

Государственное бюджетное общеобразовательное учреждение города Москвы  
«Школа №1542»

## **Защищённый мессенджер на основе технологий стеганографии**

Федотов Михаил Андреевич  
10 «И» класс ГБОУ г. Москвы №1542

Руководитель: Русаков Алексей Михайлович

Преподаватель детского технопарка «Альтаир»

**Москва, 2022**

# Оглавление

Оглавление .....	2
Введение .....	3
Цель .....	3
Задачи.....	3
Методы и этапы .....	4
Актуальность.....	4
Использованные программного решения .....	4
Обзор проектного решения .....	5
Результаты тестирования и реальное применение.....	7
Итоги и перспективы.....	8
Список литературы.....	8

## ***Введение***

В наше время всё большее количество IT-компаний сотрудничают с правоохранительными органами, сливая данные о пользователях и информацию, которой они делятся с другими пользователями. Технология стеганографии сможет обезопасить и защитить конфиденциальность общения в Интернете.

## ***Цель***

Разработать удобный в использовании мессенджер для защищённой передачи информации на основе технологий стеганографии.

## ***Задачи***

- 1) Создать минимальный жизнеспособный прототип мессенджера на основе технологий стеганографии
- 2) Изучить методы, по которым работает технология стеганографии
- 3) Добавить возможность отправлять незашифрованные сообщения
- 4) Добавить функцию шифрации текста внутрь картинки
- 5) Добавить функцию дешифрации текста из полученной картинки
- 6) Добавить функцию авторизации в системе
- 7) Создать удобный виртуальный интерфейс
- 8) Изучить мобильную конвертацию приложений на Android и iOS

## ***Методы и этапы***

Изучение материалов по данной теме	<ol style="list-style-type: none"><li>1. Знакомство с имеющимися технологиями</li><li>2. Опросы специалистов</li><li>3. Личный опыт</li></ol>
Программирование	<ol style="list-style-type: none"><li>1. Изучение фреймворков Quasar и Flask</li><li>2. Изучение языков Python и JavaScript</li><li>3. Создание и отладка прототипа</li></ol>
Внедрение	<ol style="list-style-type: none"><li>1. Выбор платформы для реализации проекта</li></ol>

## ***Актуальность***

Проблема защищённой передачи информации в последнее время всё более актуальна. Для подобных целей иногда используются такие технологии, как криптография и стеганография. Эти технологии существуют ещё с античных времён, и за это время они очень сильно развились. В данном проекте развивается идея стеганографии по трём основным направлениям:

1. возможность зашифровать текстовое сообщение в виде картинки
2. возможность, получив картинку, расшифровать текстовое сообщение, которое было в ней зашифровано
3. возможность авторизации в систему

## ***Использованные программного решения***

Код писался в интерпретаторе Visual Studio Code на языках JavaScript и Python. Были задействованы такие фреймворки, как Flask и Quasar.

