# Лекция 13. Стеганография

Стеганос - секрет

## Термины и определения

**Стеганогра́фия** (от [греч.](http://ru.wikipedia.org/wiki/%D0%93%D1%80%D0%B5%D1%87%D0%B5%D1%81%D0%BA%D0%B8%D0%B9_%D1%8F%D0%B7%D1%8B%D0%BA) στεγανός — скрытый и [греч.](http://ru.wikipedia.org/wiki/%D0%93%D1%80%D0%B5%D1%87%D0%B5%D1%81%D0%BA%D0%B8%D0%B9_%D1%8F%D0%B7%D1%8B%D0%BA) γράφω — пишу, буквально «тайнопись») — это наука о скрытой передаче информации путём сохранения в тайне самого факта передачи.

В дополнение к криптографии (скрывающей **содержание** сообщения) прячет сам факт **существования** сообщения - добавляет уровень защиты.

1996 – на конференции Information Hiding: First Information Workshop приняли единую терминологию.

**Стеганографическая (стего-) система** - объединение методов и средств, используемых для создания скрытого канала для передачи информации

**Сообщение (секретное)** — передаваемая секретная информация (будь то лист с надписями молоком, голова раба или цифровой файл).

**Контейнер** - любая информация, используемая для сокрытия секретных сообщений.

**Пустой контейнер** – контейнер, не содержащий секретного сообщения

**Заполненный (стего-) контейнер** - контейнер, содержащий секретное сообщение.

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

**Стеганографический (стего-) канал** - канал передачи стегоконтейнера.

**Ключ (стегоключ)** - секретный ключ, необходимый для сокрытия сообщения в стегоконтейнере

**Стеганографические модели** — используются для общего описания стеганографических систем.

Принципы построения стегосистемы:

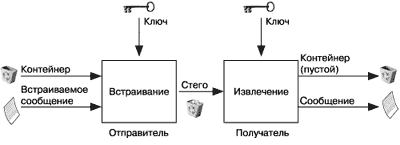
* аналитик имеет **полное представление о стеганографической системе** и деталях ее реализации
* аналитику **не известен ключ**, с помощью которого можно определить присутствие и содержание скрытого сообщения
* знание о **факте существования скрытого сообщения в одном контейнере** не позволяет извлечь сообщения в других контейнерах, пока ключ не известен
* аналитик имеет право не только читать сообщения, но и **модифицировать** их
* **начало передачи секретного** сообщения может задаваться, например, кодовым символом, который отделит часть текста письма, в которой скрыто сообщение

Требования к стегосистеме:

* Свойства контейнера должны быть модифицированы так, чтобы **изменение невозможно было выявить** (качество сокрытия внедряемого сообщения: оно не должно привлечь внимание атакующего)
* Стегосообщение должно быть **устойчиво к искажениям** (в том числе злонамеренным). Контейнер может:
  + уменьшаться или увеличиваться,
  + преобразовываться в другой формат,
  + сжиматься с использованием алгоритмов сжатия с потерей данных

Для сохранения целостности встраиваемого сообщения используют **код с исправлением ошибки** или **дублируют** сообщение.

Обобщенная модель стегосистемы:



Ключи в стегосистемах:

- **секретные** (должен быть создан или до начала обмена сообщениями, или передан по защищённому каналу)

- **открытые** (невозможно получить из него закрытый ключ)

Размер контейнера должен быть существенно больше сообщения, чтобы не вносить заметного искажения.

Цель – создание секретных средств связи: невидимые чернила, микрофотоснимки, условное расположение знаков, тайные каналы и средства связи на плавающих частотах и т. д.

Применение

- сокрытие данных

- метки (цифровые водяные знаки)

- идентификация (заголовки с метаданными)

Маркирование

## История

В средние века **распространение инквизиции** простимулировано совместное использование шифров и стеганографических методов.

XV век - монах Тритемиус (1462-1516) - описал методы скрытой передачи сообщений. В 1499 году эти записи были объединены в книгу "Steganographia".

### Покрытие сообщения

- на один носитель накладывается другой, незначащий, скрывающий основной

- нанесение сообщения на непредназначенный для этого носитель

#### Глиняные таблички

Древние [шумеры](http://ru.wikipedia.org/wiki/%D0%A8%D1%83%D0%BC%D0%B5%D1%80) использовали глиняные [клинописные](http://ru.wikipedia.org/wiki/%D0%9A%D0%BB%D0%B8%D0%BD%D0%BE%D0%BF%D0%B8%D1%81%D1%8C) таблички, в которых одна запись покрывалась слоем [глины](http://ru.wikipedia.org/wiki/%D0%93%D0%BB%D0%B8%D0%BD%D0%B0), а на втором слое писалась другая (возможно, это было повторным использованием табличек).

#### Деревянные таблички

Сообщение наносилось на деревянную дощечку, а потом она покрывалась воском. Получатель соскабливал воск, чтобы прочитать сообщение (случай передачи сообщения Демартом, который соскабливал воск с дощечек, писал письмо прямо на дереве, а потом заново покрывал дощечки воском).

