Министерство науки и высшего образования Российской Федерации

Федеральное государственное бюджетное образовательное учреждение высшего образования

**ИРКУТСКИЙ НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ**

|  |
| --- |
| Институт информационных технологий и анализа данных |
| наименование института |

|  |  |
| --- | --- |
| Допускаю к защите |  |
| Руководитель | подпись |
|  | Л.С. Вахрушева |
|  | И.О. Фамилия |

|  |
| --- |
| Использование нейронных сетей в криптографии |
|  |

наименование темы

**ПОЯСНИТЕЛЬНАЯ ЗАПИСКА**

к курсовому проекту по дисциплине

|  |  |  |
| --- | --- | --- |
| Технологии разработки программных комплексов | | |
|  | 1.13.00.00 - ПЗ |  |

обозначение документа

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Выполнил студент |  | АСУб-21-2 |  |  |  | М.А. Мозолова |
|  |  | шифр группы |  | подпись |  | И.О. Фамилия |
| Нормоконтроль |  |  |  |  |  | Л.С. Вахрушева |
|  |  |  |  | подпись |  | И.О. Фамилия |

Курсовой проект защищен с оценкой \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Иркутск 2024 г.

Министерство науки и высшего образования Российской Федерации

Федеральное государственное бюджетное образовательное учреждение высшего образования

**ИРКУТСКИЙ НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ**

ЗАДАНИЕ

НА КУРСОВОЕ ПРОЕКТИРОВАНИЕ

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| По курсу | Технологии разработки программных комплексов | | | |
| Студенту | Мозоловой М.А. | | | |
|  | (фамилия, инициалы) | | | |
| Тема проекта | | Использование нейронных сетей в криптографии | | |
|  | | | | |
| Исходные данные: | | |  | |
| Нейросетевое моделирование для стегоанализа графических и аудиофайлов с различными параметрами скрытой информации (вариант №13) | | | | |
|  | | | | |
| |  |  |  | | --- | --- | --- | | Рекомендуемая литература: |  | | | 1. Гутгарц Р.Д Проектирование автоматизированных систем обработки информации и управления: учебное пособие для академического бакалавриата. – М.: Издательство Юрайт, 2019. | | | 1. Проектирование АСОИУ [Электронный ресурс] : методические указания по выполнению курсового проекта: 09.03.01 «Информатика и вычислительная техника» для бакалавров по специальности «Автоматизированные системы обработки информации и управления» / Иркут. нац. исслед. техн. ун-т ; сост. Р. Д. Гутгарц. - Электрон. дан. - Иркутск : ИРНИТУ, 2018. | | | 1. Проектирование информационных систем : учебник и практикум для академического бакалавриата / Д. В. Чистов, П. П. Мельников, А. В. Золотарюк, Н. Б. Ничепорук ; под общ. ред. Д. В. Чистова. – М. : Издательство Юрайт, 2016. | | | 1. Рудинский И.Д. Технология проектирования автоматизированных систем обработки информации и управления : учебное пособие для вузов / И. Д. Рудинский. - Москва : Горячая линия - Телеком, 2011. | | | | | |  |

Графическая часть на \_\_\_\_ листах.

Дата выдачи задания « 20 » сентября 2024 г.

|  |  |  |  |
| --- | --- | --- | --- |
| Задание получил |  |  |  |
|  | подпись |  | И.О. Фамилия |

Дата представления проекта руководителю 2024 г.

|  |  |  |  |
| --- | --- | --- | --- |
| Руководитель курсового проектирования |  |  | Л.С.Вахрушева |

**Содержание**

[Введение 4](#_Toc185654964)

[1 Анализ 6](#_Toc185654965)

[1.1 Описание предметной области 6](#_Toc185654966)

[1.1.1 Стегоанализ и методы расшифровки информации 6](#_Toc185654967)

[1.1.2 Применение нейронных сетей для стегоанализа 8](#_Toc185654968)

[1.1.3 Вывод по обзору предметной области 9](#_Toc185654969)

[1.2 Обзор существующих программных средств 9](#_Toc185654970)

[1.2.1 Anubis 10](#_Toc185654971)

[1.2.2 DeepSound 11](#_Toc185654972)

[1.2.3 Hallucinate 13](#_Toc185654973)

[1.2.4 Вывод по обзору существующих программных средств 14](#_Toc185654974)

[1.3 Процессы As-Is и To-Be 15](#_Toc185654975)

[1.3.1 AS-IS 15](#_Toc185654976)

[1.3.2 TO-BE 16](#_Toc185654977)

[1.4 Описание вариантов использования 18](#_Toc185654978)

[1.5 Выработка требований и постановка задачи 20](#_Toc185654979)

[2 Проектирование 22](#_Toc185654980)

[2.1 Выбор и обоснование средств проектирования и реализация 22](#_Toc185654981)

[2.1.1 Средства проектирования 22](#_Toc185654982)

[2.1.2 Средства для программной реализации 22](#_Toc185654983)

[2.2 Проектирование архитектуры приложения 22](#_Toc185654984)

[2.2.1 Описание компонентов архитектуры 22](#_Toc185654985)

[2.2.2 Схема архитектуры 22](#_Toc185654986)

[2.3 Описание входных данных 23](#_Toc185654987)

[2.4 Проектирование пользовательского интерфейса 23](#_Toc185654988)

[Заключение 24](#_Toc185654989)

[Список использованных источников 25](#_Toc185654990)

# Введение

С древнейших времён и до наших дней не теряет своей актуальности задача защиты информации от несанкционированного доступа. История криптографии насчитывает многие тысячелетия. Уже в древности люди стремились скрыть важную информацию от посторонних глаз. Одним из первых методов шифрования был шифр Цезаря, используемый в Древнем Риме. Этот метод основывался на простом сдвиге букв в алфавите на определенное количество позиций. В Древней Греции применялся инструмент под названием скитала, представлявший собой деревянный стержень, на который наматывалась лента с текстом. Сообщение становилось понятным только при наматывании ленты на стержень такого же диаметра. С развитием науки и технологий появлялись более сложные методы, такие как шифр Виженера, основанный на многозначных алфавитах, а также механические устройства для шифрования, например, машины типа «Энигма», которые использовались во время Второй мировой войны.

С появлением компьютеров криптография получила новый импульс для развития. Алгоритмы шифрования стали более сложными, а объемы данных, которые требуется защищать, существенно увеличились. Сегодня методы шифрования и анализа данных применяются не только для обеспечения конфиденциальности переписки, но и для защиты финансовых операций, медицинских данных, интеллектуальной собственности и даже государственной безопасности.

Однако, помимо шифрования, важную роль играет и стеганография – искусство скрытого внедрения данных в цифровые файлы, такие как изображения, аудиозаписи или видеоролики. Стеганография позволяет передавать информацию незаметно для сторонних наблюдателей, что делает ее привлекательной как для легитимных целей, так и для злоумышленников. Это подчеркивает важность разработки методов стегоанализа – процесса выявления скрытых данных.

Стегоанализ, как часть криптографии, направлен на обнаружение скрытой информации в цифровых файлах. Это особенно актуально в условиях, когда методы стеганографии активно применяются как для обеспечения конфиденциальности данных, так и для противоправных целей, включая передачу запрещённой информации. Разработка инструментов для эффективного обнаружения скрытых данных позволяет повысить уровень защиты информационных систем и предотвратить возможные утечки конфиденциальной информации.

С увеличением объёмов передаваемых данных и усложнением угроз цифровой среды возрастает необходимость в создании новых методов защиты информации. Одной из перспективных технологий, применяемых в криптографии, является использование нейронных сетей. Использование нейронных сетей открывает новые возможности для задачи стегоанализа. Их способности к анализу сложных паттернов, возможности адаптироваться к изменениям параметров скрытой информации и обучаться на больших объемах данных делает их незаменимыми в условиях, когда традиционные методы анализа оказываются недостаточными.

В рамках проекта будет разработана и обучена нейронная сеть для стегоанализа графических и аудиофайлов с различными параметрами скрытой информации. Кроме того, будет создано программное обеспечение, объединяющее функционал шифрования, просмотра зашифрованных файлов и их расшифровки. Такой подход позволит не только углубить знания о применении нейронных сетей в криптографии, но и создать эффективный инструмент для повышения уровня информационной безопасности.

Цель проекта: разработка и обучение нейронной сети для стегоанализа графических и аудиофайлов, и создание программного обеспечения, включающего в себя инструменты шифрования, просмотра зашифрованных файлов и их расшифровки.

