Учреждение образования

«БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

**Исследование методов**

**текстовой стеганографии**

Студент: Буданова К. А.

ФИТ 3 курс 5 группа

Преподаватель:

Савельева Маргарита Геннадьевна

1. **Цель работы**

Изучение стеганографических методов встраивания/извлечения тайной информации с использованием электронного файла-контейнера текстового формата, приобретение практических навыков программной реализации методов

1. **Задания**

Разработать авторское приложение, реализующее один из методов текстовой стеганографии на основе модификации пространственно-геометрических параметров текста-контейнера. Варианты заданий приведены в таблице. Дополнительные параметры согласуются с преподавателем.

1. **Ход работы**

В соответствии с вариантом, необходимо было реализовать метод для модификации кёрнинга. Под кернингом обычно понимается процесс изменения межсимвольного расстояние между отдельными парами символов или кёрнинговыми парами (именно фактор парности отличает кернинг от апроша). В текстовых документах встречаются такие сочетания знаков, которые образовывают визуальные «дыры» либо «сгущения». Например, в текстах на основе кириллицы – это такие сочетания: «ГА», «TA», «ATA», «ЬТ» и т. п., на основе латиницы – «AY», «AV», «T», «ff», а на основе греческого алфавита – «ΘΑ», «ΔΟ», «λκ» и др. Такие сочетания называются кёрнинговыми парами.

Для реализации метода модификации кёрнинга был разработан метод ApplyKerning, который изменяет расстояние между буквами. Он представлен на рисунке 3.1.

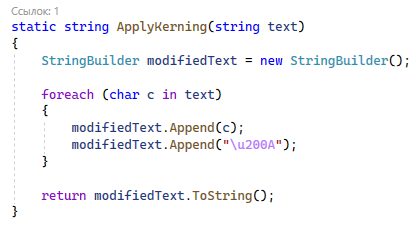


Рисунок 3.1 – Метод ApplyKerning

А метод, который использует ApplyKerning для сокрытия сообщения в тексте-контейнере, представлен на рисунке 3.2.

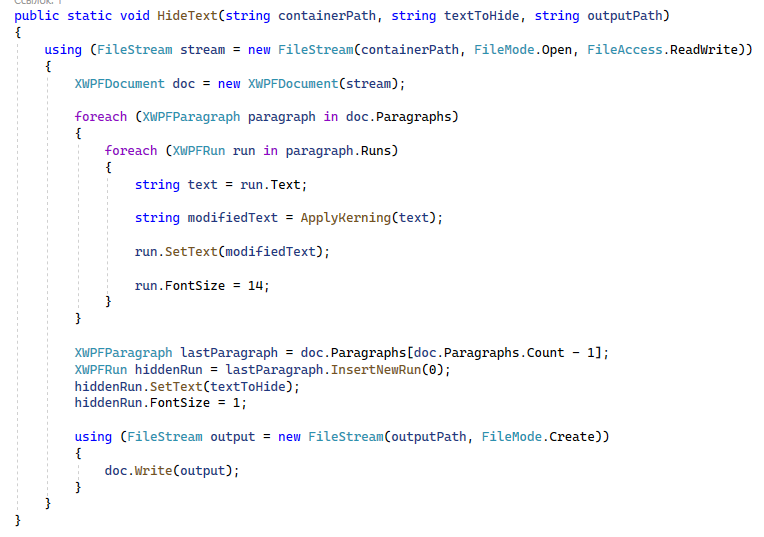


Рисунок 3.2 – Метод HideText

Для извлечения текста из контейнера есть обратный метод ExtractText, представленный на рисунке 3.3.

