**Федеральное агентство по образованию**

**Государственное образовательное учреждение высшего профессионального образования**

**«ЮЖНО-РОССИЙСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ**

**(НОВОЧЕРКАССКИЙ ПОЛИТЕХНИЧЕСКИЙ ИНСТИТУТ)»**

**ФАКУЛЬТЕТ** Информационных технологий и управления

**КАФЕДРА** Информационных и управляющих систем

**СПЕЦИАЛЬНОСТЬ** Информационные системы и технологии

**ПОЯСНИТЕЛЬНАЯ ЗАПИСКА**

к курсовому проекту (работе) по дисциплине

«Защита и безопасность данных»

на тему: «Атаки на стегосистемы. Водяные знаки»

Выполнил студент ИС-02-Д1 Шаркова М.А.

Руководитель Виниченко С.М.

К защите Защита принята с оценкой

"\_\_\_"\_\_\_\_\_\_\_\_\_\_\_\_ 2008г. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

 \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ "\_\_\_"\_\_\_\_\_\_\_\_\_\_\_\_\_\_ 2008г.

подпись \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

подпись

Волгодонск 2008

СОДЕРЖАНИЕ

1. Введение
2. Общие сведения о стеганографии

2.1 Основные понятия и определения стеганографии

2.2 Цифровые водяные знаки

2.3 Атаки на стегосистемы

2.4 Атаки на стегосистемы водяных знаков

1. Обоснование целей и задач курсового проекта
2. Инструкция для пользователя

4.1 Схема работы для пользователя

4.2 Установочные требования

4.3 Требования к системе

1. Инструкция для программиста
2. Список литературы
3. **ВВЕДЕНИЕ**

Задача защиты информации от несанкционированного доступа решалась во все времена на протяжении истории человечества. Уже в древнем мире выделилось два основных направления решения этой задачи, существующие и по сегодняшний день: криптография и стеганография. Целью криптографии является скрытие содержимого сообщений за счет их шифрования. В отличие от этого, при стеганографии скрывается сам факт существования тайного сообщения.

Слово «стеганография» имеет греческие корни и буквально означает «тайнопись». Исторически это направление появилось первым, но затем во многом было вытеснено криптографией. Тайнопись осуществляется самыми различными способами. Общей чертой этих способов является то, что скрываемое сообщение встраивается в некоторый безобидный, не привлекающий внимание объект. Затем этот объект открыто транспортируется адресату. При криптографии наличие шифрованного сообщения само по себе привлекает внимание противников, при стеганографии же наличие скрытой связи остается незаметным.

Какие только стеганографические методы не использовали люди для защиты своих секретов. Известные примеры включают в себя использование покрытых воском дощечек, вареных яиц, спичечных коробков и даже головы раба (сообщение читалось после сбривания волос гонца). В прошлом веке широко использовались так называемые симпатические чернила, невидимые при обычных условиях. Скрытое сообщение размещали в определенные буквы невинных словосочетаний, передавали при помощи внесения в текст незначительных стилистических, орфографических или пунктуационных погрешностей. С изобретением фотографии появилась технология микрофотоснимков, успешно применяемая Германией во время мировых войн. Крапление карт шулерами – это тоже пример стеганографии.

Во время Второй мировой войны правительством США придавалось большое значение борьбе против тайных методов передачи информации. Были введены определенные ограничения на почтовые отправления. Так, не принимались письма и телеграммы, содержащие кроссворды, ходы шахматных партий, поручения о вручении цветов с указанием времени и их вида; у пересылаемых часов переводились стрелки. Был привлечен многочисленный отряд цензоров, которые занимались даже перефразированием телеграмм без изменения их смысла.

Развитие средств вычислительной техники в последнее десятилетие дало новый толчок для развития компьютерной стеганографии. Появилось много новых областей применения. Сообщения встраивают теперь в цифровые данные, как правило, имеющие аналоговую природу. Это – речь, аудиозаписи, изображения, видео. Известны также предложения по встраивании информации в текстовые файлы и в исполняемые файлы программ.