Задачи для достижения цели:

1. Провести анализ существующих приложений для добавления и выявления скрытой информации в графических и аудиофайлах, выявить их преимущества и недостатки.
2. Обучить нейронную сеть с заданными параметрами на основе датасетов.
3. Реализовать программное приложение для шифрования, просмотра зашифрованных файлов и их расшифровки.

# 1 Анализ

## 1.1 Описание предметной области

Нейросетевые технологии и искусственный интеллект (ИИ) представляют собой совокупность методов и инструментов, предназначенных для моделирования интеллектуального поведения и решения сложных задач, требующих анализа данных, прогнозирования и автоматизации процессов. Основная цель этих технологий – создание систем, способных обучаться, адаптироваться и принимать решения на основе полученной информации, что делает их незаменимыми во многих сферах.

Искусственный интеллект и нейросети уже находят применение в медицине, где они помогают диагностировать заболевания и разрабатывать персонализированные подходы к лечению. В промышленности и бизнесе ИИ используется для оптимизации производственных процессов, анализа больших данных и создания систем автоматического управления. В области информационной безопасности нейронные сети позволяют обнаруживать скрытые угрозы, выявлять уязвимости и анализировать зашифрованные данные, повышая уровень защиты информации.

Эффективность использования нейронных сетей заключается в их способности обрабатывать огромные объемы данных, выявлять сложные зависимости и находить оптимальные решения быстрее и точнее, чем это возможно вручную. Эти технологии необходимы для повышения производительности, обеспечения безопасности и развития новых направлений в науке и технике, что делает их одним из ключевых факторов технологического прогресса.

### 1.1.1 Стегоанализ и методы расшифровки информации

Стегоанализ представляет собой область информационной безопасности, которая занимается выявлением скрытой информации, встроенной в цифровые носители, такие как изображения, аудио, видео или текстовые файлы. Основной задачей стегоанализа является обнаружение, анализ и, при необходимости, извлечение скрытых данных. Это направление актуально как для предотвращения незаконной передачи данных, так и для обеспечения контроля над использованием стеганографических методов.

Стеганография, в отличие от криптографии, направлена не на защиту данных путем их шифрования, а на скрытие самого факта их существования. Информация интегрируется в цифровой носитель таким образом, чтобы он выглядел как обычный файл. Например, данные могут быть внедрены в низкозначащие биты (LSB) изображения, изменяя их так, чтобы визуальные изменения были незаметны.

Методы стегоанализа можно разделить на несколько основных категорий:

* 1. Статистический анализ

Этот подход основан на изучении статистических характеристик цифровых файлов. Стеганография часто нарушает естественные статистические свойства носителя, что позволяет выявлять эти изменения. Можно выделить два основных метода анализа: анализ частотных спектров и выявление аномалий в распределении цветов или значений яркости изображения.

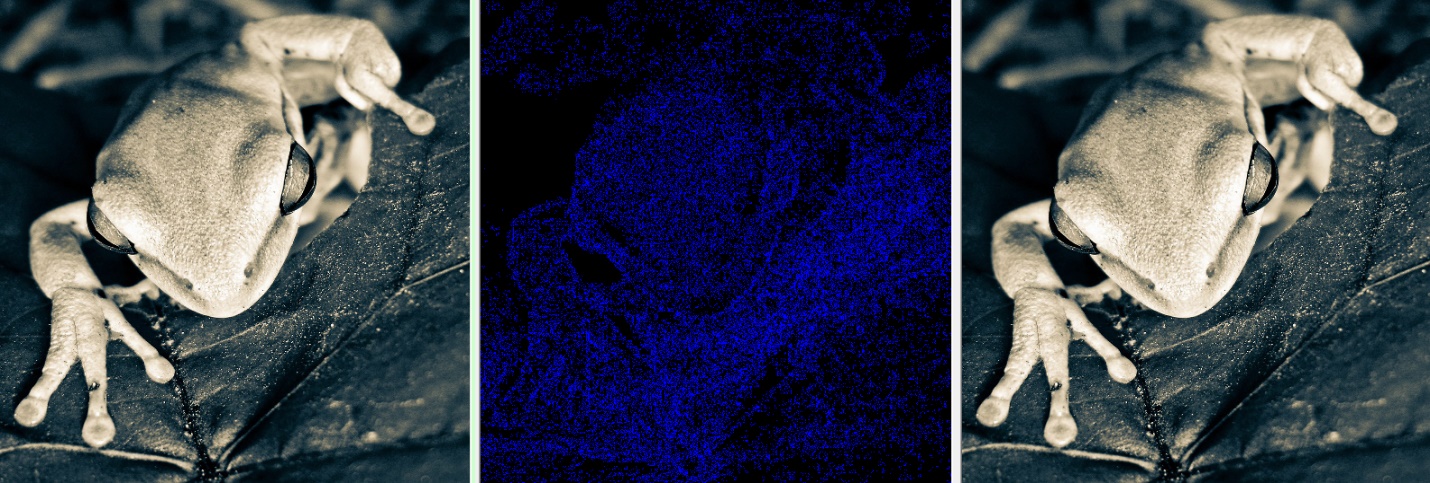


Рисунок 1 – Выявление изменений значений яркости изображения

* 1. Сравнительный анализ

При наличии доступа к оригинальному файлу изображения или аудиофайла, можно провести побитное сравнение измененного носителя с исходным. Это позволяет точно определить участки, где была внедрена информация.

* 1. Спектральный анализ

Основан на преобразовании сигнала в частотное пространство (например, с использованием преобразования Фурье или вейвлет-преобразования). Это позволяет выявить изменения, которые незаметны в пространственном представлении данных.

* 1. Метод машинного обучения

Современные подходы используют нейронные сети и алгоритмы машинного обучения для автоматизированного обнаружения скрытых данных. Эти методы позволяют обучать модель на основе примеров носителей, как и со скрытой информацией, так и без неё. Например, свёрточные нейронные сети (CNN) зачастую используются для анализа изображений, а рекуррентные сети (RNN) для работы с аудиофайлами.

После обнаружения скрытых данных важно извлечь и расшифровать их содержимое. Методы расшифровки включают в себя:

* + 1. Извлечение наименьших бит (LSB)

Этот метод используется, если известно, что данные были встроены в наименьшие биты пикселей или аудиосэмплов. Извлечение выполняется путем анализа каждого бита в данных носителя.

* + 1. Использование стеганографических алгоритмов

Если известен алгоритм, используемый для внедрения данных, можно применить обратную операцию для извлечения информации.

* + 1. Обратное преобразование сигналов

Используется, если скрытая информация была внедрена в частотную область (например, с использованием дискретного косинусного преобразования), необходимо выполнить обратное преобразование для получения исходных данных.

* + 1. Анализ шаблонов

Если при шифровании использовались шаблоны или ключи для внедрения информации, то их анализ и последующий подбор позволяют извлечь данные.

* + 1. Прямой перебор (Brute Force)

Используется в случаях, когда другие методы невозможны. Происходит перебор всех возможных комбинаций параметров внедрения данных. Этот метод требует больших вычислительных ресурсов, но может быть эффективен для небольших объемов данных.

Из всего выше сказанного, можно сделать вывод о том, что стегоанализ играет важную роль в обеспечении информационной безопасности и особенно актуален в борьбе с киберпреступностью, промышленным шпионажем и незаконной передачей данных. Кроме того, он используется в цифровой криминалистике, где важна способность обнаруживать и анализировать скрытые данные для раскрытия преступлений.

### 1.1.2 Применение нейронных сетей для стегоанализа

Применение нейронных сетей для стегоанализа открывает новые горизонты в области информационной безопасности. Традиционные методы обнаружения скрытой информации в цифровых носителях часто оказываются недостаточно точными из-за сложности современных стеганографических алгоритмов. Нейронные сети, благодаря своей способности анализировать сложные и многомерные данные, становятся эффективным инструментом для решения задач стегоанализа.

Основное преимущество нейронных сетей заключается в их способности обучаться на больших объемах данных и выявлять тонкие закономерности, недоступные для традиционных статистических подходов. Например, при анализе изображений сети способны распознавать едва заметные изменения в текстуре или распределении пикселей, вызванные внедрением скрытой информации. В аудиофайлах они могут фиксировать аномалии в частотных спектрах или временных характеристиках сигнала.

Одной из ключевых задач при использовании нейронных сетей является подготовка данных для обучения. Для этого создаются наборы данных, в которых часть файлов содержит скрытую информацию, а часть – нет. Эти данные используются для обучения сети отличать оригинальные носители от модифицированных. Обученная модель может анализировать новые файлы, определяя не только наличие скрытых данных, но и их вероятное расположение.

