

Кроме того, данная система легко расширяема — при необходимости можно добавить новые уровни прав (например, только чтение с возможностью экспорта, утверждение изменений и т.д.).

Форма для добавления прав доступа для пользователя представлена на рисунке 4.

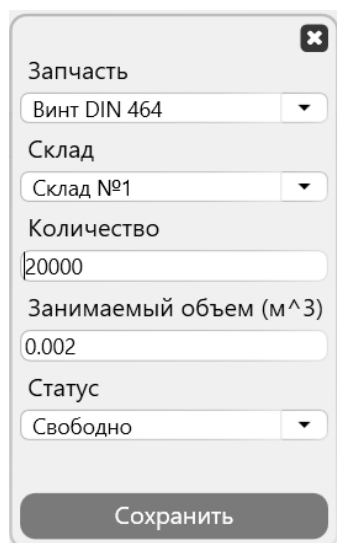


Рисунок 3 — Окно редактирования данных

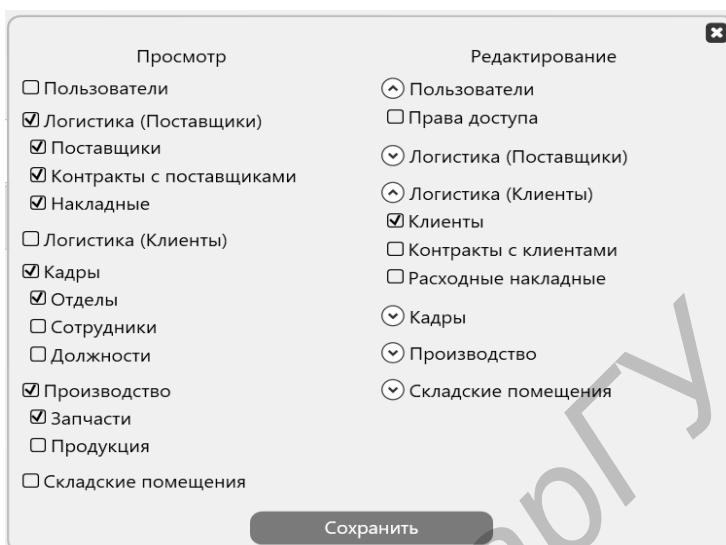


Рисунок 4 — Окно разграничения доступа

Заключение. В процессе разработки было создано приложение, предназначенное для автоматизации различных аспектов деятельности предприятия. Использование технологий современной разработки позволило обеспечить стабильную работу системы, удобство для пользователей и гибкость для дальнейшего расширения функционала.

Фреймворк WPF обеспечил создание визуально понятного и удобного интерфейса, а применение архитектурного паттерна MVVM позволило четко разделить логику представления и бизнес-логику, упростив поддержку и масштабирование проекта. В качестве системы управления базами данных была выбрана MySQL, а для взаимодействия с ней использовался Entity Framework Core, что позволило работать с таблицами в виде объектов и упростило разработку. В приложении реализована система разграничения прав доступа, обеспечивающая защиту данных от несанкционированного доступа. Дополнительно была внедрена система логирования действий пользователей, позволяющая отслеживать ключевые события в системе и повышающая уровень контроля за безопасностью и работоспособностью приложения.

Список цитируемых источников

1. Что такое MySQL. — URL: <https://mchost.ru/articles/chto-takoe-mysql/> (дата обращения: 02.05.2025).
2. Начало работы (WPF). — URL: <https://learn.microsoft.com/ru-ru/dotnet/desktop/wpf/getting-started/?view=netframeworkdesktop-4.8> — (дата обращения: 02.05.2025).
3. Что такое Visual Studio? — URL: <https://learn.microsoft.com/ru-ru/visualstudio/get-started/visual-studio-ide?view=vs-2022> — (дата обращения: 02.05.2025).

УДК 003.26.09

Р. Д. Дедулько, С. В. Лещинский, Ю. Е. Горбач

Учреждение образования «Барановичский государственный университет», Барановичи,
Республика Беларусь

РАЗРАБОТКА ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ ДЛЯ СТЕГАНОГРАФИИ С ИСПОЛЬЗОВАНИЕМ БИБЛИОТЕК PYTHON

Введение. В эпоху стремительного развития цифровых технологий и информационного обмена защита данных становится одной из важнейших задач. Один из эффективных способов обеспечения конфиденциальности информации является стеганография – это наука о тайной передаче информации путем сокрытия самого факта передачи [1].

Развитие вычислительной техники и новых каналов передачи информации привело к появлению новых методов стеганографии, в основе которых лежат особенности представления информации в компьютерных файлах, вычислительных сетях и т.п. Этот вид стеганографии получил название компьютерной стеганографии.

На данный момент существует два основных принципа компьютерной стеганографии.