Существуют два основных направления в компьютерной стеганографии: связанные с цифровой обработкой сигналов и не связанные. В последнем случае сообщения могут быть встроены в заголовки файлов, заголовки пакетов данных. Это направление имеет ограниченное применение в связи с относительной легкостью вскрытия и/или уничтожения скрытой информации. Большинство текущих исследований в области стеганографии, так или иначе, связаны с цифровой обработкой сигналов. Это позволяет говорить о цифровой стеганографии.

Можно выделить две причины популярности исследований в области стеганографии в настоящее время: ограничение на использование криптосредств в ряде стран мира и появление проблемы защиты прав собственности на информацию, представленную в цифровом виде. Первая причина повлекла за собой большое количество исследований в духе классической стеганографии (то есть скрытия факта передачи информации), вторая – еще более многочисленные работы в области так называемых водяных знаков. Цифровой водяной знак (ЦВЗ) – специальная метка, незаметно внедряемая в изображение или другой сигнал с целью тем или иным образом защищать информацию от несанкционированного копирования, отслеживать распространение информации по сетям связи, обеспечивать поиск информации в мультимедийных базах данных.

Международные симпозиумы по скрытию данных проводятся с 1996 года, по стеганографии первый симпозиум состоялся в июле 2002 года. Стеганография – быстро и динамично развивающаяся наука, использующая методы и достижения криптографии, цифровой обработки сигналов, теории связи и информации.

# **Общие сведения о стеганографии**

**2.1 Основные понятия и определения стеганографии**

Несмотря на то, что стеганография как способ сокрытия секретных данных известна уже на протяжении тысячелетий, компьютерная стеганография - молодое и развивающееся направление.

Как и любое новое направление, компьютерная стеганография, несмотря на большое количество открытых публикаций и ежегодные конференции, долгое время не имела единой терминологии.

До недавнего времени для описания модели стеганографической системы использовалась предложенная 1983 году Симмонсом так называемая "проблема заключенных". Она состоит в том, что два индивидуума (Алиса и Боб) хотят обмениваться секретными сообщениями без вмешательства охранника (Вилли), контролирующего коммуникационный канал. При этом имеется ряд допущений, которые делают эту проблему более или менее решаемой. Первое допущение облегчает решение проблемы и состоит в том, что участники информационного обмена могут разделять секретное сообщение (например, используя кодовую клавишу) перед заключением. Другое допущение, наоборот, затрудняет решение проблемы, так как охранник имеет право не только читать сообщения, но и модифицировать (изменять) их.

Позднее, на конференции Information Hiding: First Information Workshop в 1996 году было предложено использовать единую терминологию и обговорены основные термины.

**Стеганографическая система или стегосистема** - совокупность средств и методов, которые используются для формирования скрытого канала передачи информации.

При построении стегосистемы должны учитываться следующие положения:

* противник имеет полное представление о стеганографической системе и деталях ее реализации. Единственной информацией, которая остается неизвестной потенциальному противнику, 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 в других данных 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.

Обобщенная модель стегосистемы представлена на рис. 1.

**Рисунок 1 - Обобщенная модель стегосистемы**

В качестве данных может использоваться любая информация: текст, сообщение, изображение и т. п.

В общем же случае целесообразно использовать слово "**сообщение**", так как сообщением может быть как текст или изображение, так и, например, аудиоданные. Далее для обозначения скрываемой информации, будем использовать именно термин сообщение.

**Контейнер** - любая информация, предназначенная для сокрытия тайных сообщений.

**Пустой контейнер** - контейнер без встроенного сообщения; **заполненный контейнер** или **стего - контейнер**, содержащий встроенную информацию.

**Встроенное (скрытое) сообщение** - сообщение, встраиваемое в контейнер.

**Стеганографический канал** или просто **стегоканал** - канал передачи стего.

**Стегоключ** или **просто ключ** - секретный ключ, необходимый для сокрытия информации. В зависимости от количества уровней защиты (например, встраивание предварительно зашифрованного сообщения) в стегосистеме может быть один или несколько стегоключей.