Современные архитектуры нейронных сетей, такие как свёрточные нейронные сети, показывают высокую эффективность в обработке изображений, поскольку они способны анализировать пространственные взаимосвязи между пикселями. Для аудиофайлов часто применяются рекуррентные сети, которые учитывают временные зависимости в данных.

Применение нейронных сетей для стегоанализа важно не только для защиты данных, но и для борьбы с неправомерным использованием. Например, выявление скрытых сообщений в публично распространяемых файлах может быть критически важным для предотвращения киберугроз. Кроме того, нейросетевые технологии могут использоваться для тестирования устойчивости стеганографических алгоритмов, помогая разработчикам создавать более надежные методы защиты данных.

Подводя итог, можно сделать вывод о том, что нейронные сети становятся мощным инструментом при анализе изображений и аудиофайлов, позволяя не только обнаруживать скрытую информацию, но и углублять понимание процессов, связанных с её интеграцией в цифровые носители. Это направление остается динамично развивающимся и открывает новые возможности для повышения уровня информационной безопасности.

### 1.1.3 Вывод по обзору предметной области

Исследование предметной области продемонстрировало важность применения нейросетевых технологий для решения сложных задач, связанных с обработкой и анализом данных.

Во-первых, стегоанализ является многокомпонентной задачей, требующей учета различных параметров носителей информации, таких как текстура изображений или спектральные характеристики аудиофайлов. Это делает задачу выявления скрытых данных особенно сложной и требует применения методов, способных адаптироваться к нелинейным зависимостям.

Во-вторых, традиционные методы стегоанализа обладают рядом ограничений, включая низкую точность при работе с современными стеганографическими алгоритмами. Нейронные сети, напротив, способны анализировать сложные паттерны и извлекать скрытую информацию с высокой степенью надежности, что делает их более эффективным инструментом для решения подобных задач.

Третий важный аспект заключается в необходимости разработки решений, способных обеспечивать устойчивый анализ скрытой информации в условиях динамично изменяющихся характеристик данных. Это требует использования обучающихся моделей, которые могут адаптироваться к новым условиям и обеспечивать стабильные результаты.

В совокупности, анализ предметной области подчеркивает значимость использования нейросетевых технологий для повышения точности и эффективности стегоанализа, а также для создания инновационных решений в области информационной безопасности.

## 1.2 Обзор существующих программных средств

В данном разделе рассмотрены программные средства, предназначенные для шифрования скрытых данных в изображениях и аудиофайлах. Несмотря на разнообразие готовых решений, практически все из них предоставляют только базовые алгоритмы для шифрования файлов, не используя нейросетевые технологии.

### 1.2.1 Anubis

Программа Anubis предназначена для шифрования текстовой информации в изображениях и выделяется простотой использования. Одной из её особенностей является возможность защитить полученный файл дополнительным PIN-кодом, что обеспечивает базовый уровень защиты. Однако, функциональные ограничения делают её малоэффективной для решения серьёзных задач, связанных с информационной безопасностью.

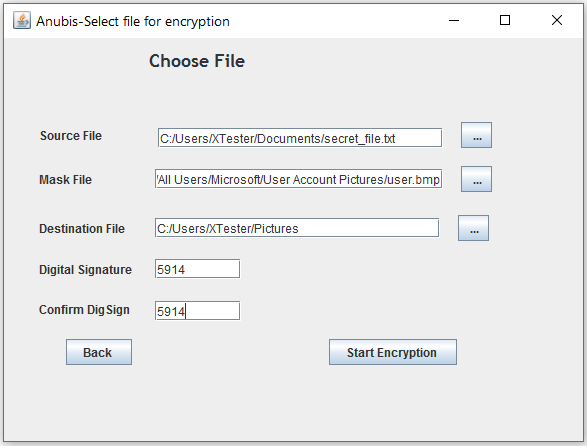


Рисунок 2 – Интерфейс Anubis

Главным недостатком Anubis является поддержка исключительно изображений формата BMP для шифрования, что значительно сужает спектр её применения. Это ограничение делает программу устаревшей, особенно в условиях, когда более современные решения способны работать с различными типами файлов.

Ещё одной серьёзной проблемой является использование единственного алгоритма шифрования, который легко распознаётся. Anubis просто дописывает данные в конец файла, при этом зашифрованная информация сопровождается характерными маркерами. Эти указатели делают процесс шифрования очевидным для обнаружения с помощью простого побайтового сравнения исходного и изменённого файлов. Более того, специализированные утилиты могут быстро идентифицировать все файлы, содержащие такие строки, что сводит на нет преимущества использования программы.

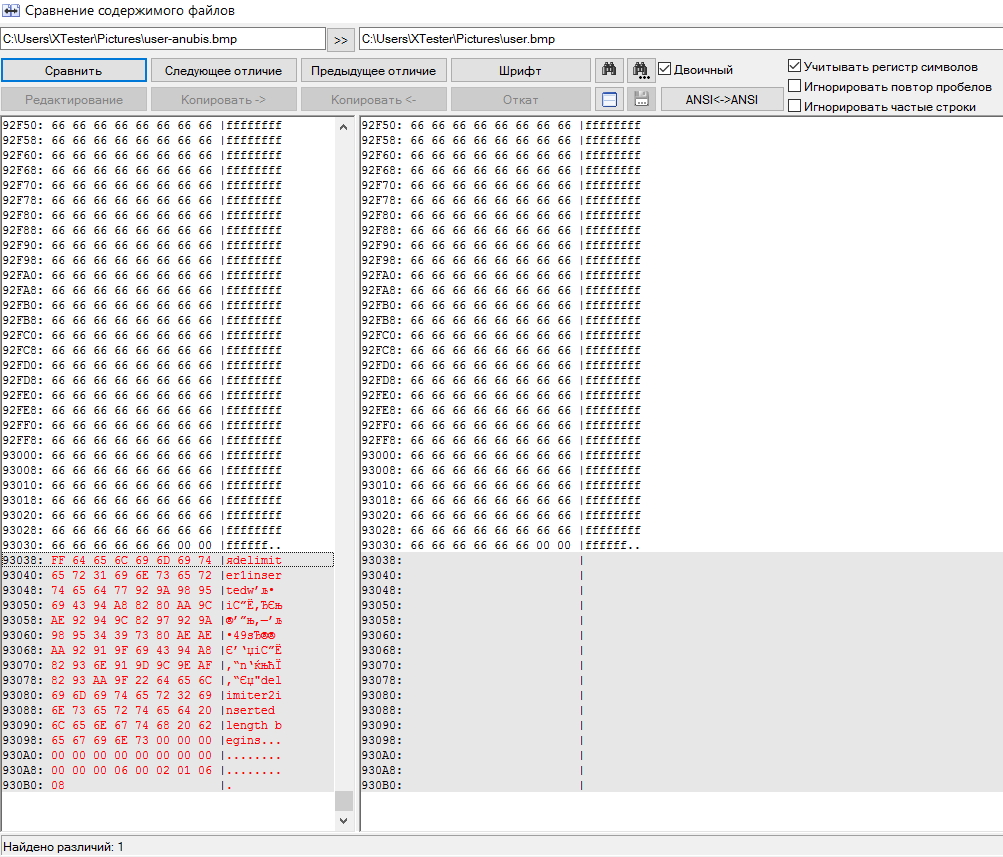


Рисунок 3 – Побайтовое сравнение с оригинальным файлом

Таким образом, Anubis можно рассматривать лишь как демонстрацию простейшего метода стеганографии, но она совершенно не подходит для серьёзных задач, требующих высокой степени защиты данных и устойчивости к анализу.

### 1.2.2 DeepSound

DeepSound предназначена для сокрытия информации внутри аудиофайлов. В качестве контейнеров могут использоваться распространённые типы файлов, такие как WAV, MP3, CDA, WMA и другие форматы. Она способна внедрять файлы любого типа и автоматически рассчитывать доступное место, в зависимости от размера контейнера и настроек качества.

Основное преимущество программы заключается в использовании алгоритма LSB (Least Significant Bit), который изменяет наименьшие биты в данных аудиофайла, минимально искажая их звучание. Такой подход делает сокрытие данных незаметным для человеческого слуха, а обнаружение файла возможно только при помощи сложного статистического анализа или побайтового сравнения с оригиналом. DeepSound также предоставляет возможность шифрования файлов с использованием алгоритма AES и длиной ключа 256 бит (32 символа), что повышает уровень защиты – при расшифровке не будет даже видно название спрятанного файла. Также, из преимуществ можно отметить то, что в один аудиофайл можно поместить сразу несколько файлов различных форматов.

