**Практическая работа №1**

**Стеганография**

Цель работы, рассмотреть виды сокрытия информации, реализовать программное средство определения скрытого сообщения, встроенного в текст, определения кодировки с использованием метода стеганографического сокрытия.

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.

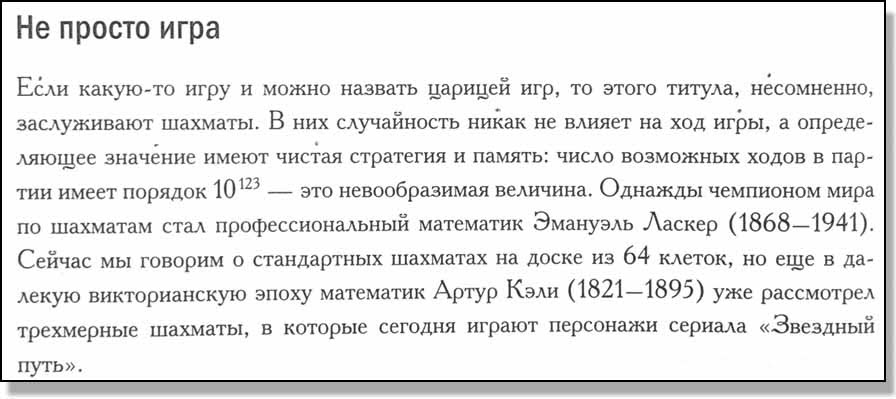


Рис.1. Сокрытие сообщения «секрет» в тексте за счет малозаметных точек  
(Хоакин Наварро. Тайная жизнь чисел. Мир математики – том 31)

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.

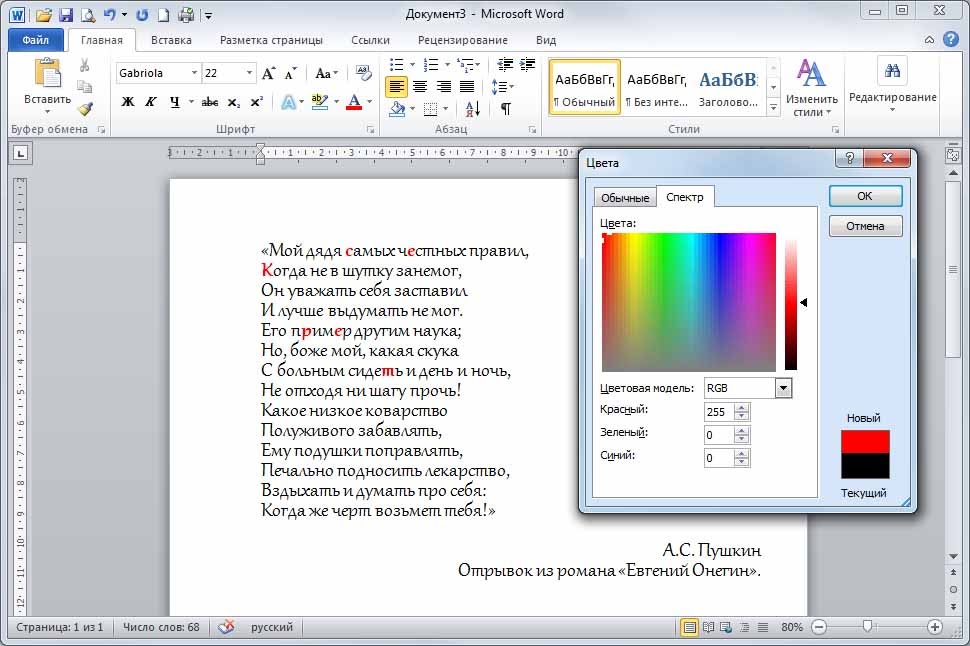


Рис.2. Принцип форматирования символов секретного сообщения «секрет»  
(цвет символов красный – RGB(255, 0, 0))