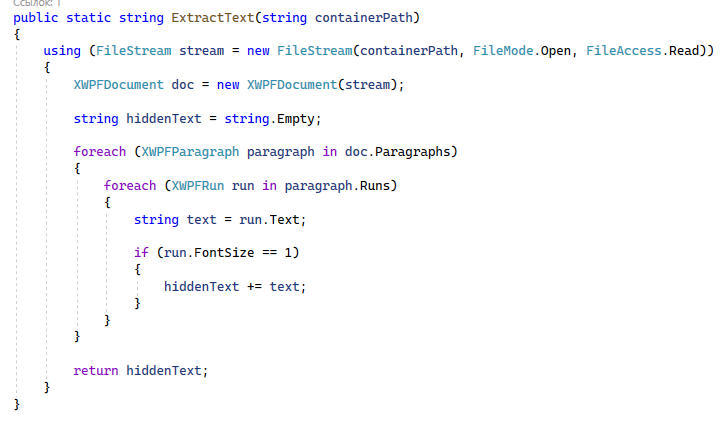


Рисунок 3.3 – Метод ExtractText

Посмотрим на результаты работы всех этих методов. После модификации текста с помощью метода на основе кёрнинга, документ сохраняется в отдельном файле. Примеры исходного и изменённого файла представлены на рисунках 3.4 – 3.5.