#### Полоски шелка

В Китае письма писали на полосках щелка. Полоски с текстом письма, сворачивались в шарики, покрывались воском и затем глотались посыльными.

#### Голова раба

[Древнегреческий](http://ru.wikipedia.org/wiki/%D0%94%D1%80%D0%B5%D0%B2%D0%BD%D1%8F%D1%8F_%D0%93%D1%80%D0%B5%D1%86%D0%B8%D1%8F) историк [Геродот](http://ru.wikipedia.org/wiki/%D0%93%D0%B5%D1%80%D0%BE%D0%B4%D0%BE%D1%82) описал метод:

- на бритую голову [раба](http://ru.wikipedia.org/wiki/%D0%A0%D0%B0%D0%B1%D1%81%D1%82%D0%B2%D0%BE) записывается сообщение

- когда волосы отрастали, раб отправляется к [адресату](http://ru.wikipedia.org/wiki/%D0%90%D0%B4%D1%80%D0%B5%D1%81%D0%B0%D1%82)

- волосы вновь сбриваются, доставленное сообщение считывается

#### Оригинальные методы

* запись на боковой стороне колоды карт, расположенных в условленном порядке;
* запись внутри вареного яйца (смесью квасцов, чернил и уксуса на скорлупе записывается послание, выдерживается в крепком рассоле или уксусе, чтобы стравить с поверхности следы, и варится яйцо вкрутую - текст сообщения оказывается под скорлупой сверху белка);
* узелки на нитках (письменность Майя) и т. д.
* Акростихи и другие языковые игры

### Использование особых чернил

#### Симпатические чернила

Написанное такими [чернилами](http://ru.wikipedia.org/wiki/%D0%A7%D0%B5%D1%80%D0%BD%D0%B8%D0%BB%D0%B0) проявляется только при определенных условиях (нагрев, освещение, химический проявитель и т.п.)[[3]](http://ru.wikipedia.org/wiki/%D2%E0%E9%ED%EE%EF%E8%F1%FC#cite_note-gromov-2)

I век н. э. - [Филон Александрийски](http://ru.wikipedia.org/wiki/%D0%A4%D0%B8%D0%BB%D0%BE%D0%BD_%D0%90%D0%BB%D0%B5%D0%BA%D1%81%D0%B0%D0%BD%D0%B4%D1%80%D0%B8%D0%B9%D1%81%D0%BA%D0%B8%D0%B9)й[[4]](http://ru.wikipedia.org/wiki/%D2%E0%E9%ED%EE%EF%E8%F1%FC" \l "cite_note-3), - первый описал

XVII - XVIII вв. - эра "черных кабинетов" (государственных органов по перехвату, перлюстрации и дешифрованию переписки)

Имели в штате криптографов, дешифровальщиков, а также химиков (из-за активного использования невидимых чернил).

Примеры:

* Восставшие дворяне в Бордо арестовали францисканского монаха Берто (агента кардинала Мазарини). Ему разрешили написать письмо знакомому священнику в город Блэй. В конце письма религиозного содержания монах написал: "Посылаю Вам глазную мазь; натрите ею глаза и Вы будете лучше видеть". Так он и переслал скрытое сообщение, и указал способ его обнаружения. В результате монах Берто был спасен.
* 1779 год (гражданская война между южанами и северянами) - агенты северян Сэмюэль Вудхулл и Роберт Тоунсенд передавали информацию Джорджу Вашингтону, используя специальные чернила.

#### Ленин из тюрьмы

**Василий Иванович Куканов**, повесть "**У истоков грядущего**" описывает применение молока в качестве чернил для написания тайных сообщений. Изучалось в советской школьной программе.

Владимир Ленин писал молоком на бумаге между строк ([Рассказы о Ленине](http://ru.wikipedia.org/wiki/%D0%A0%D0%B0%D1%81%D1%81%D0%BA%D0%B0%D0%B7%D1%8B_%D0%BE_%D0%9B%D0%B5%D0%BD%D0%B8%D0%BD%D0%B5)) Молоко проявлялось при нагреве над пламенем.

**Царская охранка знала об этом методе** (в архиве есть документ, в котором описан способ использования таких чернил и приведен текст перехваченного сообщения революционеров).

#### Чернила с нестабильным пигментом

Через определенное время пигмент разлагается, текст становится невидимым.

[Греческий](http://ru.wikipedia.org/wiki/%D0%93%D1%80%D0%B5%D1%86%D0%B8%D1%8F) [миллионер](http://ru.wikipedia.org/wiki/%D0%9C%D0%B8%D0%BB%D0%BB%D0%B8%D0%BE%D0%BD) [Аристотель Онассис](http://ru.wikipedia.org/wiki/%D0%9E%D0%BD%D0%B0%D1%81%D1%81%D0%B8%D1%81,_%D0%90%D1%80%D0%B8%D1%81%D1%82%D0%BE%D1%82%D0%B5%D0%BB%D1%8C) несколько раз использовал при подписании контрактов ручку с симпатическими чернилами.