Первый принцип состоит в том, что файлы изображений или звуков могут быть изменены в определенных пределах без утраты их функциональности, в отличие от других типов данных, для которых необходима абсолютная точность.

Второй принцип основан на том, что органы чувств человека не могут заметить небольшие изменения в цвете изображения или качества звука. Данный принцип достаточно легко применять к изображению или звуку, который несёт избыточную информацию.

Одним из наиболее популярных методов сокрытия информации является LSB-метод — этот метод заменяет последние значащие биты изображения(контейнера) на биты сообщения. Разница между оригинальным изображением и изображением с шифром для человека незаметна.

Данный метод заключается в следующем: допустим, имеется 8-битное изображение в градациях серого. 00h (0000000b) обозначение черного цвета, Fh (1111111b) — обозначение белого цвета. Всего имеется 256 градаций (2^8). Предположим, что сообщение состоит из 1 байта — например, 01101011b. При использовании 2 младших бит в описаниях пикселей, нам потребуется 4 пикселя. Допустим, данные пиксели будут черного цвета. Тогда пиксели, содержащие скрытое сообщение, будут выглядеть следующим образом: 00000001 00000010 00000010 00000011. Тогда цвет пикселей изменится: первого — на $1/255$, второго и третьего — на $2/255$ и четвертого — на $3/255$. Такие градации, мало того, что незаметны для человека, могут вообще не отобразиться при использовании низкокачественных устройств вывода.

Метод LSB применим лишь к изображениям в форматах без сжатия или со сжатием без потерь, так как для хранения скрытого сообщения используются наименее значимые биты значений пикселей, при сжатии с потерями эта информация может быть утеряна.

Основная часть. Целью данного проекта является разработка программного обеспечения для стеганографии с использованием библиотек Python.

Основной задачей стало внедрение метода LSB, который позволяет встраивать текстовые данные в изображение с минимальным искажением его качества. Важно было обеспечить точность извлечения встроенных данных, чтобы они оставались в неизменном виде после обработки. Поэтому для написания программного обеспечения был использован язык программирования Python и среда разработки Visual Studio Code.

Visual Studio Code — это бесплатный и универсальный редактор кода, который поддерживает различные языки программирования и обладает широким набором расширений для удобной работы [2].

Python — это высокоуровневый язык программирования, отличающийся эффективностью, простотой и универсальностью использования. Он широко применяется в разработке веб-приложений и прикладного программного обеспечения, а также в машинном обучении и обработке больших данных. Преимущества языка Python над другими языками программирования [3]:

1. Простота и воспринимаемость обеспечиваются минималистическим синтаксисом.
2. Обширная библиотека, благодаря которой нет необходимости разрабатывать с нуля необходимые методы и многократно используемые фрагменты кода для решения огромного числа задач.
3. Возможность интеграции с другими языками программирования.
4. Мультиплатформенность.
5. Мультипарадигменность, то есть на Python есть возможности для программирования в различных парадигмах программирования: объектно-ориентированной, структурной, функциональной, императивной, процедурной и т.д.

Для реализации интерфейса приложения и LSB-метода были использованы библиотеки Tkinter и Stegano.

Tkinter — это стандартная библиотека Python для создания графического интерфейса. Она предоставляет набор инструментов для разработки оконных приложений, включая элементы управления, такие как кнопки, текстовые поля, метки, панели и другие виджеты, которые упрощают создание интерфейсов.

Stegano — это Python-библиотека, предназначенная для реализации скрытого встраивания информации в различные виды медиафайлов. С помощью этой библиотеки можно легко зашифровать текстовые данные в изображениях, минимизируя визуальное искажение изображения и обеспечивая безопасность передаваемой информации.

На рисунке 1 представлена реализация данного программного обеспечения.

На главном окне приложения пользователь может загрузить изображение, нажав на кнопку «Загрузить изображение» и выбрав файл с диска. После этого пользователь может ввести текст для шифрования в текстовое поле. Когда текст введен, пользователь может нажать кнопку «Зашифровать», и приложение выполнит шифрование текста в изображение с использованием метода LSB. Шифрование выполняется с помощью данной команды:

```
lsb.hide(self.loaded_image.filename, message).save(save_path)
```

Эта команда использует метод `hide` из библиотеки `Stegano`, который позволяет скрыть текстовое сообщение в изображении. В качестве параметров передаются имя загруженного изображения (`self.loaded_image.filename`) и текст сообщения (`message`). После этого, результат работы метода `hide` сохраняется в файл, указанный в переменной `save_path`, с помощью метода `save`.