# Обзор проектного решения

## Вход и авторизация

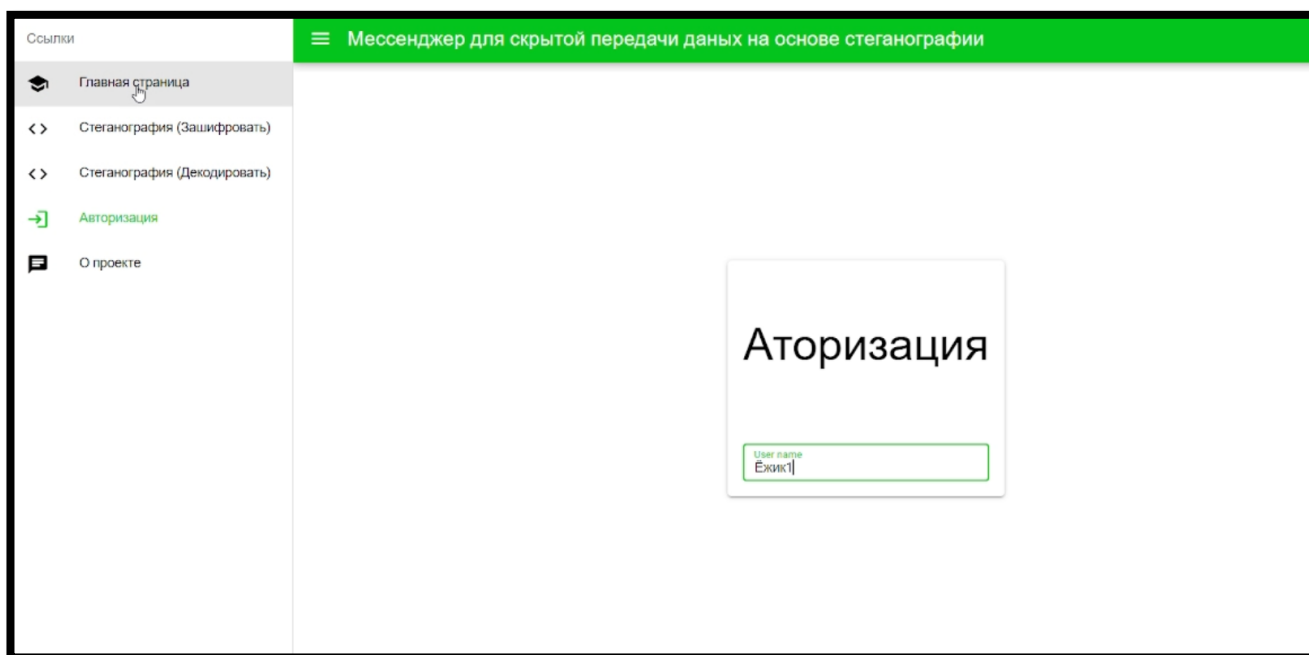


Рис. 1. Авторизация в мессенджере.

Открыв в браузере мессенджер, можно в нём авторизоваться, введя имя пользователя

## Отправка и получение сообщений

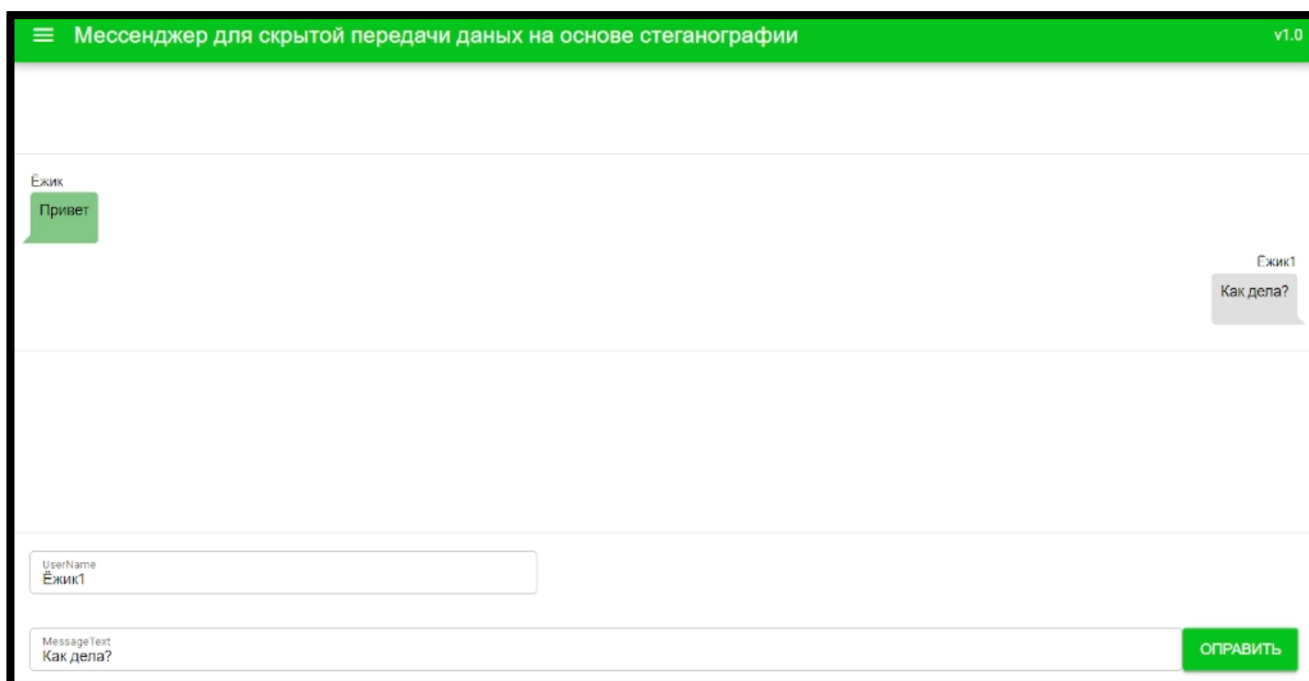


Рис. 2. Чат и отправка сообщений.

Мессенджер позволяет отправлять и получать сообщения без применения технологии стеганографии. Полученные и отправленные сообщения видны в чате, находящемся сверху страницы мессенджера.