При использовании шариковой ручки текст можно восстановить по деформации [бумаги](http://ru.wikipedia.org/wiki/%D0%91%D1%83%D0%BC%D0%B0%D0%B3%D0%B0) - устраняется с помощью мягкого пишущего узла ([фломастер](http://ru.wikipedia.org/wiki/%D0%A4%D0%BB%D0%BE%D0%BC%D0%B0%D1%81%D1%82%D0%B5%D1%80))

### Жаргон

«Жаргонный шифр», где слова имеют другое обусловленное значение (жаргон из фильма «Джентельмены удачи»)

### Трафареты

- титры в фильме «Шерлок Холмс и Доктор Ватсон» (трафарет, наложенный на текст, оставляет видимыми только значащие буквы).

### Микроэлементы в обычных сообщениях

- микроснимки, вклеенные в письма,

- микроточки, печатаемые принтерами (позволяют идентифицировать экземпляр принтера).

#### Микроточка

Микроскопический фотоснимок (менее мм), вклеиваемый в текст писем (неосведомлённый наблюдатель **не сможет его обнаружить**, либо прочесть). Адресат читал послание с помощью [микроскопа](https://ru.wikipedia.org/wiki/%D0%9C%D0%B8%D0%BA%D1%80%D0%BE%D1%81%D0%BA%D0%BE%D0%BF).

Название получила от сходства с [типографской точкой](https://ru.wikipedia.org/wiki/%D0%A2%D0%BE%D1%87%D0%BA%D0%B0_(%D0%B7%D0%BD%D0%B0%D0%BA_%D0%BF%D1%80%D0%B5%D0%BF%D0%B8%D0%BD%D0%B0%D0%BD%D0%B8%D1%8F)).

1867 – парижский [фотограф](https://ru.wikipedia.org/wiki/%D0%A4%D0%BE%D1%82%D0%BE%D0%B3%D1%80%D0%B0%D1%84) *Dagron* разработал метод [микрофильмирования](https://ru.wikipedia.org/wiki/%D0%9C%D0%B8%D0%BA%D1%80%D0%BE%D1%84%D0%B8%D0%BB%D1%8C%D0%BC)

1870 – впервые использованы в военном деле во время [франко-прусской войны](https://ru.wikipedia.org/wiki/%D0%A4%D1%80%D0%B0%D0%BD%D0%BA%D0%BE-%D0%BF%D1%80%D1%83%D1%81%D1%81%D0%BA%D0%B0%D1%8F_%D0%B2%D0%BE%D0%B9%D0%BD%D0%B0) - [Париж](https://ru.wikipedia.org/wiki/%D0%9F%D0%B0%D1%80%D0%B8%D0%B6) был в осаде и письма посылались [голубиной почтой](https://ru.wikipedia.org/wiki/%D0%93%D0%BE%D0%BB%D1%83%D0%B1%D0%B8%D0%BD%D0%B0%D1%8F_%D0%BF%D0%BE%D1%87%D1%82%D0%B0) ([голубеграмм](https://ru.wikipedia.org/wiki/%D0%93%D0%BE%D0%BB%D1%83%D0%B1%D0%B5%D0%B3%D1%80%D0%B0%D0%BC%D0%BC%D0%B0" \o "Голубеграмма)ы) - ещё не были столь малы, как микроточки.

Микроточки для стеганографии разработаны в [Германии](https://ru.wikipedia.org/wiki/%D0%93%D0%B5%D1%80%D0%BC%D0%B0%D0%BD%D0%B8%D1%8F) между [первой](https://ru.wikipedia.org/wiki/%D0%9F%D0%B5%D1%80%D0%B2%D0%B0%D1%8F_%D0%BC%D0%B8%D1%80%D0%BE%D0%B2%D0%B0%D1%8F_%D0%B2%D0%BE%D0%B9%D0%BD%D0%B0) и [второй](https://ru.wikipedia.org/wiki/%D0%92%D1%82%D0%BE%D1%80%D0%B0%D1%8F_%D0%BC%D0%B8%D1%80%D0%BE%D0%B2%D0%B0%D1%8F_%D0%B2%D0%BE%D0%B9%D0%BD%D0%B0) мировыми войнами неким «[Professor Zapp](https://ru.wikipedia.org/wiki/%D0%A6%D0%B0%D0%BF%D0%BF,_%D0%92%D0%B0%D0%BB%D1%8C%D1%82%D0%B5%D1%80" \o "Цапп, Вальтер)», и набор шпионского оборудования для создания микроточек назывался «комплектом Zapp’а». Настоящим изобретателем был выходец из России, выпускник [Московского университета](https://ru.wikipedia.org/wiki/%D0%9C%D0%93%D0%A3) [Эммануил Голдберг](https://en.wikipedia.org/wiki/Emanuel_Goldberg)

Активно использовались во Второй мировой войне.