По аналогии с криптографией, по типу стегоключа стегосистемы можно подразделить на два типа:

* с секретным ключом;
* с открытым ключом.

В стегосистеме с секретным ключом используется один ключ, который должен быть определен либо до начала обмена секретными сообщениями, либо передан по защищенному каналу.

В стегосистеме с открытым ключом для встраивания и извлечения сообщения используются разные ключи, которые различаются таким образом, что с помощью вычислений невозможно вывести один ключ из другого. Поэтому один ключ (открытый) может передаваться свободно по незащищенному каналу связи. Кроме того, данная схема хорошо работает и при взаимном недоверии отправителя и получателя.

* 1. **Цифровые водяные знаки**

В настоящее время можно выделить три тесно связанных между собой и имеющих одни корни направления приложения стеганографии: сокрытие данных (сообщений), цифровые водяные знаки (ЦВЗ) и заголовки. Остановимся подробнее на втором приложении.

Цифровые водяные знаки могут применяться, в основном, для защиты от копирования и несанкционированного использования. В связи с бурным развитием технологий мультимедиа остро встал вопрос защиты авторских прав и интеллектуальной собственности, представленной в цифровом виде. Примерами могут являться фотографии, аудио и видеозаписи и т.д. Преимущества, которые дают представление и передача сообщений в цифровом виде, могут оказаться перечеркнутыми легкостью, с которой возможно их воровство или модификация. Поэтому разрабатываются различные меры защиты информации, организационного и технического характера. Один из наиболее эффективных технических средств защиты мультимедийной информации и заключается во встраивании в защищаемый объект невидимых меток – водяных знаков. Разработки в этой области ведут крупнейшие фирмы во всем мире. Так как методы цифровых водяных знаков начали разрабатываться совершенно недавно, то здесь имеется много неясных проблем, требующих своего разрешения.

Название этот метод получил от всем известного способа защиты ценных бумаг, в том числе и денег, от подделки. В отличие от обычных водяных знаков цифровые знаки могут быть не только видимыми, но и (как правило) невидимыми. Невидимые анализируются специальным декодером, который выносит решение об их корректности. Цифровые водяные знаки могут содержать некоторый аутентичный код, информацию о собственнике, либо какую-нибудь управляющую информацию. Наиболее подходящими объектами защиты при помощи цифровых водяных знаков являются неподвижные изображения, файлы аудио и видеоданных.

Технология встраивания идентификационных номеров производителей имеет много общего с технологией водяных знаков. Отличие заключается в том, что в первом случае каждая защищенная копия имеет свой уникальный встраиваемый номер (отсюда и название – дословно «отпечатки пальцев»). Этот идентификационный номер позволяет производителю отслеживать дальнейшую судьбу своего детища: не занялся ли кто-нибудь из покупателей незаконным тиражированием. Если да, то «отпечатки пальцев» быстро укажут на виновного.

Встраивание заголовков (невидимое) может применяться, например, для подписи медицинских снимков, нанесения легенды на карту и т.д. Целью является хранение разнородно представленной информации в едином целом. Это, пожалуй, единственное приложение стеганографии, где в явном виде отсутствует потенциальный нарушитель.

Наиболее существенное отличие постановки задачи скрытой передачи данных от постановки задачи встраивания ЦВЗ состоит в том, что в первом случае нарушитель должен обнаружить скрытое сообщение, тогда как во втором случае о его существовании все знают. Более того, у нарушителя на законных основаниях может иметься устройство обнаружения ЦВЗ (например, в составе DVD-проигрывателя).

Основными требованиями, которые предъявляются к водяным знакам, являются надежность и устойчивость к искажениям, они должны удовлетворять противоречивым требованиям визуальной (аудио) незаметности и робастности к основным операциям обработки сигналов.

Цифровые водяные знаки имеют небольшой объем, однако, с учетом указанных выше требований, для их встраивания используются более сложные методы, чем для встраивания просто сообщений или заголовков. Задачу встраивания и выделения цифровых водяных знаков из другой информации выполняет специальная стегосистема. Общий вид такой стегосистемы представлен на рис. 2.