### *Шифрование сообщения в картинке*

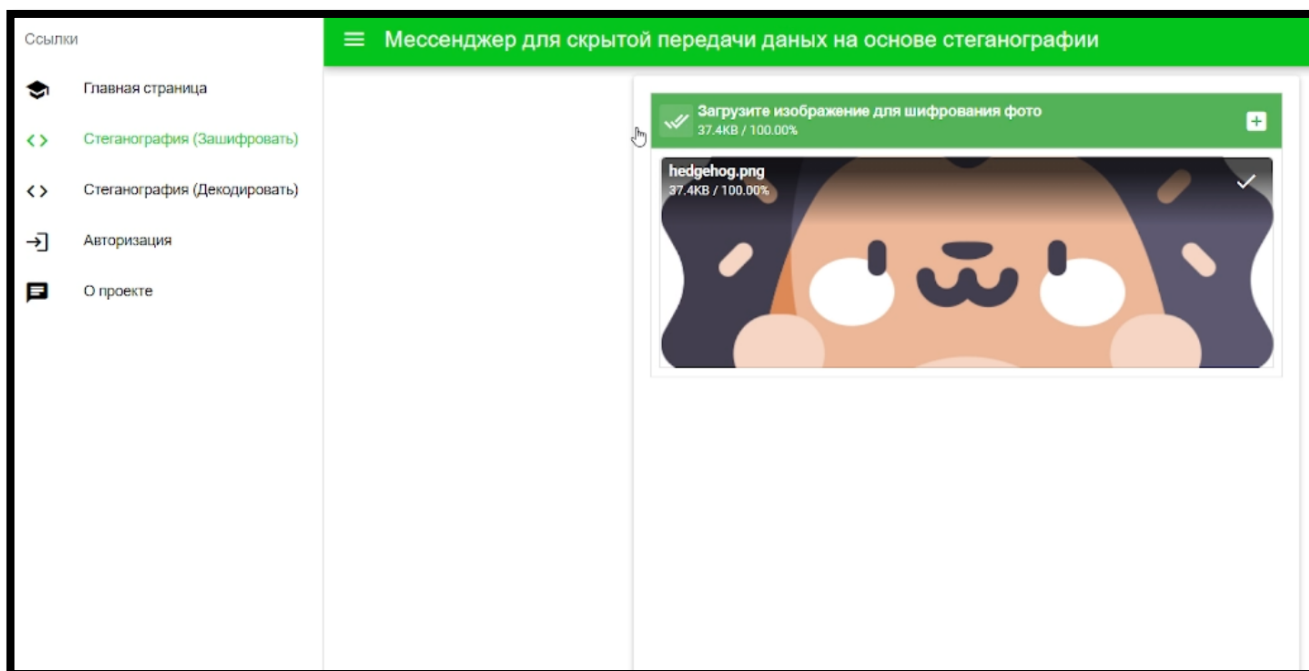


Рис. 3. Шифрование сообщения в картинке

В разделе мессенджера «Стеганография (Зашифровать)» мы пишем текст (стегосообщение), который хотим скрыто отправить. Этот текст шифруется внутрь картинки (стегоконтейнера).