Развитие: вместо [галогенидов](https://ru.wikipedia.org/wiki/%D0%93%D0%B0%D0%BB%D0%BE%D0%B3%D0%B5%D0%BD%D0%B8%D0%B4%D1%8B) [серебра](https://ru.wikipedia.org/wiki/%D0%A1%D0%B5%D1%80%D0%B5%D0%B1%D1%80%D0%BE) использовали светочувствительные материалы на основе [анилина](https://ru.wikipedia.org/wiki/%D0%90%D0%BD%D0%B8%D0%BB%D0%B8%D0%BD), что усложнило поиск микроточек.

#### Идентификация микроточкой

2001 – Австралия - на важнейшие детали автомобиля в неприметных местах [лазерной](https://ru.wikipedia.org/wiki/%D0%9B%D0%B0%D0%B7%D0%B5%D1%80) гравировкой наносится метка, содержащая [Персональный идентификационный номер](https://ru.wikipedia.org/wiki/PIN-%D0%BA%D0%BE%D0%B4) или VIN

Видны в [ультрафиолетовом свете](https://ru.wikipedia.org/wiki/%D0%A3%D0%BB%D1%8C%D1%82%D1%80%D0%B0%D1%84%D0%B8%D0%BE%D0%BB%D0%B5%D1%82%D0%BE%D0%B2%D0%BE%D0%B5_%D0%B8%D0%B7%D0%BB%D1%83%D1%87%D0%B5%D0%BD%D0%B8%D0%B5) и не видны человеческому глазу.

Затрудняет угонщикам легальную продажу украденной машины в виде запчастей. Приблизительная стоимость маркировки одного автомобиля - 100-150 [австралийских долларов](https://ru.wikipedia.org/wiki/%D0%90%D0%B2%D1%81%D1%82%D1%80%D0%B0%D0%BB%D0%B8%D0%B9%D1%81%D0%BA%D0%B8%D0%B9_%D0%B4%D0%BE%D0%BB%D0%BB%D0%B0%D1%80) (75-100 [$ США](https://ru.wikipedia.org/wiki/%D0%94%D0%BE%D0%BB%D0%BB%D0%B0%D1%80_%D0%A1%D0%A8%D0%90)).

#### Метки принтера

Защита от использования принтеров для печати денежных купюр: на каждой отпечатанной странице в специальном порядке размещается группа точек (D=доли миллиметра) - модель принтера и его серийный номер, по которым можно выявить экземпляр, на котором была отпечатана банкнота

Принтеры **HP** и **Xerox** используют для этой цели **группу точек бледно-желтого цвета** - при сильном увеличении заметны на синем фоне

## Цифровые методы

**Алгоритмы изменения (дополнения) контейнера**:

* Искажение сигнала (например, метод LSB)
* «Впаивание» скрытой информации поверх оригинала (например, узкополосный сигнал накладывается на широкий диапазон частот)
* Использование особенностей формата контейнера (например, запись в [метаданные](http://ru.wikipedia.org/wiki/%D0%9C%D0%B5%D1%82%D0%B0%D0%B4%D0%B0%D0%BD%D0%BD%D1%8B%D0%B5) или в не используемые/зарезервированные поля).

### Выбор контейнера

Принципы:

- поток контейнера должен быть достаточно продолжительным всего встраиваемого сообщения

- для отметки начала и конца сообщения используют сигналы синхронизации или границ пакета

- выбираются скрывающие биты в подходящей псевдослучайной последовательности

Виды контейнеров **по протяженности**:

* непрерывные (потоковые)
* ограниченной (фиксированной) длины.

Виды стеганографии:

* **конструирующая** (контейнер создается самой стегосистемой - программа MandelSteg: контейнером является генерируемый фрактал Мандельброта)
* **селектирующая** (контейнер выбирается из некоторого множества контейнеров - генерируется большое число альтернативных контейнеров и выбирается наиболее подходящий – важна естественность контейнера)
* **безальтернативная** (контейнер поступает извне - отсутствует возможность выбора контейнера - берется первый попавшийся контейнер, не всегда подходящий к встраиваемому сообщению)

**Способы встраивания:**

- линейные (аддитивные) - линейная модификация контейнера; извлечение в декодере производится корреляционными методами,

- нелинейные - скалярное либо векторное квантование

- другие - фрактального кодирования изображений.

**Примеры аддитивных алгоритмов:**

* [А17 (Cox)](http://ru.wikipedia.org/w/index.php?title=%D0%9017_(Cox)&action=edit&redlink=1)
* А18 (Barni)
* [L18D (Lange)](http://ru.wikipedia.org/w/index.php?title=L18D_(Lange)&action=edit&redlink=1)
* А21 (J. Kim).
* [А25 (С. Podilchuk)](http://ru.wikipedia.org/w/index.php?title=%D0%9025_(%D0%A1._Podilchuk)&action=edit&redlink=1).