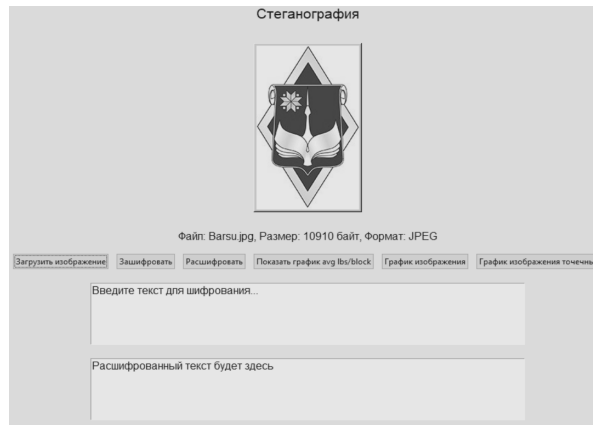


Рисунок 1 — Главное окно приложения

После этого пользователь может загрузить зашифрованное изображение и расшифровать скрытое текстовое сообщение. Расшифрование выполняется с помощью команды:

```
secret_message = lsb.reveal(self.loaded_image.filename)
```

Эта команда использует метод `reveal` из библиотеки `Stegano`. Эта функция анализирует изображение, в котором ранее было зашифровано сообщение, и извлекает скрытую информацию. В качестве параметра передается имя загруженного изображения (`self.loaded_image.filename`). Результатом работы метода является строка, содержащая расшифрованное сообщение, которое сохраняется в переменную `secret_message`.

На рисунках 2,3,4 продемонстрирован слева график оригинального изображения, а справа — график этого же изображения, но с зашифрованным посланием. Видно, что первые несколько десятков блоков значений были переписаны (построение такого графика является еще одной возможностью обнаружить сам факт наличия послания в изображении, но в изображении с большим расширением это заметить трудно). На рисунках 2 и 3 представлены графики для RGB расцветки. На рисунке 4 — точечный график для отслеживания самих средних значений битов.

RGB — это адаптивная цветовая модель получения любых оттенков видимого человеческим глазом спектра, при которой смешиваются красный, зеленый и синий. Аббревиатура RGB расшифровывается как Red, Green, Blue. Данная модель широко применяется в цифровой технике и веб-дизайне, потому что позволяет получить более 16 миллионов цветов.

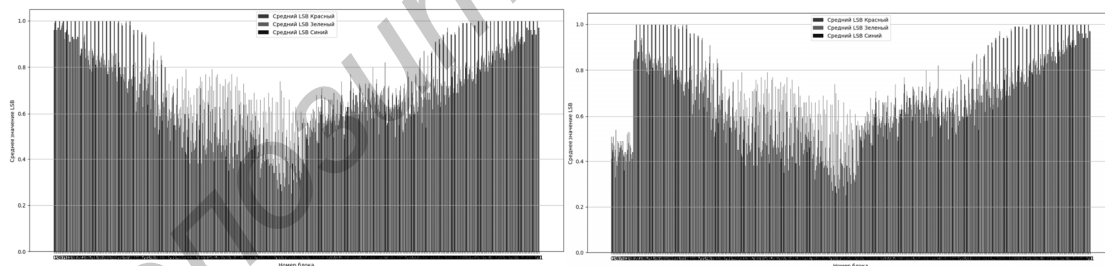


Рисунок 2 — График средних значений наименее значимых битов (LSB) для каждого цветового канала изображения, разделенного на блоки

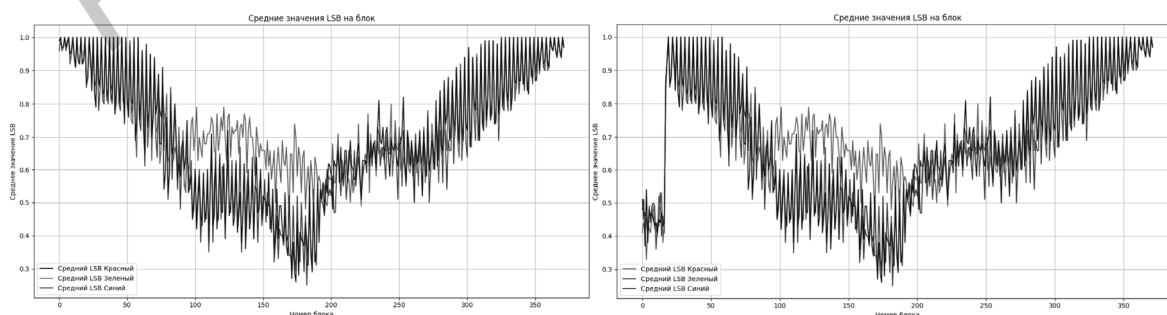


Рисунок 3 — График средних значений наименее значимых битов (LSB) для каждого цветового канала на блоках изображения

