Учреждение образования

«Белорусский государственный технологический университет»

**Кафедра информационных систем и технологий**

**«Отчёт по лабораторной работе 14»**

“ ИССЛЕДОВАНИЕ СТЕГАНОГРАФИЧЕСКОГО

МЕТОДА НА ОСНОВЕ ПРЕОБРАЗОВАНИЯ

НАИМЕНЕЕ ЗНАЧАЩИХ БИТОВ”

**Выполнил:** студент 3 курса

4 группы специальности ПОИТ

Кравцова Диана Вячеславовна

**Проверил:** преподаватель

Блинова Евгения Александровна

Минск 2021

1. **Теоретические сведения**

Определение 1. Стеганографическая система (stegosystem, стегосистема или стеганосистема – в русскоязычной тематической литературе используются оба сокращения) – совокупность средств и методов, которые используются для формирования скрытого канала передачи (или хранения) информации.

При этом скрытый канал организуется на базе и внутри открытого канала с использованием особенностей восприятия информации. «Скрытость» канала передачи тайной информации отличает стеганографии от криптографии: в первом случае тайной является сам факт наличия канала (передачи информации).

Определение 2. Абстрактно стеганографическая система обычно определяется, как некоторое множество отображений одного пространства (множества возможных сообщений, М) в другое пространство (множество возможных стеганосообщений, S, и наоборот.

Основные компоненты стеганосистемы:

контейнер, С (файл-контейнер или электронный документ произвольного формата), в котором размещается (осаждается, скрывается)

тайное сообщение, М; именно контейнер является упомянутым скрытым каналом; тайное сообщение, М, осаждаемое в контейнер для передачи или хранения (например, с целью доказательства или защиты авторских прав на документ-контейнер [2, 53-56]; здесь речь может идти о невидимых цифровых водяных знаках, ЦВЗ);

ключи или ключевая информация, K системы, выполняющие ту же функцию, что и криптографические ключи; ключей может быть несколько, в соответствии с этим современные стеганосистемы характеризуют как многоключевые: один ключ отождествляется с методом осаждения/извлечения тайной информации, другой – с выбором элементов (например, битов) контейнера для его модификации при осаждении тайной информации, третий (или третьи) – для предварительного (перед осаждением) преобразования тайной информации (например, на основе помехоустойчивого кодирования, сжатия или зашифрования) и т. д. [2, 57, 58];

контейнер с осажденным сообщением или стеганоконтейнер, S, который передается по открытому каналу, также являющемуся важным компонентом анализируемой системы; стеганоконтейнер будем именовать также стеганосообщением;

для полноты упомянем также субъектов системы: отправителя и получателя.

В зависимости от формата документа-контейнера цифровую (или компьютерную) стеганографию подразделяют на классы [2, 52, 5964]:

* аудиостеганография,
* видеостеганография,
* графическая стеганография,
* текстовая стеганография и др.

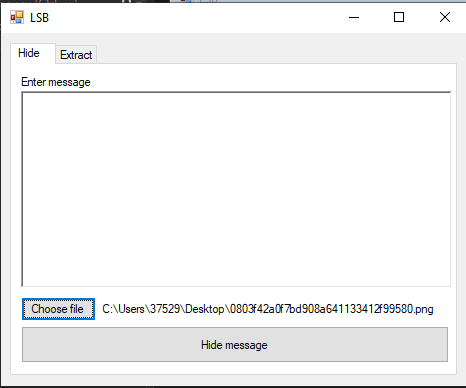
Определение 3. Стеганографической системой ∑ будем называть совокупность сообщений M, контейнеров C, ключей K, стеганосообщений (заполненных контейнеров) S и преобразований (прямого F и обратного F-1), которые их связывают.