### Практические реализации

1. Переименовать файл
2. Приклеить скрываемый файл к другому (добавление RAR архива в конец JPEG изображения – изображение откроется в любой программе для просмотра/редактирования картинок, а также откроется в WinRar). Недостаток: легко заметить (картинка 200х200 весит 2 мегабайта)
3. Сохранение в мета данные, которые есть у всех медиа-форматов. Премущества: не нарушает формат файла, а работа с мета-данными хорошо задокументирована (есть готовые библиотеки). Недостаток: данные видно.

#### JPEG

JPEG-формат поддерживает **EXIF тэг** (данные в тэге хранятся парами ключ=значение). Можно добавить нестандартный ключ, содержащий зашифрованные данные (обычная программа, наткнувшись на этот ключ, проигнорирует его и не отобразит).

#### AVI

Файлы формата AVI поддерживают мета-данные (можно создать **свой ключ**, который будет проигнорирован программами )

Программа для просмотра мета-данных AVI файлов: [abcAvi Tag Editor](http://abcavi.kibi.ru/)

Недостаток: есть множество программ, которые отображают абсолютно полностью их содержимое, включая нестандартные значения.

#### MP3

Реализация на PHP хранении информации в тэге ID3v1([Прячем текст в MP3](http://habrahabr.ru/blogs/php/112914/)).

Тэг ID3v1 ограничен по размеру и виден проигрывателю. Тэг ID3v2.4 позволяет хранить нестандартные данные большого объема (некоторые программы хранят там настройки громкости и нормализации для каждого файла). Медиа-плееры не отображают не известные им параметры.

Тэг Lyrics3, созданный для хранения в файле текста песен..

Продвинутое хранение секретных данных в MP3 файлах (реализован в программе [MP3Stego](http://www.petitcolas.net/fabien/steganography/mp3stego/index.html), 2006):

1. данные шифруются,
2. в процесс кодирования из WAV в MP3 файл подмешиваются закодированные данные.

### Least Significant Bit (LSB)

Замена наименьших значащих битов в контейнере на биты скрываемого сообщения

Медиафайлы имеют **огромную психовизуальную избыточность**, поэтому искажение, обычно, незначительно трансфорует изображение, звук, видео и не обнаруживается визуально и на слух.

В цифровых изображениях, видео, аудио, текстурах 3D-объектов:

- использует погрешность дискретизации

- внесение искажений, которые находятся ниже порога чувствительности среднестатистического человека

Но, опытный глаз цензора с художественным образованием легко обнаружит изменение цветовой гаммы при внедрении сообщения в репродукцию "Мадонны" Рафаэля или "Черного квадрата" Малевича.

Пример:

8-битное изображение в градациях серого (256 градаций - 28): 00h (00000000b) - черный, FFh (11111111b) - белый цвет.

Кодируем сообщение из 1 байта (например, 01101011b)

Используем 2 младших бита в описаниях пикселей (потребуется 4 пикселя).

Предположим, что пиксели были черного цвета. Тогда:

|  |  |  |
| --- | --- | --- |
| № байта | Новый пиксель | Изменения пикселя |
| 1 | 00000001 | на 1/255 |
| 2 | 00000010 | 2/255 |
| 3 | 00000010 | 2/255 |
| 4 | 00000011 | 3/255 |

Такие градации незаметны для человека, и могут быть незаметны при использовании низкокачественных устройств вывода.

**Недостатки метода LSB**

- неустойчив ко всем видам атак

- применим только к контейнерам без сжатия с потерей (не применим к JPG, MP3 или AVI)

- выдает себя на изображениях с однородной поверхностью

- может использоваться только при отсутствии шума в канале передачи данных

- портит данные

**Способы обнаружения:**

- поиск аномальных характеристик распределения значений диапазона младших битов -контейнера

- большая библиотека картинок в формате BMP – это подозрительно

### Улучшение LSB

Перейти на форматы файлов с потерей, к примеру, JPEG. В отличие от LSB они более **устойчивы к геометрическим преобразованиям**. Это получается за счёт **варьирования качества сжатия изображения** в широком диапазоне – затрудняет определение вложенного сообщения

**Свойства:**

- не нарушает правила контейнера

- файл не хранит избыточную информацию

Алгоритм Коха-Жао, который прячет данные только в картинках - кодирует один бит информации в блоках 8х8 пикселей.

Реализация: [плагин для Total Commander'a](http://wincmd.ru/plugring/darkcrypttc.html) – прячет данные в контейнерах картинок и WAV (только для кодека PCM).