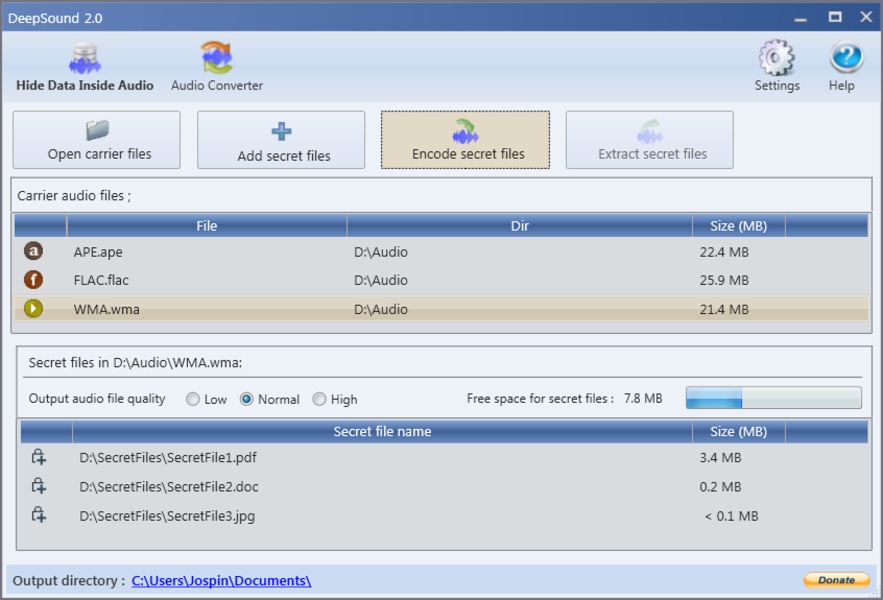


Рисунок 4 – Интерфейс DeepSound

Благодаря использованию алгоритма шифрования наименее значимого бита (LSB), в побайтовом сравнении догадаться о наличии скрытых файлов можно только имея оригинальный файл, так как на изменённых битах отсутствуют какие-либо указатели, в сравнении с предыдущей программой.

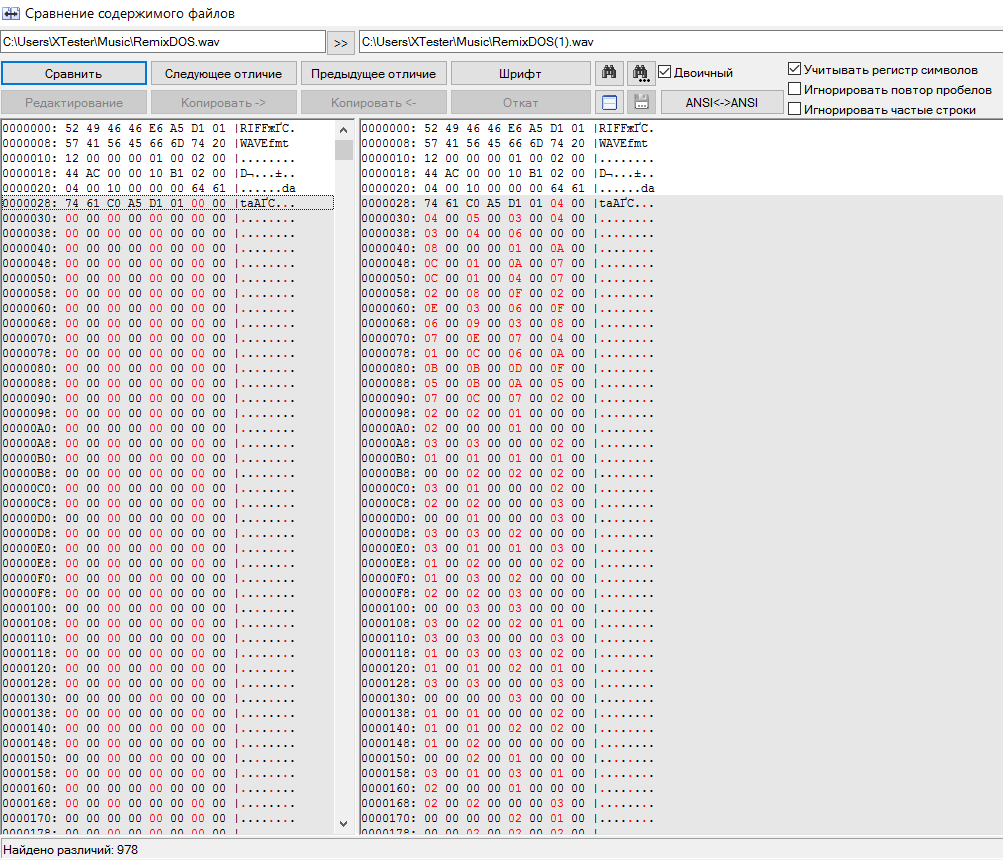


Рисунок 5 – Побайтовое сравнение с оригинальным файлом

Существенным недостатком является то, что после внедрения данных в MP3 или другие форматы контейнеры преобразуются в несжатые форматы WAV, APE или FLAC. Это приводит к значительному увеличению размера итогового файла, из чего можно сделать вывод о том, что данная программа больше подходит для сокрытия только небольших объемов данных.

Подводя итоги, можно сказать, что несмотря на свои недостатки, DeepSound может быть очень полезна и надёжна для решения задачи сокрытия данных в аудиофайлах.

### 1.2.3 Hallucinate

Hallucinate – программа для реализации стеганографического преобразования изображений. Также, как и предыдущая программа, шифрование файлов внутри изображения основано на алгоритме наименее значимого бита (LSB). Несмотря на свою кажущуюся простоту, она предлагает достаточно гибкие настройки, позволяющие адаптировать процесс стеганографии под конкретные нужды пользователя.

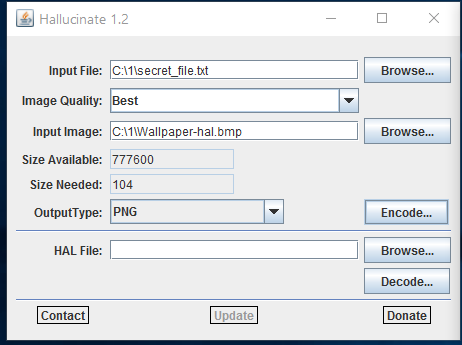


Рисунок 6 – Интерфейс Hallucinate

Основной функцией Hallucinate является выбор любого типа файла и контейнера, в котором его нужно скрыть. Программа поддерживает работу с различными типами медиафайлов, такими как PNG и BMP. Одной из ключевых возможностей является настройка качества итогового медиафайла. Программа предоставляет пользователю восемь уровней качества, каждый из которых влияет на количество информации, которую можно скрыть, а также на визуальное восприятие конечного изображения. Чем сильнее огрубляется исходное изображение, тем больше файлов можно спрятать в контейнере, но тем заметнее это отображается на итоговом медиафайле, содержащем скрытую информацию.

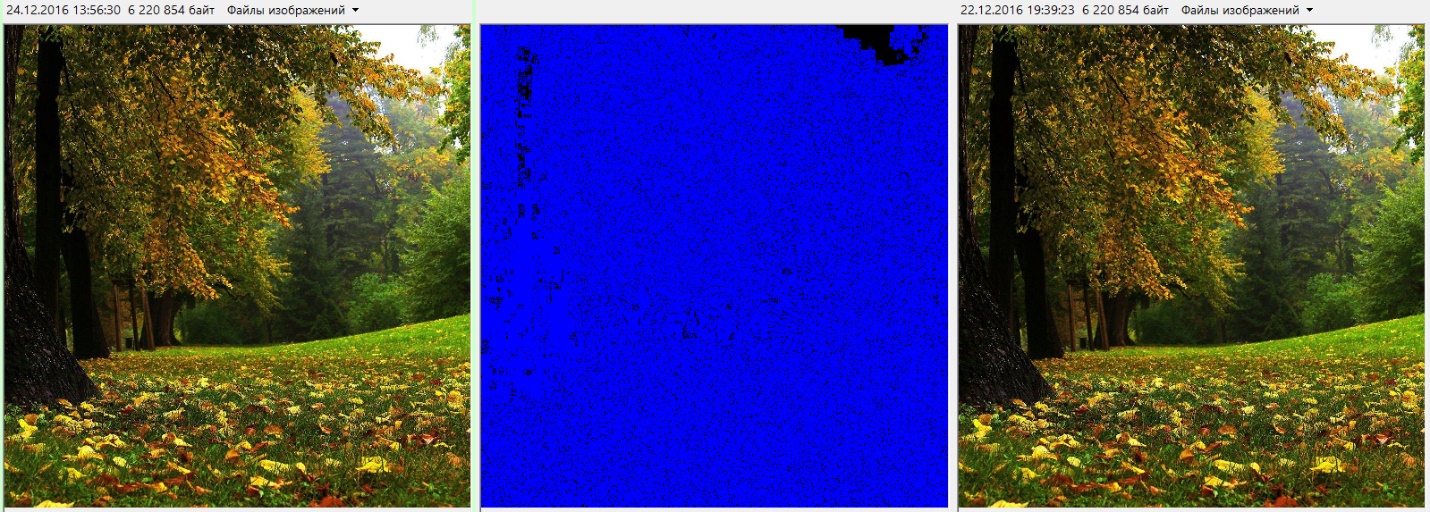


Рисунок 7 – Сравнение оригинального изображения и изменённого при помощи программы Hallucinate

При визуальном осмотре разница между изображениями не слишком заметна. Обнаружить изменения удалось лишь при помощи стороннего программного обеспечения Beyond Compare. Зашифрованный текстовый файл закодирован в изменениях яркости отдельных пикселей, равномерно распределенных по всему кадру. Пиксели плотно расположены только в самых темных и самых светлых участках.

