

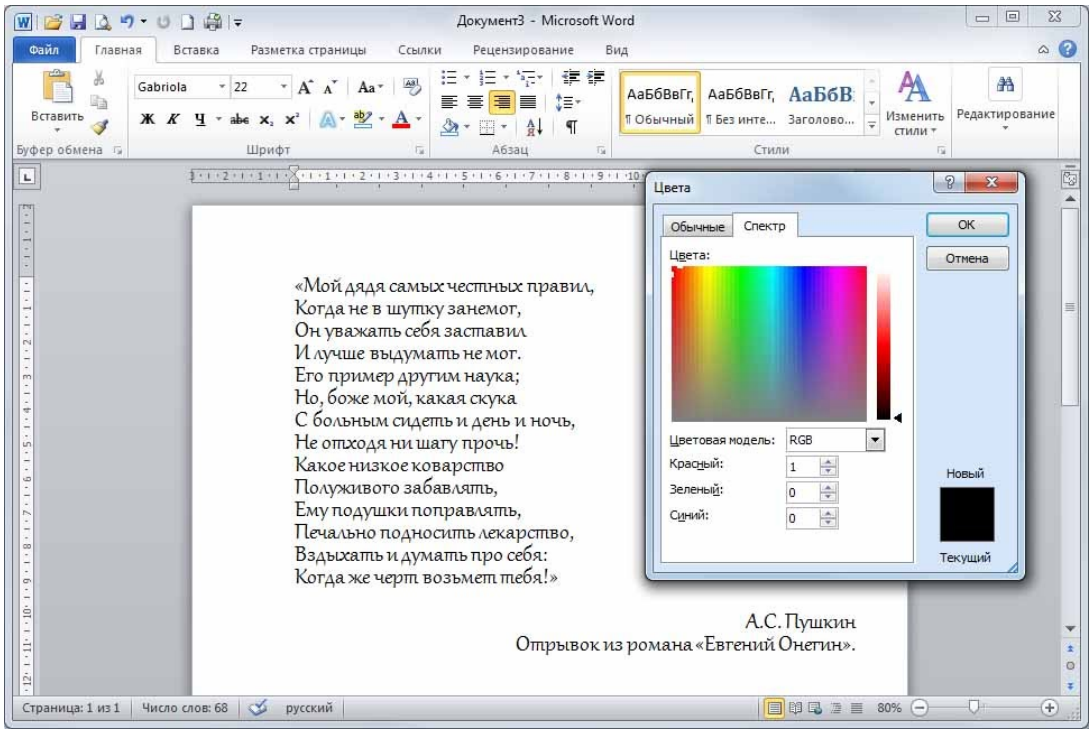


Рис.3. Стеганографическое сокрытие символов секретного сообщения «секрет» (цвет символов «почти черный» – RGB(1, 0, 0))

На рис.3 цвет символов секретного сообщения RGB(1, 0, 0) практически не отличается от цвета символов остального текста RGB(0, 0, 0).

3. Кодирование. Предыдущий метод можно усилить за счет использования предварительного кодирования символов секретного сообщения (например, азбукой Морзе или Windows 1251). Перед форматированием символы секретного сообщения вначале кодируются битовыми строками длиной n согласно принятой кодировке. В исходном тексте выбираются n первых символов, которые будут соответствовать битовому представлению первого символа секретного сообщения. Для нулей битовой строки оставляют исходное форматирование, для единиц – незначительно меняют (см. рис. 3). Процедуру последовательно повторяют для оставшихся символов секретного сообщения. Например, слово «секрет» согласно кодировке Windows 1251 в битовом представлении будет выглядеть $11110001\ 11100101\ 11101010\ 11110000\ 11100101\ 11110010_2$.