Пример:

Файловая система StegFS для [Linux](http://ru.wikipedia.org/wiki/Linux) скрывает данные в неиспользуемых областях [файлов](http://ru.wikipedia.org/wiki/%D0%A4%D0%B0%D0%B9%D0%BB), подменяет символы в названиях [файлов](http://ru.wikipedia.org/wiki/%D0%A4%D0%B0%D0%B9%D0%BB), текстовая стеганография и т.д.:

* зарезервированные поля [форматов файлов](http://ru.wikipedia.org/wiki/%D0%A4%D0%BE%D1%80%D0%BC%D0%B0%D1%82_%D1%84%D0%B0%D0%B9%D0%BB%D0%B0) (часть [поля расширений](http://ru.wikipedia.org/wiki/%D0%A0%D0%B0%D1%81%D1%88%D0%B8%D1%80%D0%B5%D0%BD%D0%B8%D0%B5_%D1%84%D0%B0%D0%B9%D0%BB%D0%B0), не заполненная информацией о расширении, по умолчанию заполняется нулями - можем использовать для записи данных). Недостатки - низкая скрыть и малый объем передаваемой информации.
* неиспользуемое место [гибких дисков](http://ru.wikipedia.org/wiki/%D0%93%D0%B8%D0%B1%D0%BA%D0%B8%D0%B9_%D0%B4%D0%B8%D1%81%D0%BA) ([информация](http://ru.wikipedia.org/wiki/%D0%98%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D0%B8%D1%8F) записывается в неиспользуемые части [диска](http://ru.wikipedia.org/wiki/%D0%96%D0%B5%D1%81%D1%82%D0%BA%D0%B8%D0%B9_%D0%B4%D0%B8%D1%81%D0%BA), к примеру, на нулевую дорожку). Недостатки: маленькая производительность и передача небольших сообщений.
* особые свойства полей форматов, не отображаемые на экране («невидимые» поля для получения сносок и указателей). Пример: написание черным шрифтом на черном фоне. Недостатки: маленькая производительность, небольшой объём передаваемой информации.
* особенности [файловых систем](http://ru.wikipedia.org/wiki/%D0%A4%D0%B0%D0%B9%D0%BB%D0%BE%D0%B2%D0%B0%D1%8F_%D1%81%D0%B8%D1%81%D1%82%D0%B5%D0%BC%D0%B0) (на жестком диске файл (не считая некоторых ФС, например, [ReiserFS](http://ru.wikipedia.org/wiki/ReiserFS)) занимает целое число [кластеров](http://ru.wikipedia.org/wiki/%D0%9A%D0%BB%D0%B0%D1%81%D1%82%D0%B5%D1%80) (минимальных адресуемых объемов информации). [FAT32](http://ru.wikipedia.org/wiki/FAT32) - стандартный размер кластера — 4 [Кб](http://ru.wikipedia.org/wiki/%D0%9A%D0%B8%D0%BB%D0%BE%D0%B1%D0%B0%D0%B9%D1%82). Для хранения 1 Кб на диске выделяется 4 Кб информации, из которых 3 можно использовать для хранения информации. Недостаток: лёгкость обнаружения.

### Сетевая стеганография

2003 – использование особенностей протоколов передачи данных( Кжиштоф Шчипёрски ( Krzysztof Szczypiorski ):

* **WLAN стеганография** (Wireless Local Area Networks). Пример - система HICCUPS (Hidden Communication System for Corrupted Networks). Что делает?
* **LACK (**Lost Audio Packets Steganography) **стеганография** - использует IP-телефонию (пакеты, которые задерживаются, или намеренно повреждаются игнорируются приемником, или сокрытие информации в полях заголовка, которые не используются). VoIP ( voice over IP) по протоколу RTP ( Real - Time Transport Protocol). Чрезмерно задержанные пакеты считаются посторонним приемником бесполезными и отбрасываются. Посвященный получатель вместо удаления полученных RTP пакетов, извлекает скрытую информацию

### Цифровые водяные знаки (ЦВЗ - watermarking)

Используются

- в [системах защиты авторских прав](http://ru.wikipedia.org/wiki/%D0%A2%D0%B5%D1%85%D0%BD%D0%B8%D1%87%D0%B5%D1%81%D0%BA%D0%B8%D0%B5_%D1%81%D1%80%D0%B5%D0%B4%D1%81%D1%82%D0%B2%D0%B0_%D0%B7%D0%B0%D1%89%D0%B8%D1%82%D1%8B_%D0%B0%D0%B2%D1%82%D0%BE%D1%80%D1%81%D0%BA%D0%B8%D1%85_%D0%BF%D1%80%D0%B0%D0%B2)

- для хранения идентифицирующей информации (подписи к медицинским снимкам)

- для хранения индивидуального кода изделия (для контроля дальнейшей судьбы изделия)

- для хранения управляющей информации в системах DRM (Digital rights management)

Алгоритмы встраивания метки, являющейся узкополосным сигналом, в широком диапазоне частот маркируемого контейнера:

- информация скрывается путем фазовой модуляции информационного сигнала (несущей) с псевдослучайной последовательностью чисел.

- имеющийся диапазон частот делится на несколько каналов и передача производится между этими каналами.