При побайтовом сравнении файлов можно заметить сходства с предыдущим сравнением файла, зашифрованным программой DeepSound, так как был использован аналогичный алгоритм шифрования LSB. В форматы файлов MP3 и PNG вносятся минимальные искажения, неразличимые без специальных методов сравнения, и обнаружить изменения в файлах без исходного довольно сложно. Выдает скрытую информацию только частотный анализ, но хорошо работает этот метод только для обнаружения крупных зашифрованных файлов. Маленький текстовый файл, спрятанный в большой картинке, остается практически незаметным.

### 1.2.4 Вывод по обзору существующих программных средств

Изучив существующие программные решения для сокрытия информации в изображениях и аудиофайлах, можно сделать вывод о том, что большинство из них сосредоточены исключительно на реализации процесса шифрования данных и создания стегоконтейнеров. Такие программы, как Anubis, DeepSound и Hallucinate, предоставляют пользователям инструменты для интеграции скрытых данных в мультимедийные файлы, но они обладают существенными ограничениями. В частности, шифрование информации в этих решениях зачастую не является достаточно скрытным для противостояния углублённому анализу. Алгоритмы некоторых программ оставляют характерные следы в файлах, что облегчает их обнаружение.

Ещё одним недостатком описанных программ является отсутствие встроенных инструментов для расшифровки или анализа скрытых данных. Без использования дополнительных сторонних программ невозможно обнаружить или извлечь скрытые файлы из стегоконтейнеров. Такие ограничения делают существующие решения малоэффективными для применения в условиях, где требуется не только скрывать данные, но и обеспечивать их надёжную защиту и возможность обратного извлечения.

Ещё один важный аспект – отсутствие использования современных технологий, таких как нейронные сети. Ни одна из рассмотренных программ не использует нейронные сети для повышения эффективности или защиты процессов шифрования. Это оставляет пространство для внедрения инновационных подходов, которые могли бы существенно улучшить функциональные возможности подобных решений.

Применение нейронных сетей в разрабатываемом проекте станет уникальной особенностью, позволяющей значительно повысить уровень защиты данных. Нейронные сети обладают способностью обучаться и адаптироваться к различным типам данных и скрытых паттернов, что обеспечит не только высокое качество шифрования, но и возможность автоматизированного выявления скрытых файлов в изображениях и аудиофайлах. Разработка нового программного решения, использующего нейронные сети для шифрования, расшифровки и анализа данных, позволит не только устранить текущие недостатки, присущие аналогам, но и предложить инновационный инструмент, который станет шагом вперёд в области стеганографии и информационной безопасности.

## 1.3 Процессы As-Is и To-Be

### 1.3.1 AS-IS

На текущий момент процесс анализа стеганографических файлов без использования нейронных сетей включает в себя несколько этапов. Специалист вручную анализирует файлы с помощью визуального осмотра и инструментов для выявления аномалий, таких как изменения в структуре изображения или аудиофайла. Затем проводится извлечение скрытой информации, используя различные алгоритмы и методы криптоанализа. Основными ограничениями такого подхода являются высокая трудоемкость, зависимость от квалификации специалиста и ограниченные возможности для обработки большого объема данных.