Учет особенностей зрения

**Предвар**ит.

кодер

**Кодер**

Канал атаки

Выделение ЦВЗ

Детектор ЦВЗ

Декодер ЦВЗ

**Ключ К**

**ЦВЗ**

**Контейнер**

**Нет**

**Да**

**Рисунок 2 - Структурная схема типичной стегосистемы ЦВЗ**

Прежде, чем осуществить вложение цифрового водяного знака в контейнер, водяной знак должен быть преобразован к некоторому подходящему виду. Например, если в качестве контейнера выступает изображение, то и последовательность ЦВЗ зачастую представляется как двумерный массив бит. Для того, чтобы повысить устойчивость к искажениям нередко выполняют его помехоустойчивое кодирование, либо применяют широкополосные сигналы. Первоначальную обработку скрытого сообщения выполняет показанный на рис. 2 прекодер. В качестве важнейшей предварительной обработки цифрового водяного знака (а также и контейнера) назовем вычисление его обобщенного преобразования Фурье. Это позволяет осуществить встраивание ЦВЗ в спектральной области, что значительно повышает его устойчивость к искажениям. Предварительная обработка часто выполняется с использованием ключа для повышения секретности встраивания. Далее водяной знак «вкладывается» в контейнер, например, путем модификации младших значащих бит коэффициентов. Этот процесс возможен благодаря особенностям системы восприятия человека. Хорошо известно, что изображения обладают большой психовизуальной избыточностью. Глаз человека подобен низкочастотному фильтру, пропускающему мелкие детали. Особенно незаметны искажения в высокочастотной области изображений. Эти особенности человеческого зрения используются, например, при разработке алгоритмов сжатия изображений и видео.

Процесс внедрения цифровых водяных знаков также должен учитывать свойства системы восприятия человека. Стеганография использует имеющуюся в сигналах психовизуальную избыточность, но другим, чем при сжатии данных образом. Приведем простой пример. Рассмотрим полутоновое изображение с 256 градациями серого, то есть с удельной скоростью кодирования 8 бит/пиксел. Хорошо известно, что глаз человека не способен заметить изменение младшего значащего бита. Еще в 1989 году был получен патент на способ скрытого вложения информации в изображение путем модификации младшего значащего бита. В данном случае детектор стего анализирует только значение этого бита для каждого пиксела, а глаз человека, напротив, воспринимает только старшие 7 бит. Данный метод прост в реализации и эффективен, но не удовлетворяет некоторым важным требованиям к ЦВЗ.

В большинстве стегосистем для внедрения и выделения цифровых водяных знаков используется ключ. Ключ может быть предназначен для узкого круга лиц или же быть общедоступным. Например, ключ должен содержаться во всех DVD-плейерах, чтобы они могли прочесть содержащиеся на дисках ЦВЗ. Не существует, насколько известно, стегосистемы, в которой бы при выделении водяного знака требовалась другая информация, чем при его вложении.

В стегодетекторе происходит обнаружение цифрового водяного знака в (возможно измененном) защищенном ЦВЗ изображении. Это изменение может быть обусловлено влиянием ошибок в канале связи, операций обработки сигнала, преднамеренных атак нарушителей. Во многих моделях стегосистем сигнал-контейнер рассматривается как аддитивный шум. Тогда задача обнаружения и выделения стегосообщения является классической для теории связи. Однако такой подход не учитывает двух факторов: неслучайного характера сигнала контейнера и требований по сохранению его качества. Эти моменты не встречаются в известной теории обнаружения и выделения сигналов на фоне аддитивного шума. Их учет позволит построить более эффективные стегосистемы.