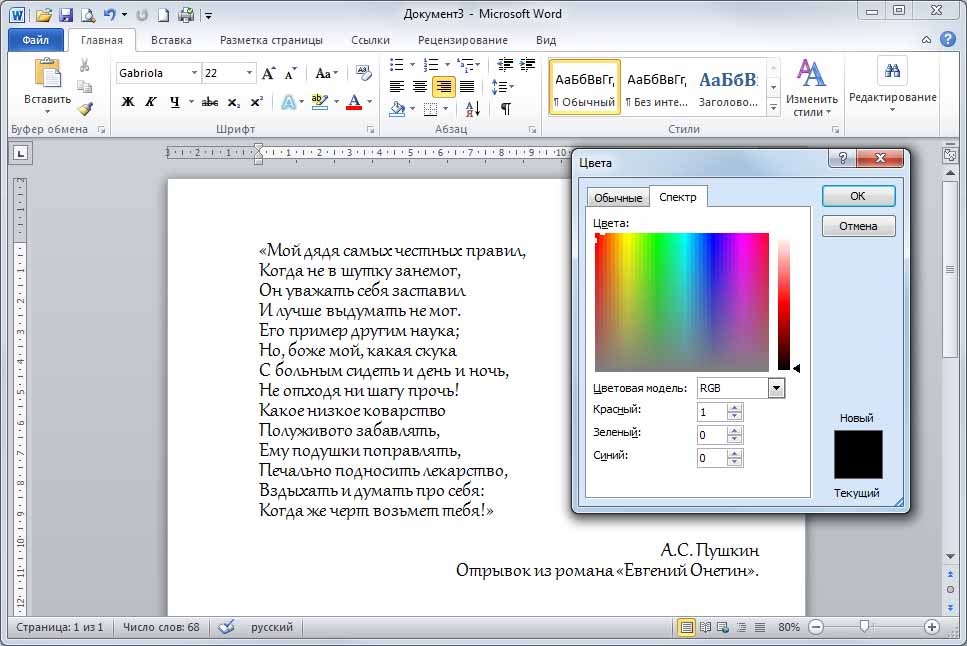


Рис.3. Стеганографическое сокрытие символов секретного сообщения «секрет»  
(цвет символов «почти черный» – RGB(1, 0, 0))

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](https://sites.google.com/site/anisimovkhv/learning/kripto/lecture/tema20#unicode)). 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](https://sites.google.com/site/anisimovkhv/learning/kripto/lecture/tema20#unicode) в битовом представлении будет выглядеть 11110001 11100101 11101010 11110000 11100101 111100102.

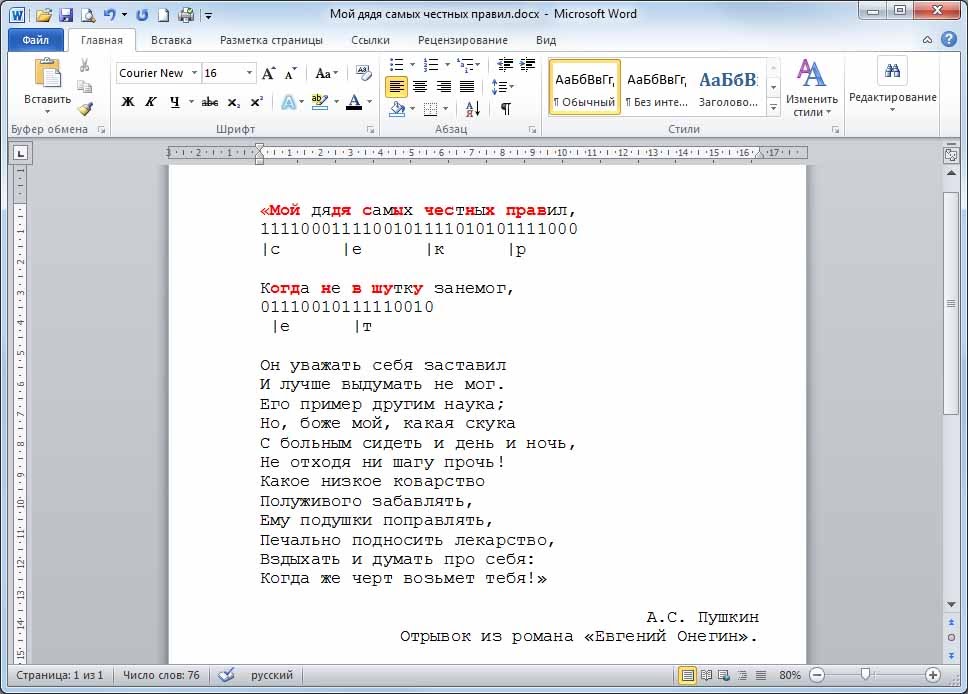


Рис.4. Принцип кодирования и форматирования символов секретного сообщения «секрет»  
(цвет нулей черный – RGB(0, 0, 0); цвет единиц красный – RGB(255, 0, 0))

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)](https://sites.google.com/site/anisimovkhv/learning/kripto/lecture/tema20#bodo);

- КОИ-8R;

- cp866;

- [Windows 1251](https://sites.google.com/site/anisimovkhv/learning/kripto/lecture/tema20#unicode).