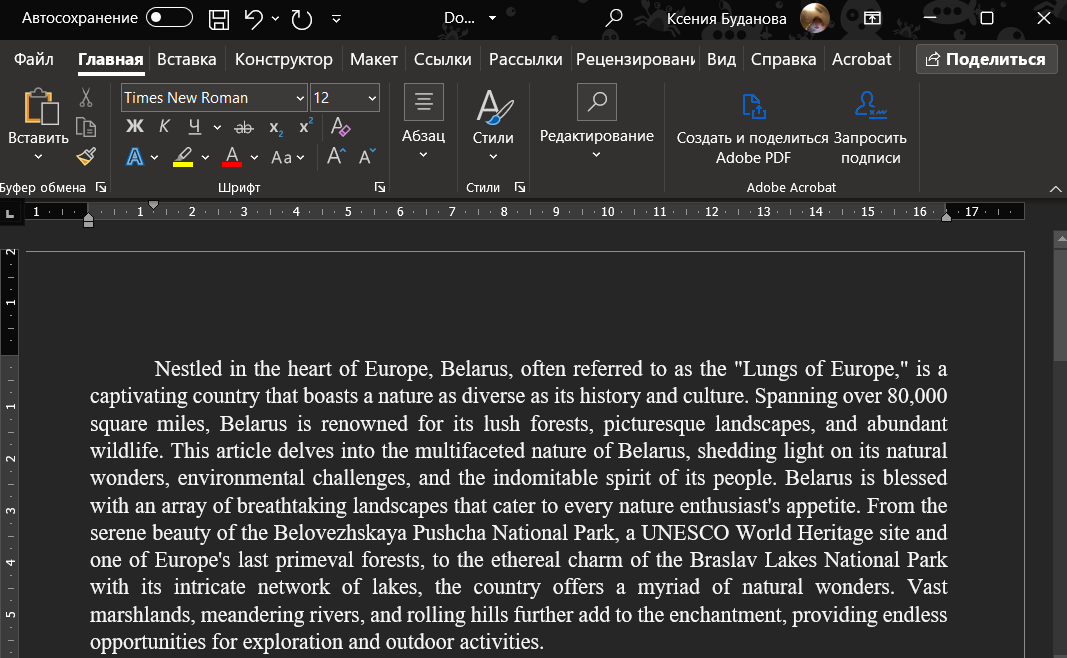


Рисунок 3.4 – Исходный документ

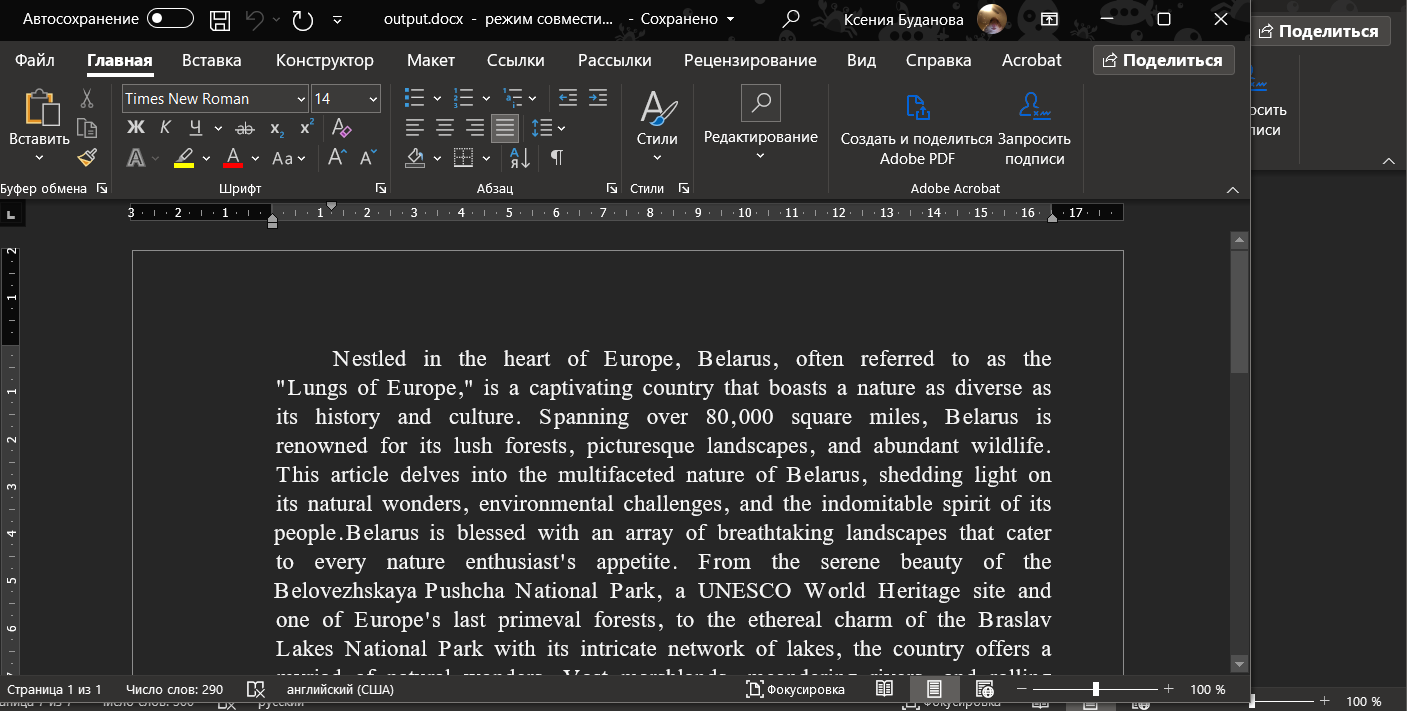


Рисунок 3.5 – Изменённый документ

Рассмотрим программное средство Sword. Оно представлено на рисунке 3.6. Рассмотрим процесс осаждения выбранного нами текста в файл.