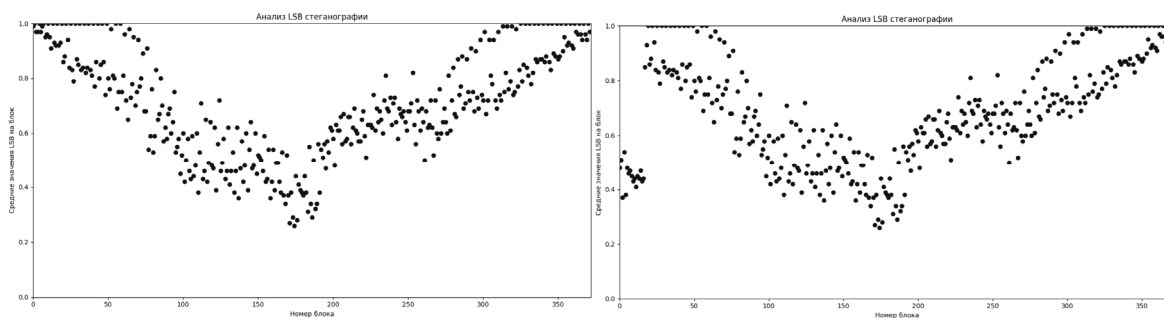


Рисунок 4 — Точечный график средних значений наименее значимых битов (LSB) разделенный на блоки

Заключение. Разработанный программный продукт решает задачу стеганографии LSB-методом желаемого изображения с возможностью расшифровки и экспертного анализа по трем типам графиков.

Список цитируемых источников

1. Кустов, В. Н. Цифровая стеганография — от прошлого к будущему / В. Н. Кустов, Д. К. Прококо // Вестник научных конференций. — 2017. — № 2—3(18). — С. 61—71.
2. Skyeng. — URL: <https://skyeng.ru/magazine/chto-takoe-visual-studio-code/> (дата обращения: 25.11.2024).
3. Skillfactory media. — URL: <https://blog.skillfactory.ru/glossary/python/> (дата обращения: 25.11.2024).

УДК 621.315.322.4

И. В. Дубень, Д. В. Гордич, А. Д. Пахольчик

*Учреждение образования «Барановичский государственный университет»,
Барановичи, Республика Беларусь*

СИСТЕМА РЕГУЛИРОВАНИЯ ТЕМПЕРАТУРЫ НАГРЕВАТЕЛЬНЫХ УСТРОЙСТВ БЕЗ ДАТЧИКОВ ТЕМПЕРАТУРЫ

Введение. Распределённые электронагреватели играют важнейшую роль в решении задач, связанных с контактным нагревом крупных объектов и протяжённых конструкций. Они применяются для предотвращения замерзания трубопроводов, подогрева водосточных систем, поддержания оптимальных температур технологических ёмкостей и многое другое. Традиционные резистивные нагревательные устройства демонстрируют высокую эффективность и надёжность в большинстве случаев эксплуатации.

Современные требования рынка всё чаще обращают внимание на инновационные материалы, такие как карбоновое (углеродное) волокно, которое становится перспективной заменой металлическим компонентам в нагревательных кабелях. Благодаря силиконовой или тефлоновой изоляции они обеспечивают высокую теплопроводность, способность работать в широком диапазоне температур, а минимальный радиус изгиба и большие значения и широкий диапазон удельного сопротивления (от 17 до 133 Ом/м) позволяют использовать их в различных применениях [1]. Монтаж производится параллельно включенными секциями длиной по 10...12 м, что позволяет обеспечить необходимую поверхность нагрева и надёжность устройства в целом.

Выполненный нами анализ распределённых резистивных нагревательных устройств, и в частности, электрообогреваемых полов [1, 2] показал, что в большинстве случаев необходимо использование регулятора мощности как минимум с одним датчиком температуры, который размещают непосредственно в зоне нагрева.

Как известно [3], тепловыделение зависит от условий теплопередачи на всей поверхности нагрева, которая может достигать 8...12 м² и более, в т. ч. от температуры самого нагревательного элемента с учетом его температурного коэффициента сопротивления. Поэтому контроль температуры только в одном месте установки датчика температуры может быть недостаточным. Кроме того, в большинстве известных терморегуляторов регулирование осуществляется дискретным образом — путем включения и отключения напряжения по достижении минимального и максимального пороговых значений температуры [2].

Нами разработана автоматическая система регулирования нагрева на основе микроконтроллера Arduino Nano без использования датчика температуры — в функции потребляемого тока путем периодического измерения удельного сопротивления нагревательного элемента и пакетного способа управления нагрузкой [4].

Основная часть. Микроконтроллер Arduino представляет собой многофункциональное устройство, которое может применяться для управления различными системами, в т. ч. нагревательными устройствами. В нашем случае плата Arduino контролирует температуру карбонового нагревательного провода типа 12K (CF-12-F) [5] длиной 10 м с номинальным удельным сопротивлением 33 Ом/м (при температуре 20 °С).