**Требования**:

- устойчивость к искажениям

- незаметность

- способность к восстановлению после искажений, в том числе умышленных (робастность).

Пример помехоустойчивого кодирования – для скрываемого сообщения вычисляется его обобщенное [Фурье-преобразование](http://ru.wikipedia.org/wiki/%D0%A4%D1%83%D1%80%D1%8C%D0%B5_%D0%BF%D1%80%D0%B5%D0%BE%D0%B1%D1%80%D0%B0%D0%B7%D0%BE%D0%B2%D0%B0%D0%BD%D0%B8%D0%B5)

Полухрупкий и хрупкий ЦВЗ - аналоговая [ЭП](http://ru.wikipedia.org/wiki/%D0%AD%D0%A6%D0%9F) для хранения информации о попытках нарушения целостности контейнера (канала передачи данных).

Пример

- [плагин](http://ru.wikipedia.org/wiki/%D0%9F%D0%BB%D0%B0%D0%B3%D0%B8%D0%BD) от [Digimarc](http://ru.wikipedia.org/w/index.php?title=Digimarc&action=edit&redlink=1) к [Adobe Photoshop](http://ru.wikipedia.org/wiki/Adobe_Photoshop) встраивает в изображение информацию об авторе.

Метка неустойчива - программа Stirmark созданная Fabien Petitcolas разрушает стеговложения.

### Поиск ЦВЗ

Стегодетектор - устройство для обнаружения факта существования открытого сообщения и его считывания

Используют:

- расстояние по [Хэммингу](http://ru.wikipedia.org/wiki/%D0%A5%D1%8D%D0%BC%D0%BC%D0%B8%D0%BD%D0%B3),

- взаимокорреляцию между полученным сигналом и его оригиналом

- статистические методы, строящие модели исследуемого класса сигналов.

### Аудиостеганография

**Эхо-методы** используют неравномерные промежутки между эхо-сигналами для кодирования последовательности значений. При наложении ряда ограничений соблюдается условие незаметности для человеческого восприятия.

Эхо характеризуется

- начальной амплитудой

- степенью затухания

- задержкой

При достижении некоего порога между сигналом и эхом они смешиваются и [человеческое ухо](http://ru.wikipedia.org/wiki/%D0%A3%D1%85%D0%BE) не может отличить эти сигналы.

Наличие этой точки **сложно определить**, и она **зависит от качества исходной записи** и **«слушателя»**. Чаще всего используется задержка около 1/1000, что вполне приемлемо для большинства записей и слушателей. Для обозначения бита используется две различных задержки (обе меньше порога чувствительности уха слушателя к получаемому эху).

Эхо-методы устойчивы к амплитудным и частотным атакам, но неустойчивы к [атакам](http://ru.wikipedia.org/wiki/%D0%9A%D1%80%D0%B8%D0%BF%D1%82%D0%BE%D0%B3%D1%80%D0%B0%D1%84%D0%B8%D1%87%D0%B5%D1%81%D0%BA%D0%B0%D1%8F_%D0%B0%D1%82%D0%B0%D0%BA%D0%B0) по времени.

### Фазовое кодирование

**Фазовое кодирование** (phase coding, фазовое кодирование) —замена исходного звукового элемента на относительную [фазу](http://ru.wikipedia.org/wiki/%D0%A4%D0%B0%D0%B7%D0%B0_%D0%BA%D0%BE%D0%BB%D0%B5%D0%B1%D0%B0%D0%BD%D0%B8%D0%B9), которая и является секретным сообщением. Фаза подряд идущих элементов должна быть добавлена таким образом, чтобы сохранить относительную фазу между исходными элементами. Фазовое кодирование является одним из самых эффективных методов скрытия информации.

### Метод расширенного спектра

**Метод встраивания сообщения** - специальная случайная последовательность (зачем?) встраивается в контейнер, затем, используя согласованный фильтр, данная последовательность [детектируется](http://ru.wikipedia.org/wiki/%D0%94%D0%B5%D1%82%D0%B5%D0%BA%D1%82%D0%B8%D1%80%D0%BE%D0%B2%D0%B0%D0%BD%D0%B8%D0%B5). Данный метод позволяет встраивать большое количество сообщений в контейнер, и они не будут создавать помехи друг другу. Метод заимствован из [широкополосной](http://ru.wikipedia.org/wiki/Broadband) связи.

## [Стегоанализ](http://ru.wikipedia.org/wiki/%D0%A1%D1%82%D0%B5%D0%B3%D0%BE%D0%B0%D0%BD%D0%B0%D0%BB%D0%B8%D0%B7) и атаки на стегосистемы

Попытка обнаружить, извлечь, изменить скрытое стеганографическое сообщение

### По известному заполненному контейнеру

Есть: одно или несколько стего (в случае нескольких - считается, что запись проводилось одинаковым способом).