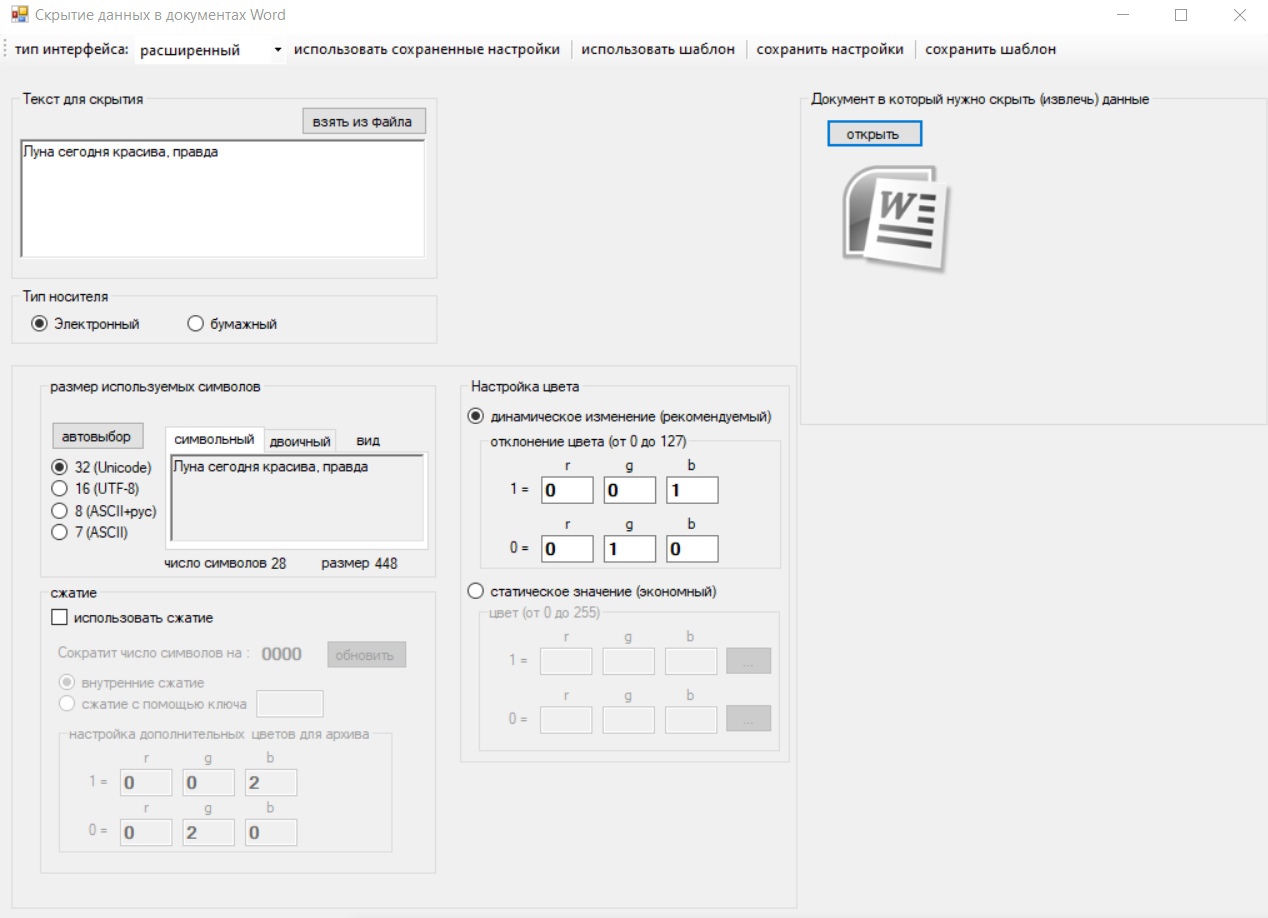


Рис. 3.6 – Приложение Sword, выбираем документ-контейнер

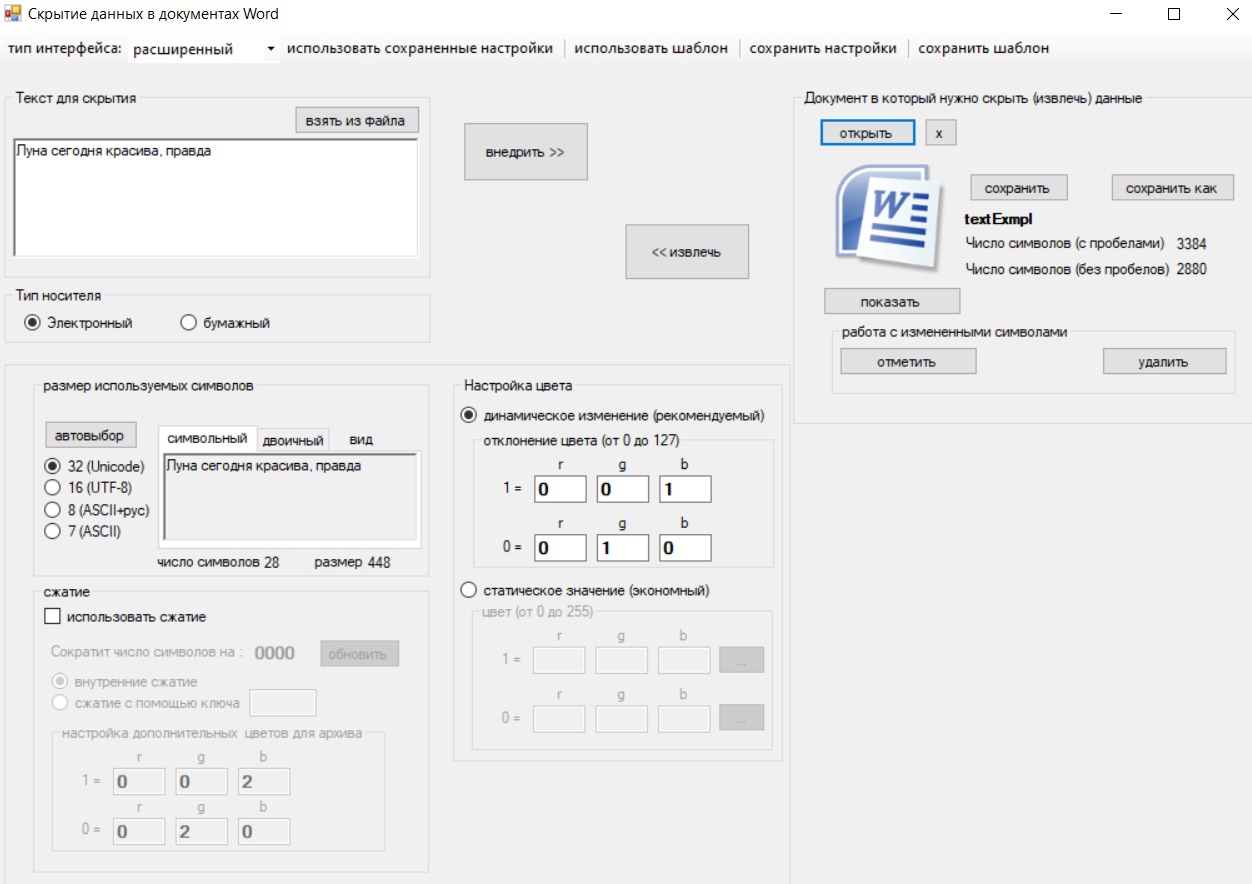