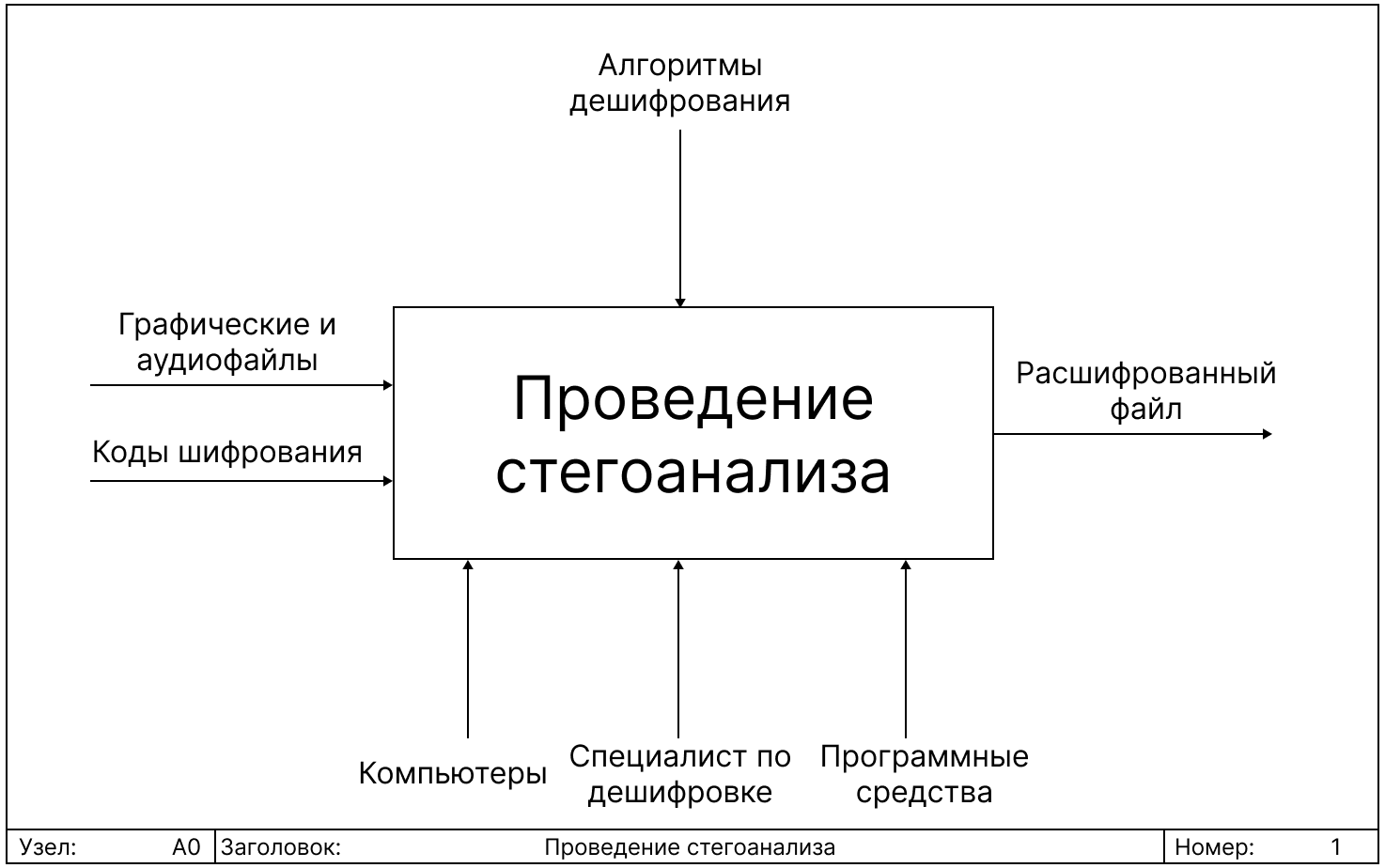


Рисунок 8 – Контекстная диаграмма AS-IS

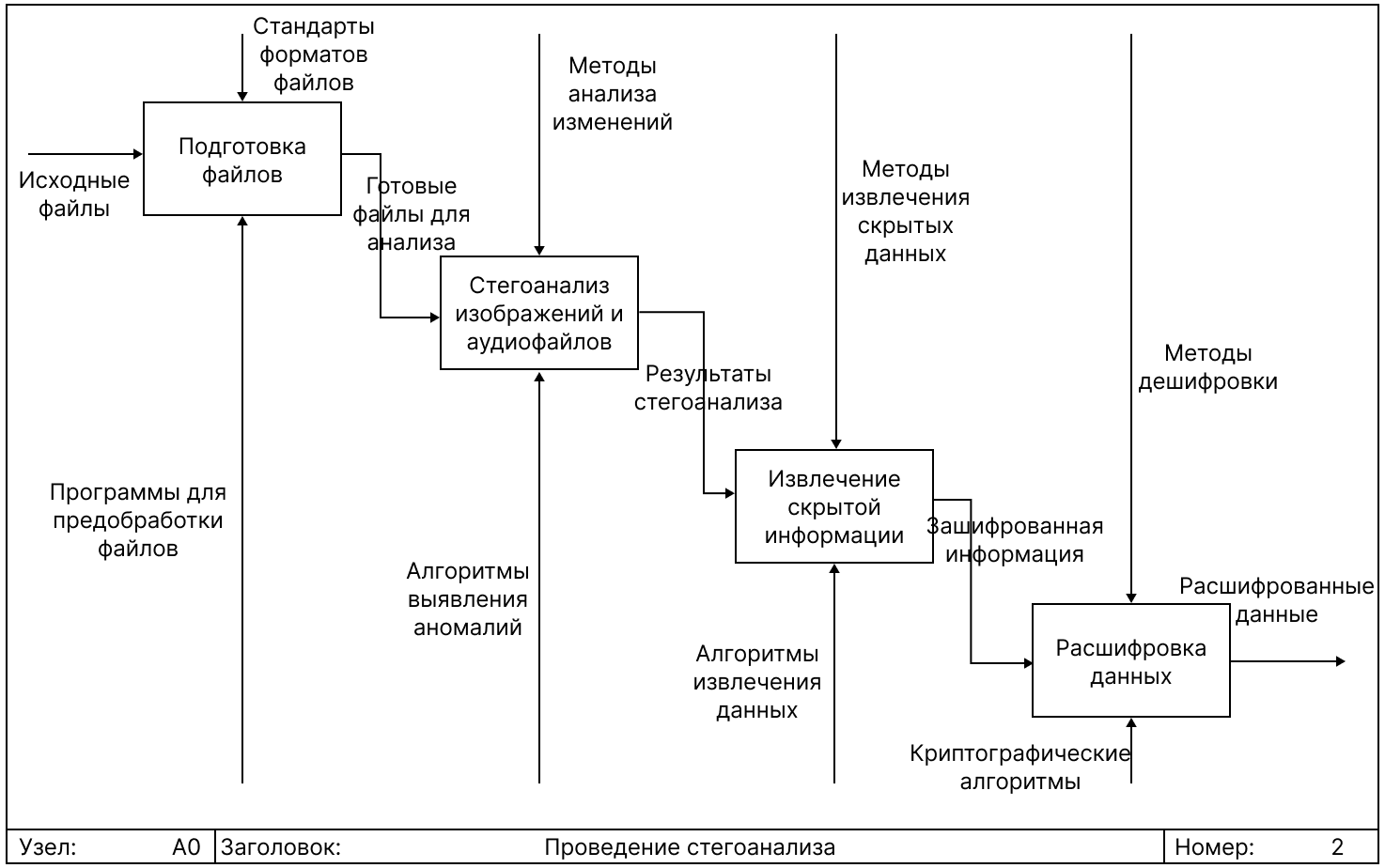


Рисунок 9 – Диаграмма декомпозиции AS-IS

### 1.3.2 TO-BE

В целевом состоянии процесс включает в себя использование нейронную сеть для стегоанализа графических и аудиофайлов с целью извлечения скрытой информации. В отличие от традиционного метода, где анализ проводится вручную с использованием статических алгоритмов, в новом процессе нейронные сети автоматизируют обнаружение аномалий в изображениях и аудиофайлах, что значительно увеличивает точность и скорость анализа.