 Различают стегодетекторы, предназначенные для обнаружения факта наличия водяного знака и устройства, предназначенные для его выделения (стегодекодеры). В первом случае возможны детекторы с жесткими (да/нет) или мягкими решениями. Для вынесения решения о наличии/отсутствии цифрового водяного знака удобно использовать такие меры, как расстояние по Хэммингу, либо взаимную корреляцию между имеющимся сигналом и оригиналом (при наличии последнего, разумеется). А что делать, если у нас нет исходного сигнала? Тогда в дело вступают более тонкие статистические методы, основанные на построении моделей исследуемого класса сигналов.

* 1. **Атаки на стегосистемы**

Для осуществления той или иной угрозы нарушитель применяет атаки.

Наиболее простая атака – **субъективная**. Злоумышленник внимательно рассматривает изображение (слушает аудиозапись), пытаясь определить “на глаз”, имеется ли в нем скрытое сообщение. Ясно, что подобная атака может быть проведена лишь против совершенно незащищенных стегосистем. Тем не менее, она, наверное, наиболее распространена на практике, по крайней мере, на начальном этапе вскрытия стегосистемы. Первичный анализ также может включать в себя следующие мероприятия:

1. Первичная сортировка стего по внешним признакам.
2. Выделение стего с известным алгоритмом встраивания.
3. Определение использованных стегоалгоритмов.
4. Проверка достаточности объема материала для стегоанализа.
5. Проверка возможности проведения анализа по частным случаям.
6. Аналитическая разработка стегоматериалов. Разработка методов вскрытия стегосистемы.
7. Выделение стего с известными алгоритмами встраивания, но неизвестными ключами и т.д.

Из криптоанализа известны следующие разновидности атак на шифрованные сообщения :

- атака с использованием только шифртекста;

- атака с использованием открытого текста;

- атака с использованием выбранного открытого текста;

- адаптивная атака с использованием открытого текста;

- атака с использованием выбранного шифртекста.

По аналогии с криптоанализом в стегоанализе можно выделить следующие типы атак.

- **Атака на основе известного заполненного контейнера**. В этом случае у нарушителя есть одно или несколько стего. В последнем случае предполагается, что встраивание скрытой информации осуществлялось отправителем одним и тем же способом. Задача злоумышленника может состоять в обнаружении факта наличия стегоканала (основная), а также в его извлечении или определения ключа. Зная ключ, нарушитель получит возможность анализа других стегосообщений.

- **Атака на основе известного встроенного сообщения**. Этот тип атаки в большей степени характерен для систем защиты интеллектуальной собственности, когда в качестве водяного знака используется известный логотип фирмы. Задачей анализа является получение ключа. Если соответствующий скрытому сообщению заполненный контейнер неизвестен, то задача крайне трудно решаема.

- **Атака на основе выбранного скрытого сообщения**. В этом случае злоумышленние имеет возможность предлагать отправителю для передачи свои сообщения и анализировать получающиеся стего.

- **Адаптивная атака на основе выбранного скрытого сообщения**. Эта атака является частным случаем предыдущей. В данном случае злоумышленник имеет возможность выбирать сообщения для навязывания отправителю адаптивно, в зависимости от результатов анализа предыдущих стего.

- **Атака на основе выбранного заполненного контейнера**. Этот тип атаки больше характерен для систем ЦВЗ. Стегоаналитик имеет детектор стего в виде «черного ящика» и несколько стего. Анализируя детектируемые скрытые сообщения, нарушитель пытается вскрыть ключ.

У злоумышленника может иметься возможность применить еще три атаки, не имеющие прямых аналогий в криптоанализе.

- **Атака на основе известного пустого контейнера**. Если он известен злоумышленнику, то путем сравнения его с предполагаемым стего он всегда может установить факт наличия стегоканала. Несмотря на тривиальность этого случая, в ряде работ приводится его информационно-теоретическое обоснование. Гораздо интереснее сценарий, когда контейнер известен приблизительно, с некоторой погрешностью (как это может иметь место при добавлении к нему шума).

- **Атака на основе выбранного пустого контейнера**. В этом случае злоумышленник способен заставить отправителя пользоваться предложенным ей контейнером. Например, предложенный контейнер может иметь большие однородные области (однотонные изображения), и тогда будет трудно обеспечить секретность внедрения.