Рис. 3.7 – Выбираем текст-контейнер

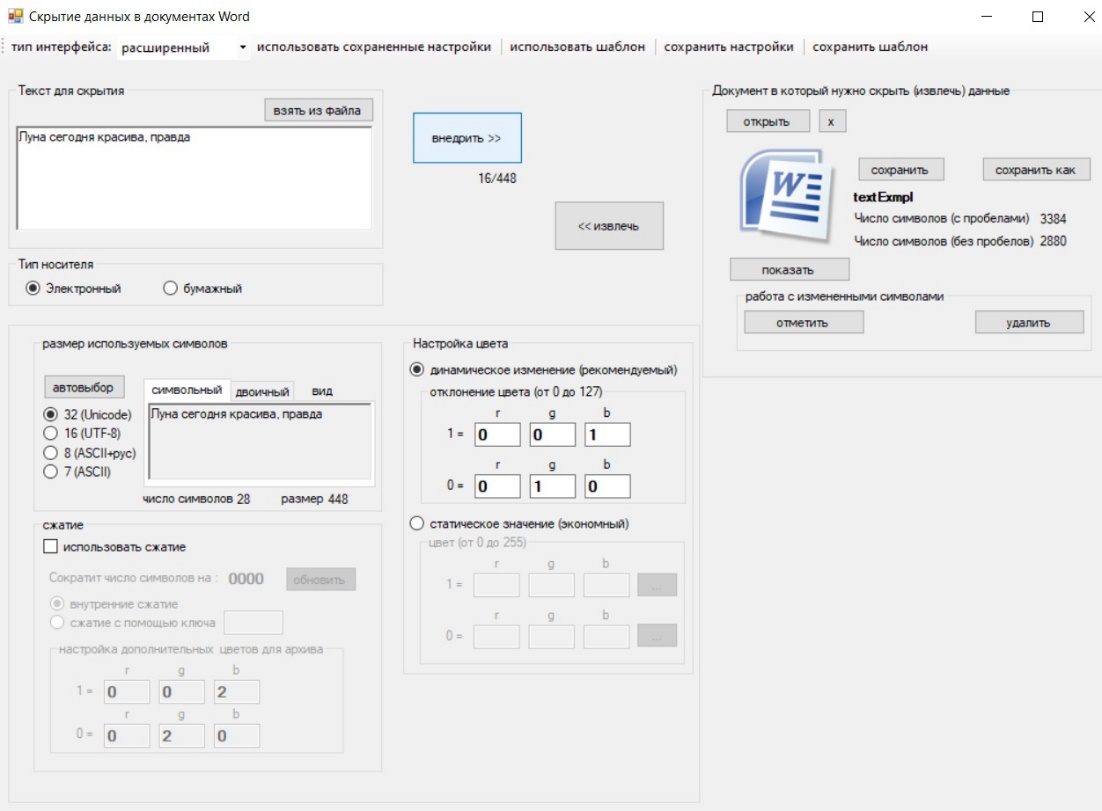


Рис. 3.8 – Внедряем сообщение в контейнер

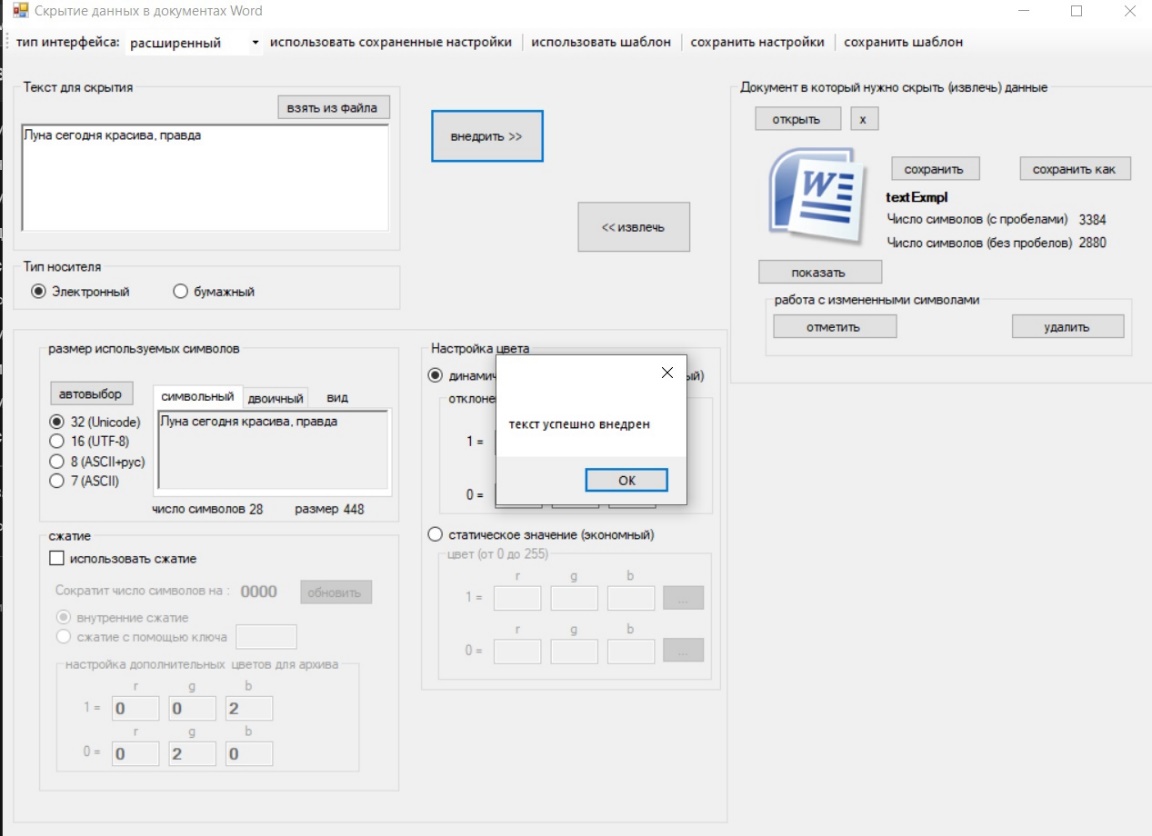


Рис. 3.9 – Сообщение об успешном внедрении

Сообщение было осаждено. Далее, извлечём скрытое сообщение из текста-контейнера. Результаты представлены на рисунках 3.9 – 3.10.