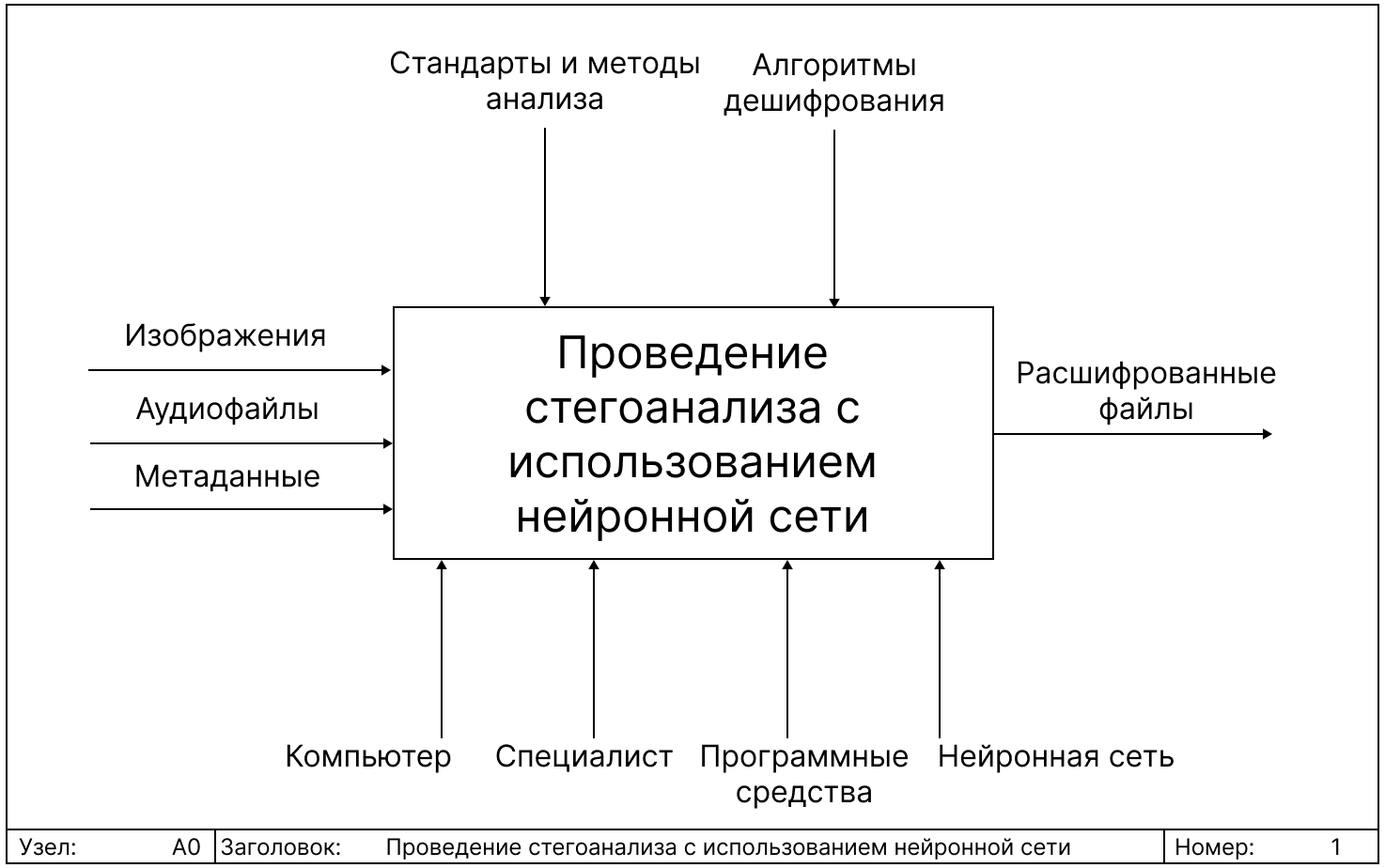


Рисунок 10 – Контекстная диаграмма TO-BE

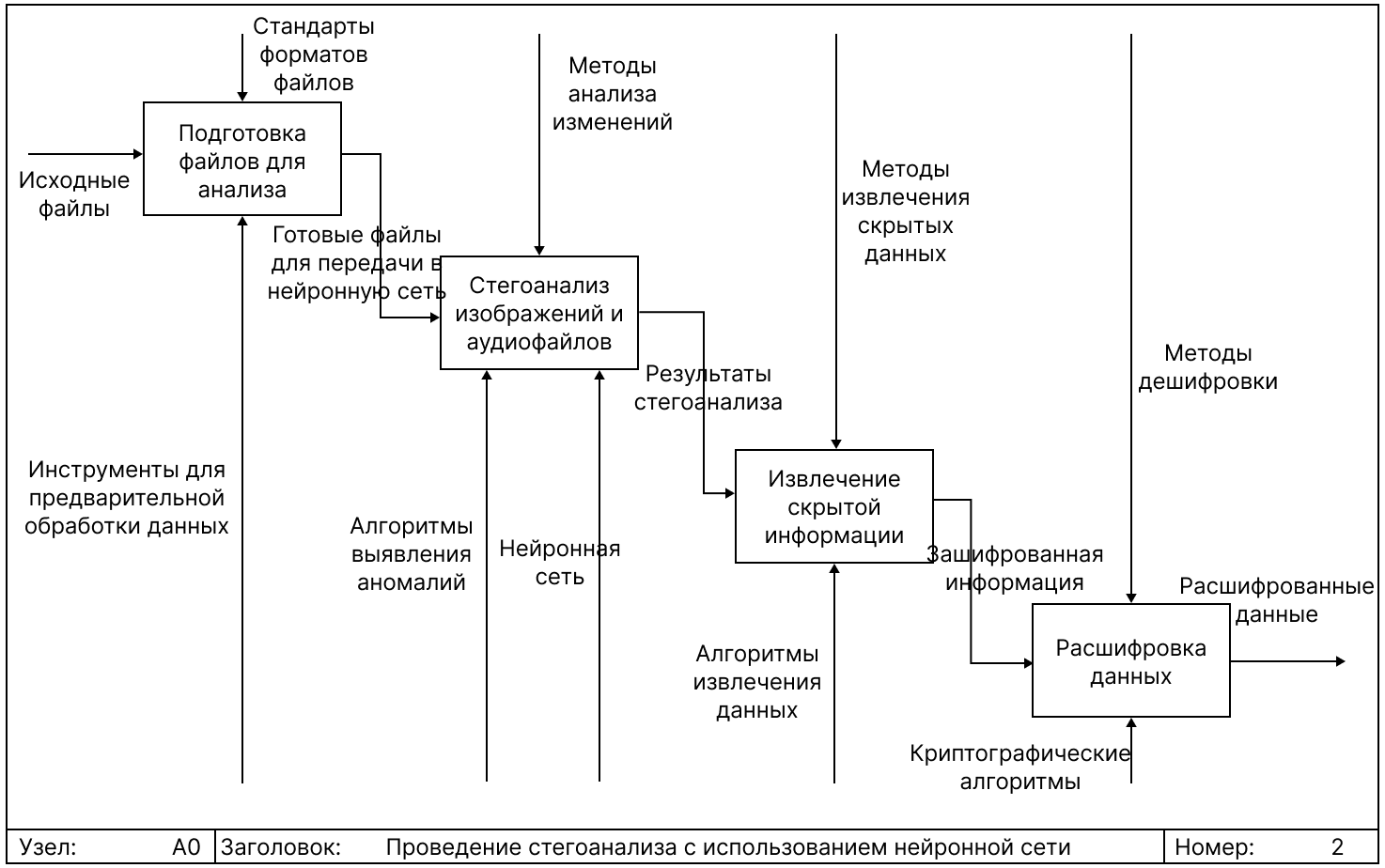


Рисунок 11 – Диаграмма декомпозиции TO-BE

Анализ текущего и целевого состояния процессов стегоанализа графических и аудиофайлов позволяет выделить значительные различия в подходах и возможностях каждого из них, а также оценить преимущества, которые дает внедрение нейронных сетей в процесс.

В текущем состоянии процесс анализа стеганографических файлов зависит от человеческого анализа и традиционных алгоритмов, что делает его трудоемким и ограниченным. Специалисты вручную исследуют изображения и аудиофайлы, пытаясь выявить аномалии и изменения в структуре файлов, которые могут свидетельствовать о скрытой информации. Этот процесс требует высокой квалификации и внимательности, а также может занимать значительное время, особенно при большом объеме данных. Важной проблемой является то, что используемые алгоритмы не всегда способны эффективно обнаружить скрытые данные, особенно если они использовали сложные или продвинутые методы сокрытия информации. В случае с изображениями это может быть связано с невозможностью традиционных алгоритмов учесть все виды манипуляций с пикселями, а в аудиофайлах — с ограниченными возможностями для анализа частотных изменений, которые могут быть использованы для скрытия информации. Все это снижает общую эффективность процесса и его способность работать с большими объемами данных, поскольку каждый файл анализируется вручную.

Целевое состояние предполагает внедрение нейронной сети для автоматизации и улучшения процесса стегоанализа. Использование нейронных сетей, в частности свёрточных нейронных сетей (CNN) для изображений и рекуррентных нейронных сетей (RNN) для аудиофайлов, позволит значительно улучшить точность и скорость анализа. Нейронные сети обучаются на больших объемах данных, что позволяет им распознавать даже очень тонкие и незаметные изменения в структуре файлов, которые могли бы быть упущены традиционными методами. Такой подход также значительно ускоряет процесс, поскольку нейронные сети могут работать с множеством файлов одновременно, в отличие от традиционного ручного метода, где каждый файл требует детального и длительного анализа. Внедрение нейронных сетей снижает зависимость от квалификации специалистов, поскольку система будет обучаться на примерах и автоматически выявлять аномалии без необходимости в постоянном вмешательстве человека. Кроме того, такой подход может работать с гораздо большими объемами данных, что делает его более масштабируемым и подходящим для современных задач.

Исходя из вышеперечисленного, переход от текущего состояния к целевому состоянию с использованием нейронных сетей значительно повысит эффективность и надежность процесса стегоанализа. Система, основанная на нейронных сетях, будет быстрее, точнее и способна обрабатывать большие объемы данных, что сделает её более подходящей для использования в реальных условиях, где важна как скорость, так и качество анализа.

## 1.4 Описание вариантов использования

Диаграмма вариантов использования описывает основные функции системы, ориентированные на взаимодействие пользователя и инженера с программным обеспечением для шифрования, дешифровки и анализа скрытых данных. На диаграмме выделены ключевые пользователи (актёры) и их взаимодействие с основными функциями системы, включая настройку параметров, обучение нейронной сети и использование системы для обработки данных.

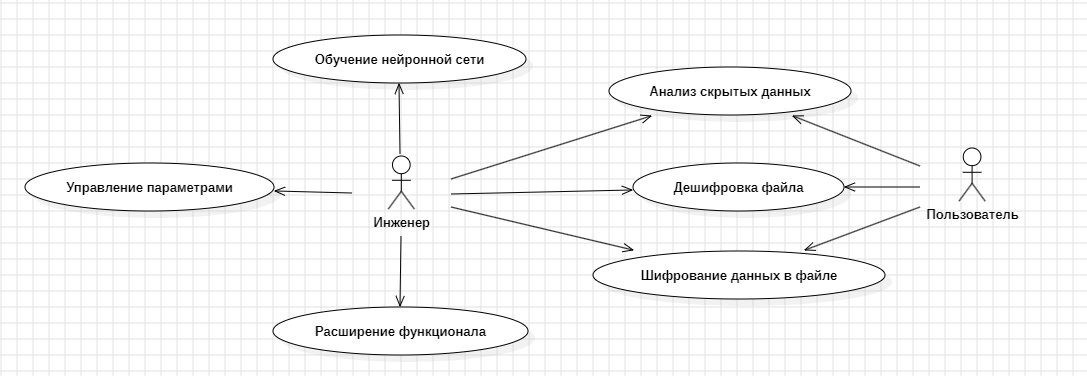


Рисунок 8 – Диаграмма прецендентов

Основные актёры:

1. Инженер – специалист, отвечающий за разработку и настройку программного обеспечения, включая обучение нейронной сети, расширение функционала и управление параметрами;
2. Пользователь — конечный потребитель, который использует приложение для шифрования данных, их расшифровки и анализа скрытых данных.

Основные варианты использования:

1. Шифрование данных в файле:

* Пользователь выбирает файл для шифрования и задаёт параметры (тип контейнера, ключ шифрования);
* Цель: скрыть информацию в выбранном файле с использованием стеганографических методов.

1. Дешифровка файла:

* Пользователь загружает файл-контейнер для расшифровки;
* Цель: извлечь и восстановить скрытую информацию из файла.

1. Анализ скрытых данных:

* Пользователь загружает файл для анализа, и система автоматически проверяет наличие скрытых данных;
* Цель: определить, содержатся ли в файле скрытые данные и с какими параметрами они могут быть извлечены.