- **Атака на основе известной математической модели контейнера или его части**. При этом атакующий пытается определить отличие подозрительного сообщения от известной ему модели. Например допустим, что биты внутри отсчета изображения коррелированы. Тогда отсутствие такой корреляции может служить сигналом об имеющемся скрытом сообщении. Задача внедряющего сообщение заключается в том, чтобы не нарушить статистики контейнера. Внедряющий и атакующий могут располагать различными моделями сигналов, тогда в информационно-скрывающем противоборстве победит имеющий лучшую модель.

* 1. **Атаки на стегосистемы водяных знаков**

Как отмечалось ранее, водяные знаки должны удовлетворять противоречивым требованиям визуальной (аудио) незаметности и робастности к основным операциям обработки сигналов.

Возможна различная классификация атак на стегосистемы. Она была рассмотрена ранее. Теперь же рассмотрим атаки, специфичные для систем с водяными знаками. Можно выделить следующие категории атак против таких стегосистем.

1. **Атаки против встроенного сообщения** - направлены на удаление или порчу водяных знаков путем манипулирования стего. Входящие в эту категорию методы атак не пытаются оценить и выделить водяной знак. Примерами таких атак могут являться линейная фильтрация, сжатие изображений, добавление шума, выравнивание гистограммы, изменение контрастности и т.д.

2. **Атаки против стегодетектора** – направлены на то, чтобы затруднить или сделать невозможной правильную работу детектора. При этом водяной знак в изображении остается, но теряется возможность его приема. В эту категорию входят такие атаки, как аффинные преобразования (то есть масштабирование, сдвиги, повороты), усечение изображения, перестановка пикселов и т.д.

2. **Атаки против протокола использования водяного знака** – в основном связаны с созданием ложных водяных знаков, ложных стего, инверсией водяных знаков, добавлением нескольких водяных знаков и т.д..

4. **Атаки против самого водяного знака** – направлены на оценивание и извлечение водяного знака из стегосообщения, по возможности без искажения контейнера. В эту группу входят такие атаки, как атаки сговора, статистического усреднения, методы очистки сигналов от шумов, некоторые виды нелинейной фильтрации и другие.

Надо заметить, что рассматриваемая классификация атак не является единственно возможной и полной. Кроме того, некоторые атаки (например, удаление шума) могут быть отнесены к нескольким категориям.

3 **Обоснование целей и задач курсовой работы**

**Целью** данной курсовой работы является реализация программными методами одного из направлений приложений стеганографии – сокрытие сообщений в файлах формата JPEG.

Достижение этой цели возможно путем решения следующих **задач:**

* определение основных понятий стеганографии;
* выбор метода сокрытия данных;
* исследование структуры файла формата JPEG.

Программный продукт создан при помощи среды Delphi 7.0.

В целом, в задачи курсового проекта входило создание работоспособного приложения, обеспечивающего сокрытие информации произвольного размера в файле формата JPEG и доступ к уже имеющейся информации.

Как стало известно, структура формата JPEG позволяет дописывать в конец файла, после двух особых байт, означающих завершение графического изображения, информацию небольшого объема, которая не повлечет за собой особо заметного искажения изображения. Эта особенность была положена в основу реализации курсового проекта.

В настоящее время использование графических изображений в качестве стегоконтейнеров очень распространено. Это обусловлено следующими причинами:

- существованием практически значимой задачи защиты фотографий, картин, видео от незаконного тиражирования и распространения;

- относительно большим объемом цифрового представления изображений, что позволяет внедрять цифровые водяные знаки большого объема;

- заранее известным размером контейнера, отсутствием ограничений, накладываемых требованиями реального времени;

- наличием в большинстве реальных изображений текстурных областей, имеющих шумовую структуру и хорошо подходящих для встраивания информации;

- слабой чувствительностью человеческого глаза к незначительным изменениям цветов изображения, его яркости, контрастности, содержанию в нем шума, искажениям вблизи контуров;

- хорошо разработанными в последнее время методами цифровой обработки изображений.