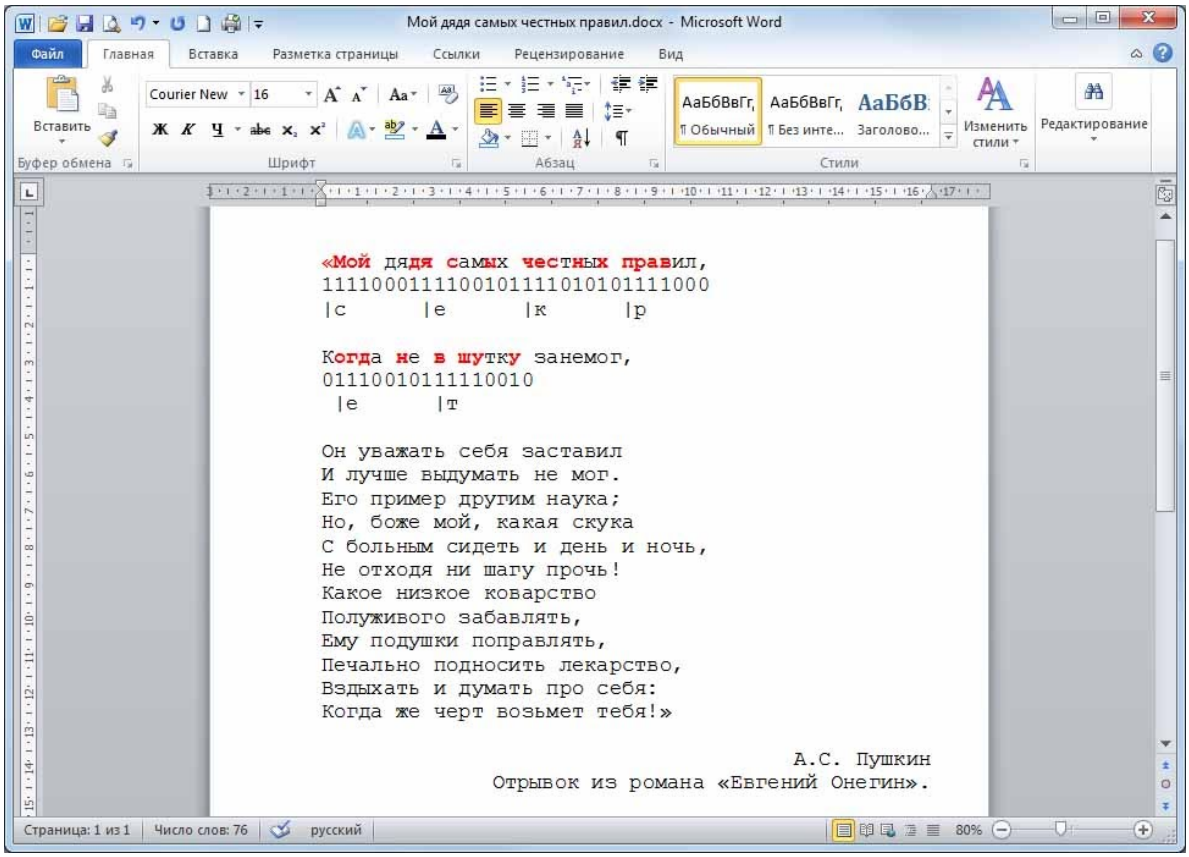


Рис.4.

Принцип кодирования и форматирования символов секретного сообщения «секрет» (цвет нулей черный – RGB(0, 0, 0); цвет единиц красный – RGB(255, 0, 0))

2. Задание на выполнение практической работы

1) Для заданного файла необходимо написать программу определения скрытого сообщения, определить кодировку и используемый метод его стеганографического сокрытия.

(реализовать программно **все** методы стеганографического сокрытия и **все** представленные кодировки)

2) Способы форматирования символов, применяемые для секретных сообщений (символов целиком, нулей или единиц):

- цвет символов;
- цвет фона;
- размер шрифта;
- масштаб шрифта;
- межсимвольный интервал.

3) Применяемые двоичные кодировки символов:

- код Бодо (МТК-2);
- КОИ-8R;
- ср866;
- Windows 1251.

4) Варианты индивидуальных заданий (выбираются согласно номеру в журнале):

1. variant01.docx;
2. variant02.docx;
3. variant03.docx;
4. variant04.docx;
5. variant05.docx;
6. variant06.docx;
7. variant07.docx;
8. variant08.docx;
9. variant09.docx;
10. variant10.docx;
11. variant11.docx;
12. variant12.docx;
13. variant13.docx;
14. variant14.docx;
15. variant15.docx;
16. variant16.docx;
17. variant17.docx;
18. variant18.docx;
19. variant19.docx;
20. variant20.docx;
21. variant21.docx;
22. variant22.docx;
23. variant23.docx;
24. variant24.docx;
25. variant25.docx.

В качестве текстов использованы стихи Агния Барто, секретных сообщений – японские пословицы и поговорки. Файлы с заданиями сформированы с помощью программы

5) Отчет по практической работе должен содержать:

- цель работы;
- фрагмент стиха, содержащий секретное сообщение (см. рис.4);
- с подчеркиванием символов, соответствующих единицам (вместо выделения красным цветом);
- с битовыми строками;
- с символами секретного сообщения;
- вывод

(например, «В файле «variant01.docx», скрыта фраза «Один бог забыл - другой поможет.» посредством использования кодировки ср866 и размера символов: для нулей – 14пт, для единиц – 14.5пт»).