### *Дешифровка сообщения из полученной картинки*

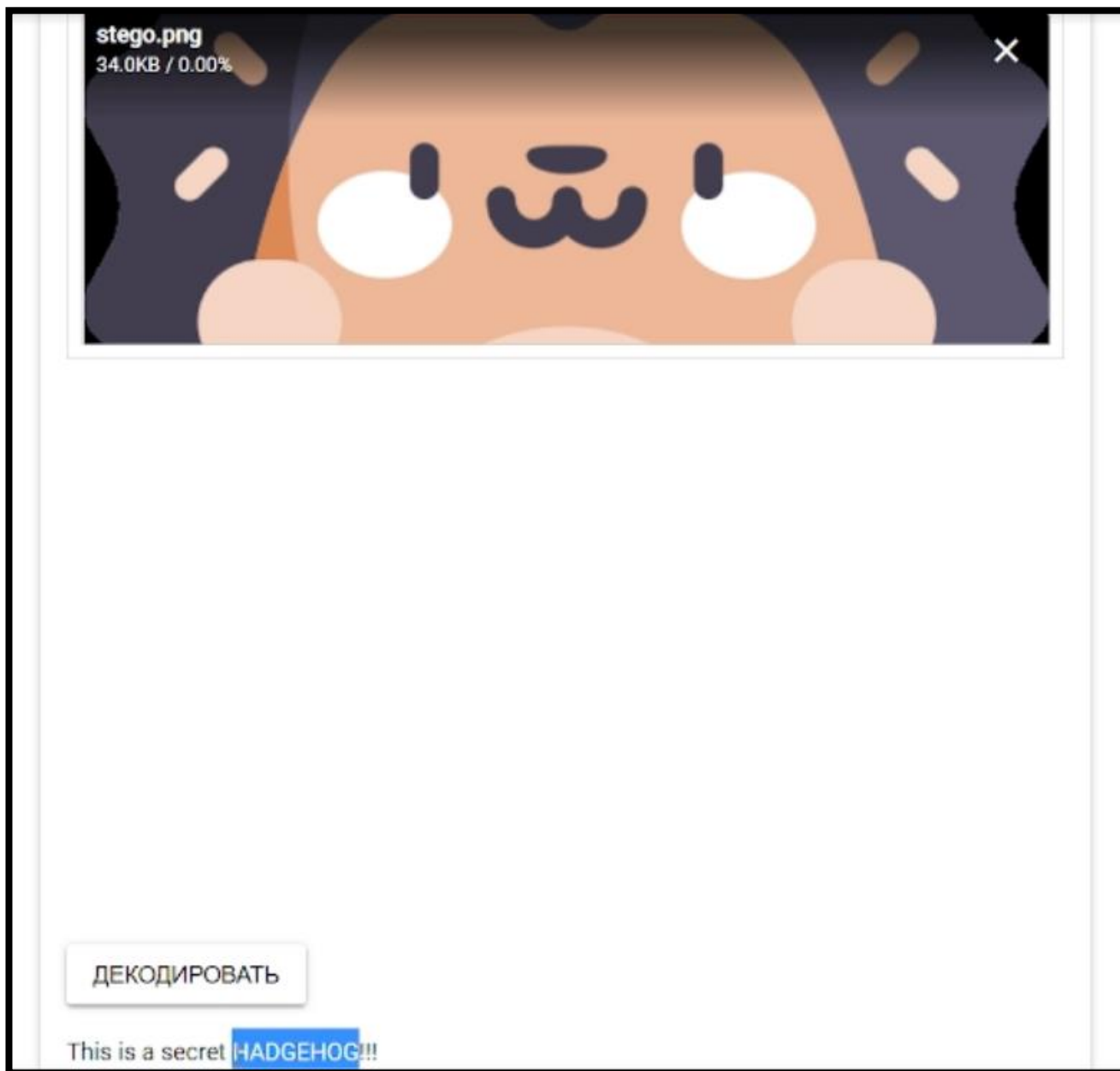


Рис. 4. Дешифровка сообщения из картинки

Получив картинку, её можно положить в раздел мессенджера под названием «Стеганография (Декодировать)». В этом разделе картинка (стегоконтейнер) преобразуется в изначальный текст (стегосообщение).

### ***Результаты тестирования и реальное применение***

Мессенджер уже использовался по своему назначению. Он способен передавать информацию защищённо и скрыто. Суть технологии стеганографии в том, что текстовое сообщение шифруется внутрь картинки, из которой оно снова может быть дешифровано и прочитано другим пользователем

## ***Итоги и перспективы***

В итоге, в проекте было реализовано:

- Создание рабочего прототипа защищённого мессенджера
- Создание понятного визуального интерфейса для мессенджера
- Внедрение технологий стеганографии в прототип мессенджера
- Разработка системы авторизации

Технология стеганографии обладает огромным потенциалом. Эта технология способна передавать сокрытые данные, внутри других, не сокрытых данных. В данном прототипе показаны две составляющих стеганографии: шифрация и дешифрация данных.

Заказчиками и потребителями данного программного продукта являются люди, беспокоящиеся о своей безопасности в сети Интернет.

При выполнении работы были проанализированы проблемы, связанные с самой технологией стеганографии: невысокая скорость и возможность зашифровать лишь текстовые сообщения.

Следующими направлениями разработки данного приложения могут быть:

1. Облегчить систему шифрации и дешифрации сообщений
2. Возможность создавать групповые чаты с несколькими пользователями
3. Портирование приложения на мобильные устройства под управлением операционных систем Android и iOS

## ***Список литературы***

1. [Электронный ресурс] Руководство по языку программирования Python Дата обновления 05.02.2022.  
URL: <https://metanit.com/python/tutorial/>
2. [Учебник]. Бэрри П. Изучаем программирование на Python. Изд-во Litres, 2019.



3. [Электронный ресурс] Руководство по фреймворку Quasar. Дата обновления 01.02.2022. URL: <https://quasar.dev/>
4. [Учебник] Златопольский Д. Основы программирования на языке Python. – Litres, 2019.
5. [Электронный ресурс] Язык программирования Python 3 для начинающих и чайников] URL: <https://pythonworld.ru/>
6. [Учебник] Шихи Д. Серия: Структуры данных в Python. Начальный курс. Изд-во ДМК-Пресс. 2021.