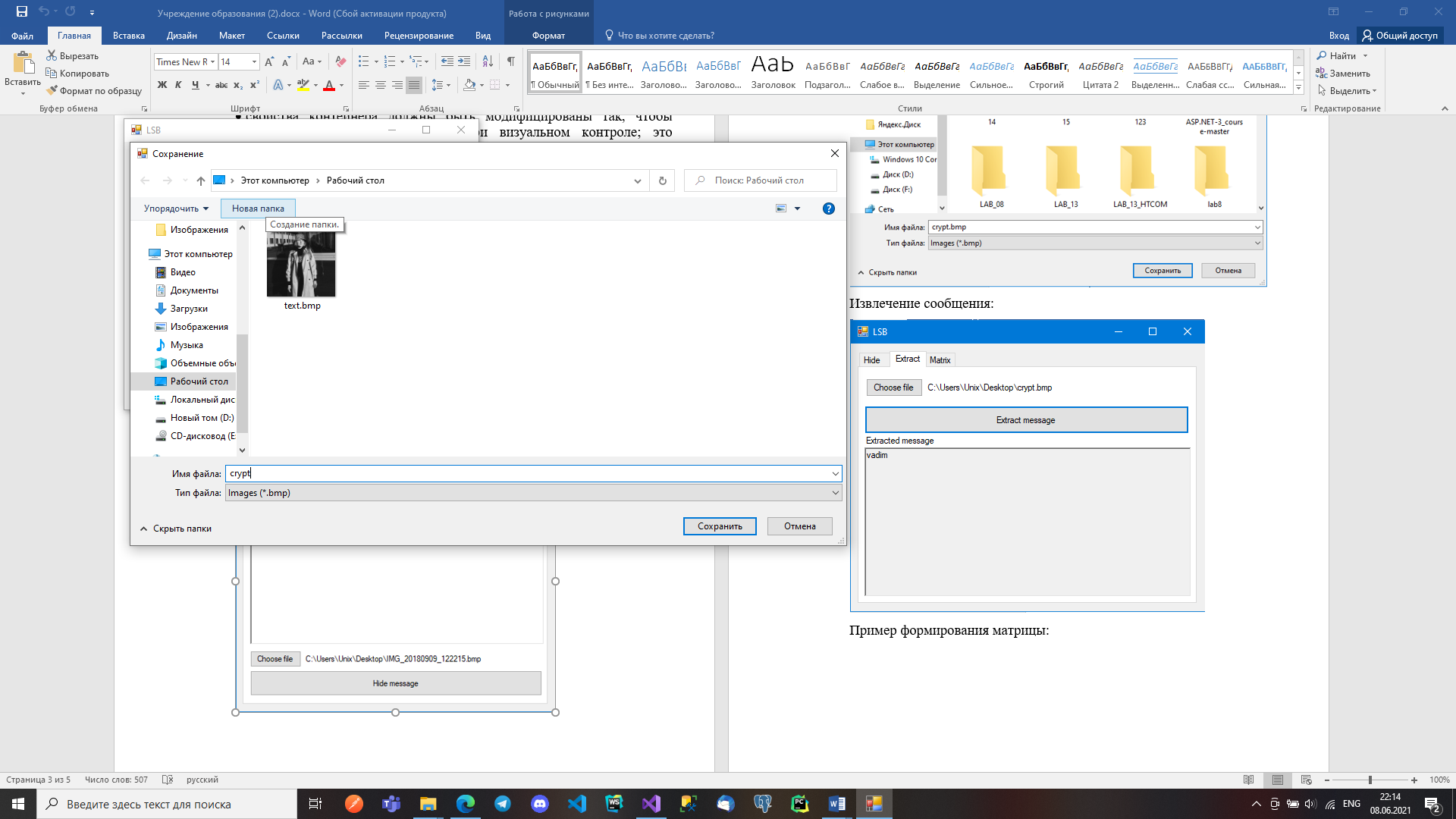
При построении стеганосистемы должны, таким образом, учитываться следующие основные положения:

* свойства контейнера должны быть модифицированы так, чтобы изменение невозможно было выявить при визуальном контроле; это требование определяет качество сокрытия внедряемого сообщения: для обеспечения беспрепятственного прохождения стеганосообщения по каналу связи оно никоим образом не должно привлечь внимание атакующего;
* противник (интруз) имеет полное представление о стеганографической системе и деталях ее реализации; единственной информацией, которая остается ему неизвестной, является ключ, с помощью которого только его держатель может установить факт присутствия и содержание скрытого сообщения;
* если противник каким-то образом узнает о факте существования скрытого сообщения, это не должно позволить ему извлечь подобные сообщения до тех пор, пока ключ хранится в тайне;
* потенциальный противник должен быть лишен каких-либо технических и иных преимуществ в распознавании или раскрытии содержания тайных сообщений.