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

1. [variant01.docx](https://docs.google.com/document/d/1L_JcES4dj_qab3U6SBWUbT-40DWeSYHu/view?usp=sharing);

2. [variant02.docx](https://docs.google.com/document/d/10z90o65QGfHMPxP-sJDJvD-osujkHln6/view?usp=sharing);

3. [variant03.docx](https://docs.google.com/document/d/1l3wWDMntByVZGYONdyYKEf62VecYniaQ/view?usp=sharing);

4. [variant04.docx](https://docs.google.com/document/d/1lqbw1HSXibCmO09GPdoG2wdvTzRA4W4c/view?usp=sharing);

5. [variant05.docx](https://docs.google.com/document/d/1G9NeNG6VIfnm1qOeWMj3qBHZ9wCo79OW/view?usp=sharing);

6. [variant06.docx](https://docs.google.com/document/d/1XhDV80YaoMi28k9m8AvEUIF-M8PCMzdg/view?usp=sharing);

7. [variant07.docx](https://docs.google.com/document/d/1KsaCG5NoJE2k-o7qTtS0D1t0hj-VeenO/view?usp=sharing);

8. [variant08.docx](https://docs.google.com/document/d/1w4s7QqesuOgxCbOXd7GukYvm4jw789xF/view?usp=sharing);

9. [variant09.docx](https://docs.google.com/document/d/1Gles2Df9wbwNKSRA8MT2eO4xvQvTlc4-/view?usp=sharing);

10. [variant10.docx](https://docs.google.com/document/d/1wEXL4HKcn8w8IrHQyYQrLek0NsRg1pJy/view?usp=sharing);

11. [variant11.docx](https://docs.google.com/document/d/1eS8Mg6lRY1ziAhO0b2XiDt-NwSgFWJ3r/view?usp=sharing);

12. [variant12.docx](https://docs.google.com/document/d/1XutEBsnemh7apJySEMGL4acBVnDBivAZ/view?usp=sharing);

13. [variant13.docx](https://docs.google.com/document/d/1DZhoISTOEhu367JTL3B7V9s6pdfBL3TA/view?usp=sharing);

14. [variant14.docx](https://docs.google.com/document/d/1oFmWiAWTgWftr7TAfJCnQqqmFidoOQSP/view?usp=sharing);

15. [variant15.docx](https://docs.google.com/document/d/1R_5znOMXVYYCWIEnujCgUAc0Ls_Z_EjV/view?usp=sharing);

16. [variant16.docx](https://docs.google.com/document/d/1othqNa3E9LLKjPIJEdD6DfNoLvw_D0jb/view?usp=sharing);

17. [variant17.docx](https://docs.google.com/document/d/1GkVO98GjmbR-7n8qMZ7y4K1eRvpanqZy/view?usp=sharing);

18. [variant18.docx](https://docs.google.com/document/d/1yZHF_IGpDQvuQuAceRNTfRiOYxOxiHnz/view?usp=sharing);

19. [variant19.docx](https://docs.google.com/document/d/1Icb2udI1qRUhwtzOkg7Xdxrad5sJWeRZ/view?usp=sharing);

20. [variant20.docx](https://docs.google.com/document/d/1dtlsTQuLQNk8PxXTUscat1bey3gfqzmi/view?usp=sharing);

21. [variant21.docx](https://docs.google.com/document/d/1kI9mX0BEhJnZLsUn5d16RgOsxvoTVLgn/view?usp=sharing);

22. [variant22.docx](https://docs.google.com/document/d/1d4w7QZYPq1yZEiKtiI9VWYOzvIXP0r37/view?usp=sharing);

23. [variant23.docx](https://docs.google.com/document/d/1aE2jPR2PCPoLYfUX-d7cVu_3Fh0BT0q3/view?usp=sharing);

24. [variant24.docx](https://docs.google.com/document/d/1uRjDUkW3klRgMN0MXHpXQUV8A_JlRMuw/view?usp=sharing);

25. [variant25.docx](https://docs.google.com/document/d/1uDS_mk4Fnuko0KNi3wbkrCCd8VrPPMpO/view?usp=sharing).

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 cp866 и размера символов: для нулей – 14пт, для единиц – 14.5пт»).