4 **Инструкция для пользователя**

4.1 **Схема работы для пользователя**

Для начала работы с программой пользователю необходимо запустить программный продукт. Появившаяся форма предоставляет возможность выбора файла формата JPEG, с которым будет вестись работа. Если никакой документ не будет выбран, то пользователь не сможет получить доступ к остальным кнопкам формы.

Когда необходимый файл выбран, пользователь может проверить его на наличие спрятанной в нём ранее информации, нажав на кнопку «Просмотр». В случае, если в данном документе находится какая-либо информация, она будет отображена в соответствующем окне. Если сообщение достаточно крупное, то расположенная в окне просмотра полоса прокрутки позволит без затруднения увидеть весь текст до конца. Однако, нужно иметь ввиду, что чем длиннее спрятанное в файле сообщение, тем больше времени программа затратит на его обработку. Если же в данном документе отсутствует спрятанная информация, то пользователю будет выдано соответствующее сообщение.

Пользователю так же предоставляется возможность скрыть в выбранном файле свою собственную информацию. Для этого ему необходимо ввести желаемый текст в окне «Текст сообщения» и нажать на кнопку «Записать». Таким образом, введенные данные будут спрятаны в исходном документе. Стоит учесть, что попытка скрыть данные большого размера приведет к серьёзным искажениям в изображении исходного файла. Пользователь может прятать в документ с уже имеющимся сообщением другие сообщения. При этом они будут дописываться в конец уже имеющегося. Все спрятанные в файле данные можно в любой момент просмотреть, проделав вышеописанные операции.

4.2. **Установочные требования**

Для начала работы с программой пользователю достаточно просто скопировать ее с носителя на свой компьютер.

4.3.**Требования к системе**

Программные требования:

* + Delphi 7.0;

Системные требования:

* + Процессор не менее 400 МГц;
	+ место на жестком диске – не менее 400 Мб;
	+ ОС Microsoft Windows 98, 2000 или XP.
	1. **Инструкция для программиста**

В среде Delphi 7.0 был создан новый проект. В состав этого проекта входит форма ввода всех необходимых данных, а также юнит, содержащий непосредственно тело программы.

В составе программы можно выделить три основные процедуры. К ним относится процедура выбора файла, процедура просмотра сообщения, если таковое имеется внутри выбранного файла, и процедура добавления сообщения.

При нажатии пользователем кнопки «Обзор», открывается диалоговое окно, позволяющее выбрать необходимый для обработки файл. В случае, если никакой документ не будет выбран, пользователь не сможет получить доступ к остальным кнопкам формы.

При нажатии пользователем кнопки «Просмотр», происходит вызов процедуры просмотра сообщения. Выбранный файл открывается и осуществляется проверка двух последних байт в файле. Стандартные байты окончания JPEG файла имеют коды 255 и 217, и если два проверяемых байта имеют такие же значения, то выдаётся сообщение об отсутствии какой-либо скрытой информации. Если же проверяемые байты имеют отличные значения, то программа считывает по два последних байта с конца файла до тех пор, пока не обнаружит конец JPEG. Вся остальная информация является внедренной и программа считывает её по два байта, формируя строку текстового сообщения, которое по окончанию формирования отображается в окне «Текст сообщения».

При нажатии пользователем кнопки «Записать», происходит вызов процедуры добавления сообщения. Набранные в окне «Текст сообщения» данные проверяются на четность, для того чтобы обеспечить в последующем удобную запись по 2 байта за раз. Если длина сообщения нечетная, то к данной строке в конце добавляется пробел. Далее данные записываются в конец выбранного файл по два байта за раз.

**Список литературы**

1. Основные положения стеганографии –

http://www.citforum.ru/internet/securities/stegano

1. Цифровая стеганография / Сост. Грибунин В.Г., Оков И.Н., Туринцев И.В.
2. Безопасность, криминалистика, промышленный шпионаж - http://www.phreaking.ru/showpage
3. Скрытая утечка информации –

http://www.cio-world.ru/bitrix/php\_interface