1. Управление параметрами:

* Инженер задаёт параметры шифрования и настройки нейронной сети для повышения эффективности работы системы;
* Цель: обеспечить гибкость и адаптивность приложения в зависимости от специфики задач.

1. Обучение нейронной сети:

* Инженер загружает обучающие данные, настраивает параметры и запускает процесс обучения;
* Цель: улучшить способности системы к анализу скрытых данных и расшифровке.

1. Расширение функционала:

* Инженер добавляет новые алгоритмы шифрования, типы файлов или параметры для анализа;
* Цель: увеличить возможности приложения и обеспечить его актуальность.

## 1.5 Выработка требований и постановка задачи

Анализ предметной области показал, что в современной криптографии, основанной на методах стеганографии, наблюдается рост требований к безопасности, точности и универсальности инструментов, используемых для сокрытия информации. Традиционные подходы, включающие использование алгоритмов шифрования и методов внедрения данных в мультимедийные контейнеры, зачастую оказываются уязвимыми перед современными методами анализа. Отсутствие гибкости и недостаточная защита скрытых данных подчеркивают необходимость разработки более эффективных и адаптивных решений.

Существующие программные средства, такие как Anubis, DeepSound и Hallucinate, выполняют задачи сокрытия информации, однако они не лишены ряда недостатков. Эти программы ограничены как типами поддерживаемых файлов-контейнеров, так и простотой применяемых алгоритмов шифрования. Более того, ни одно из этих решений не предлагает функционала, позволяющего выявлять скрытые данные, а их шифровальные методы остаются предсказуемыми и уязвимыми перед побайтовым или статистическим анализом. Выявленный недостаток стандартных подходов к стеганографии подчеркивает необходимость внедрения инновационных технологий, которые способны обеспечить устойчивость скрытой информации перед современными угрозами.

В ходе анализа было также установлено, что современные программные средства не используют нейронные сети для улучшения шифрования и анализа данных. Это открывает перспективу создания уникального решения, которое объединит преимущества машинного обучения и современных криптографических методов. Нейронные сети обладают потенциалом для автоматического распознавания паттернов в полученных данных и обучения на основе сложных зависимостей, что позволяет реализовать более сложные и устойчивые методы шифрования.

На основе анализа предметной области и существующих решений сформулирована задача: разработать программное обеспечение, использующее нейронные сети для шифрования и расшифровки данных. В отличие от традиционных методов, данное решение будет направлено на:

* + - 1. Автоматизация процесса стегоанализа. Интеграция нейронных сетей обеспечит возможность автоматического поиска скрытых файлов в контейнерах и их последующей дешифровки.
      2. Поддержку различных типов файлов. Программа будет универсальной, поддерживая широкий спектр форматов изображений и аудиофайлов для повышения её применимости.
      3. Адаптивность и масштабируемость. Нейросетевые алгоритмы способны адаптироваться к новым типам данных, обеспечивая долгосрочную актуальность программного решения.
      4. Простоту и удобство использования. Современный пользовательский интерфейс и высокая степень автоматизации сделают программу доступной для широкого круга пользователей.

Создание данного программного обеспечения позволит не только устранить недостатки существующих аналогов, но и внедрить новый стандарт безопасности в области стеганографии. Разработка такого инструмента станет значимым шагом вперёд в использовании нейронных сетей для решения задач криптографии и информационной защиты.

# 2 Проектирование

## 2.1 Выбор и обоснование средств проектирования и реализация

### 2.1.1 Средства проектирования

На этапе проектирования приложения используются инструменты для создания прототипов и моделей системы, что позволяет визуализировать пользовательские сценарии, разработать интерфейс, продумать архитектуру и логику взаимодействий.

* Figma – это облачное средство для проектирования интерфейсов и создания интерактивных прототипов. В Figma планируется выполнить визуализацию пользовательских сценариев, включая элементы навигации, структуру страниц и отдельных интерфейсных элементов. Figma поддерживает совместное редактирование и комментирование проекта, что ускоряет процесс создания и согласования макетов;
* Microsoft Visio – средство для построения диаграмм, таких как BPMN и IDEF0, которые помогут детально отобразить структуру системы и процессы, происходящие внутри неё. Эти инструменты визуализируют функциональные и информационные потоки, что особенно важно для согласования на этапе разработки.

### 2.1.2 Средства для программной реализации

На этапе реализации были выбраны технологии, обеспечивающие надёжную разработку интерфейса программы.

Для написания и редактирования кода используются следующие среды:

* Visual Studio Code – лёгкий редактор кода с обширной поддержкой расширений для работы с Java, Python, C++ и другими языками программирования. Поддержка функций автодополнения и отладки делает его универсальным инструментом для написания кода;
* PyCharm – специализированная IDE для Python, включающая мощные средства отладки и аналитики кода, что особенно полезно при написании кода для нейронной сети.

Управление версиями:

* Git – система контроля версий, которая позволит отслеживать изменения кода, обеспечивая командную работу и сохранение всех итераций разработки;
* GitHub / GitLab – платформы для хостинга и управления проектами, предоставляющие функции для совместной разработки, управления задачами и рецензирования кода.

## 2.2 Проектирование архитектуры приложения

А

### 2.2.1 Описание компонентов архитектуры

А

### 2.2.2 Схема архитектуры

А

## 2.3 Описание входных данных

А

## 2.4 Проектирование пользовательского интерфейса

А

# Заключение

В рамках проекта была поставлена цель

# Список использованных источников

* 1. Дрюченко М.А., Сирота А.А. Стегоанализ цифровых изображений с использованием глубоких нейронных сетей и гетероассоциативных интегральных преобразований // (статьи и методические указания) [сайт] [2022]. URL: https://cyberleninka.ru/article/n/stegoanaliz-tsifrovyh-izobrazheniy-s-ispolzovaniem-glubokih-neyronnyh-setey-i-geteroassotsiativnyh-integralnyh-preobrazovaniy (дата обращения 21.11.2024).
  2. Natarajan Meghanathan, Lopamudra Nayak. Steganalysis algorithms for detecting the hidden information in image, audio and video cover media // (статьи и методические указания) [сайт] [2010]. URL: https://www.researchgate.net/ publication/41099668\_Steganalysis\_algorithms\_for\_detecting\_the\_hidden\_information\_in\_image\_audio\_and\_video\_cover\_media (дата обращения 01.12.2024).
  3. Гераськин А.С., Смирнов Е.Д. Обнаружение скрытого стеганографического вложения и признаков монтажа в области данных аудиофайла // (статьи и методические указания) [сайт] [2020]. URL: https://journals.vsu.ru/sait/article/view/2917 (дата обращения 28.11.2024).
  4. Терещенко С.Н., Перов А.А., Осипов А.Л. Особенности применения предобученных свёрточных нейронных сетей к задачам стегоанализа графических изображений // (статьи и методические указания) [сайт] [2021]. URL: https://www.iae.nsk.su/images/stories/5\_Autometria/5\_Archives/2021/4/12\_ Tereshchenko.pdf (дата обращения 28.11.2024).
  5. Очимов С.Ю. Стегоанализ аудиофайлов, базирующийся на алгоритмах сжатия // (статьи и методические указания) [сайт] [2021]. URL: https://cyberleninka.ru/article/n/stegoanaliz-audiofaylov-baziruyuschiysya-na-algoritmah-szhatiya (дата обращения 10.12.2024).
  6. Ntivuguruzwa Jean De La Croix, Tohari Ahmad, Fengling Han. Comprehensive survey on image steganalysis using deep learning // (статьи и методические указания) [сайт] [2024]. URL: https://www.sciencedirect.com/ science/article/pii/S2590005624000195 (дата обращения 10.12.2024).
  7. Карпеко О.В. Карин С.А., Спиридонов С.Г., Карин А.И. Способ выявления скрытой информации в потоке данных дистанционного зондирования объекта на основе нейросетевых стегодетекторов // (статьи и методические указания) [сайт] [2022]. URL: https://cyberleninka.ru/article/n/ sposob-vyyavleniya-skrytoy-informatsii-v-potoke-dannyh-distantsionnogo-zondirovaniya-obekta-na-osnove-neyrosetevyh-stegodetektorov (дата обращения 10.12.2024).
  8. Вильховский Д.Э. Обзор методов стеганографического анализа изображений в работах зарубежных авторов // (статьи и методические указания) [сайт] [2020]. URL: https://www.researchgate.net/profile/Alexander-Guts/publication/347971987\_Steganalysis\_of\_low\_stego-payload\_color\_images\_ using\_software\_complex/links/6027f8f14585158939a23a1c/Steganalysis-of-low-stego-payload-color-images-using-software-complex.pdf (дата обращения 18.12.2024).