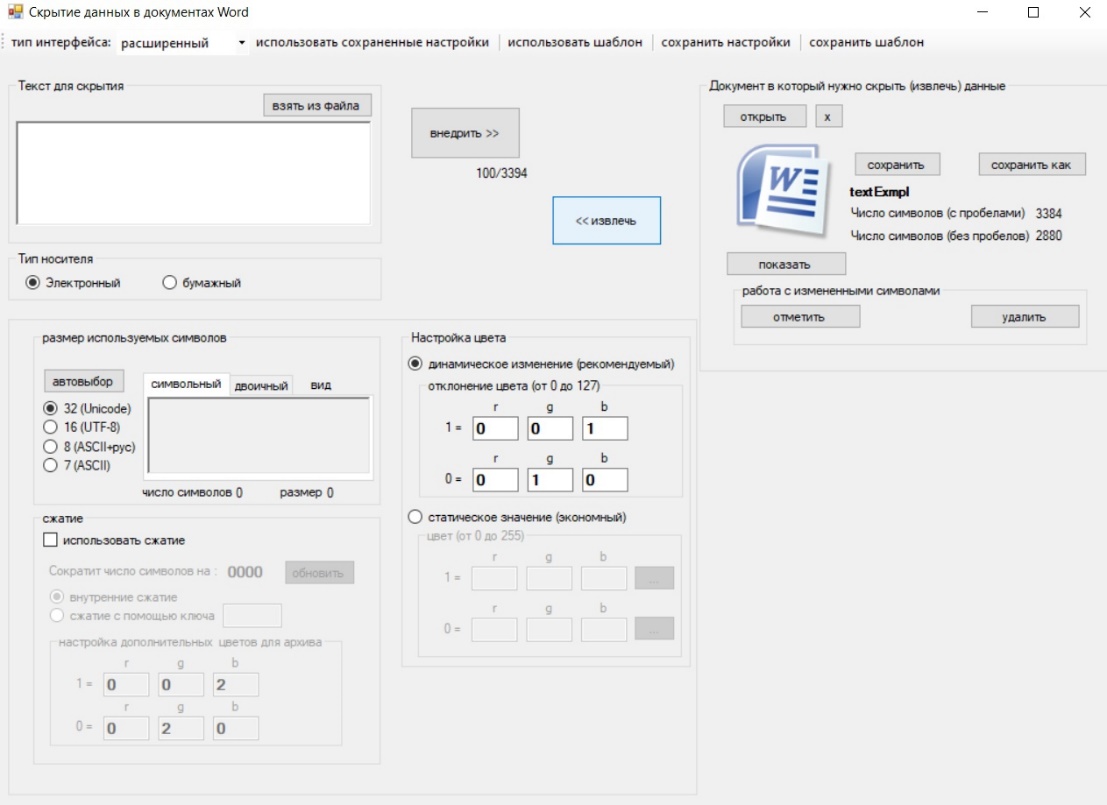


Рис. 3.8 – Извлечение сообщения из контейнера

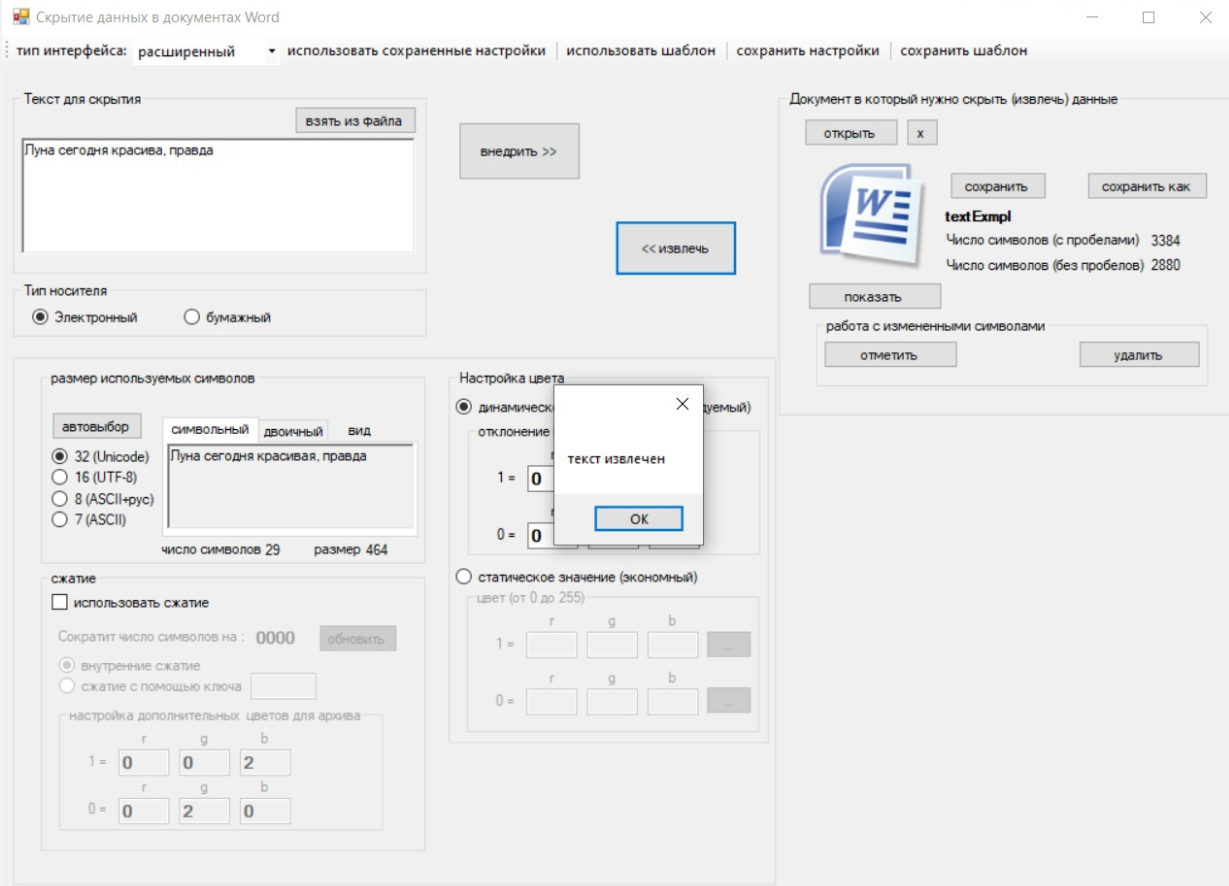


Рис. 3.9 – Извлечённое сообщение

**Вывод**

В ходе лабораторной работы были приобретены практические навыки программной реализации стеганографического метода осаждения/извлечения тайной информации с использованием текстовой стеганографии.

Также было разработано авторское приложение в соответствии с целью лабораторной работы.