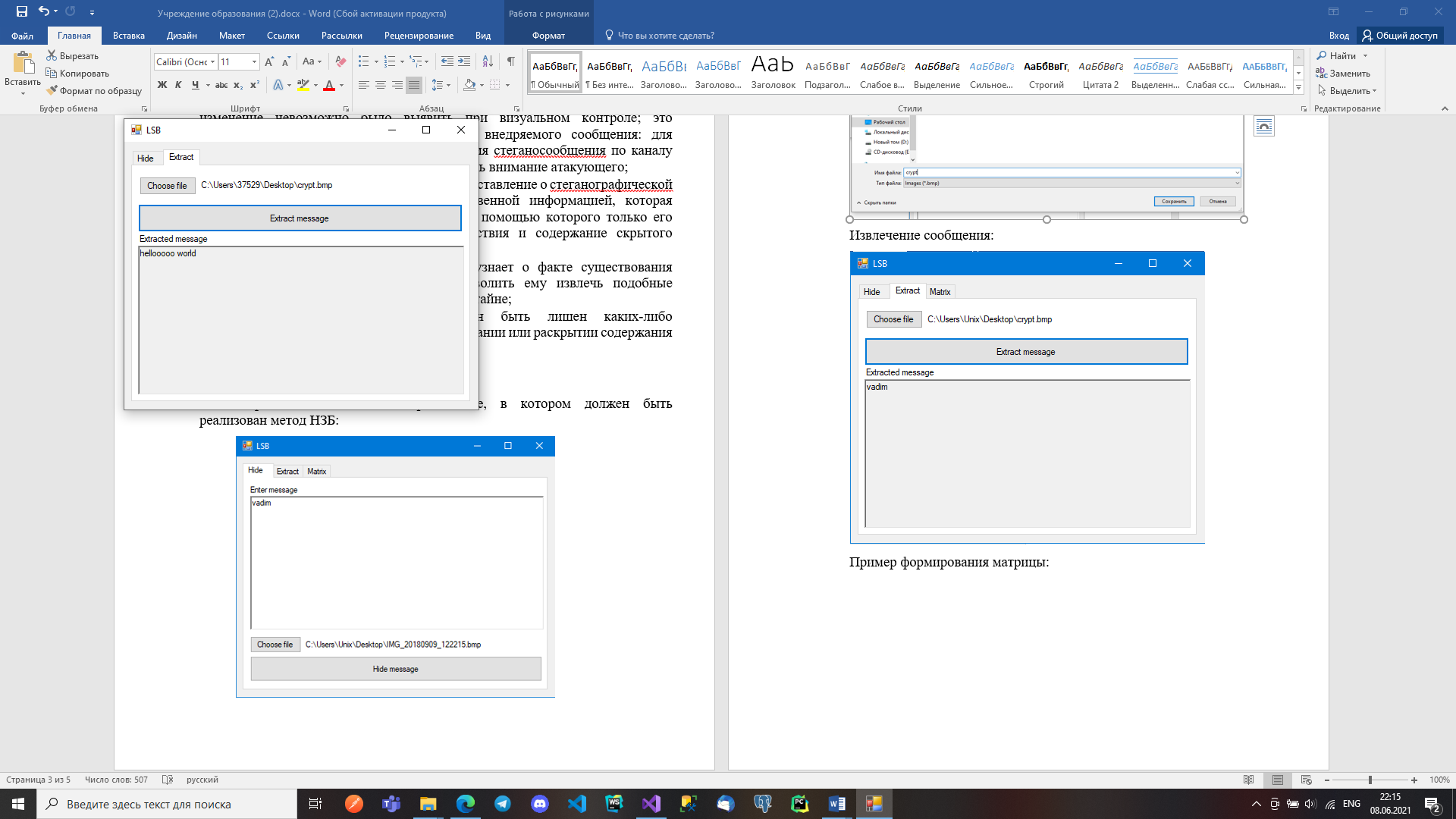
1. **Практическая часть**

Разработать собственное приложение, в котором должен быть реализован метод НЗБ:





Извлечение сообщения:



Пример формирования матрицы:



Изображение со спрятанным сообщением:



Такое изображение для стеганоконтейнера может служить основой для выполнения стеганоанализа.