Задача:

- обнаружить факт наличия стегоканала,

- получить доступ к нему или определить ключ

- имея ключ, раскрыть другие стегосообщения

### По известной математической модели контейнера

Есть: модель

Пример:

- биты внутри отсчета изображения [коррелированны](http://ru.wikipedia.org/wiki/%D0%9A%D0%BE%D1%80%D1%80%D0%B5%D0%BB%D1%8F%D1%86%D0%B8%D1%8F)

-> отсутствие корреляции означает наличие скрытого сообщения

Задача внедряющего сообщение: не нарушить [статистических](http://ru.wikipedia.org/wiki/%D0%A1%D1%82%D0%B0%D1%82%D0%B8%D1%81%D1%82%D0%B8%D0%BA%D0%B0) закономерностей в контейнере

### Атака на основе известного пустого контейнера

Известен пустой контейнер

Задача: сравнивая его с предполагаемым стего, установить наличие стего[канала](http://ru.wikipedia.org/wiki/%D0%9A%D0%B0%D0%BD%D0%B0%D0%BB_%D1%81%D0%B2%D1%8F%D0%B7%D0%B8).

Контейнер может быть известен с некоторой [погрешностью](http://ru.wikipedia.org/wiki/%D0%9F%D0%BE%D0%B3%D1%80%D0%B5%D1%88%D0%BD%D0%BE%D1%81%D1%82%D1%8C) (при добавлении к нему [шума](http://ru.wikipedia.org/wiki/%D0%A8%D1%83%D0%BC)).

Другие типы атак:

* по известному встроенному сообщению;
* на основе выбранного скрытого сообщения;
* атака на основе выбранного скрытого сообщения;
* на основе выбранного заполненного контейнера;
* на основе выбранного пустого контейнера;

## Предполагаемое использование террористами

Примеры использования:

- [аватар](https://ru.wikipedia.org/wiki/%D0%90%D0%B2%D0%B0%D1%82%D0%B0%D1%80%D0%B0_(%D0%BA%D0%B0%D1%80%D1%82%D0%B8%D0%BD%D0%BA%D0%B0))ки для передачи скрытых сообщений ( картинка содержит в себе сообщение «Босс сказал, что мы должны взорвать мост в полночь»). Шифрование с помощью <http://mozaiq.org/encrypt> с использованием сочетания символов «växjö» в качестве пароля.

- фотографии на [eBay](https://ru.wikipedia.org/wiki/EBay) для передачи сообщений.[[13]](https://ru.wikipedia.org/wiki/%D1%F2%E5%E3%E0%ED%EE%E3%F0%E0%F4%E8%FF#cite_note-13)

05.02. 2001[USA Today](https://ru.wikipedia.org/wiki/USA_Today) опубликовала 2 статьи «Террористы прячут инструкции онлайн»[[11]](https://ru.wikipedia.org/wiki/%D1%F2%E5%E3%E0%ED%EE%E3%F0%E0%F4%E8%FF#cite_note-11) и «Террористические группы прячутся за веб-шифрованием».[[12]](https://ru.wikipedia.org/wiki/%D1%F2%E5%E3%E0%ED%EE%E3%F0%E0%F4%E8%FF#cite_note-12)

10.07.2002 - там же опубликована статья «Боевики окутывают веб с помощью ссылок на джихад»

Автор - корреспондент [Джек Келли](https://ru.wikipedia.org/w/index.php?title=%D0%9A%D0%B5%D0%BB%D0%BB%D0%B8,_%D0%94%D0%B6%D0%B5%D0%BA_(%D0%B6%D1%83%D1%80%D0%BD%D0%B0%D0%BB%D0%B8%D1%81%D1%82)&action=edit&redlink=1) - уволен в [2004 году](https://ru.wikipedia.org/wiki/2004_%D0%B3%D0%BE%D0%B4) когда выяснилось, что данная информация сфабрикована.[[14]](https://ru.wikipedia.org/wiki/%D1%F2%E5%E3%E0%ED%EE%E3%F0%E0%F4%E8%FF#cite_note-14)

30.10.2001 - [The New York Times](https://ru.wikipedia.org/wiki/The_New_York_Times) опубликовала статью «Замаскированные сообщения террористов могут скрываться в киберпространстве»[[15]](https://ru.wikipedia.org/wiki/%D1%F2%E5%E3%E0%ED%EE%E3%F0%E0%F4%E8%FF#cite_note-15) - [Аль-Каида](https://ru.wikipedia.org/wiki/%D0%90%D0%BB%D1%8C-%D0%9A%D0%B0%D0%B8%D0%B4%D0%B0) использовала стеганографию для скрытия сообщений в изображениях, передаваемых по [электронной почте](https://ru.wikipedia.org/wiki/%D0%AD%D0%BB%D0%B5%D0%BA%D1%82%D1%80%D0%BE%D0%BD%D0%BD%D0%B0%D1%8F_%D0%BF%D0%BE%D1%87%D1%82%D0%B0) и [Usenet](https://ru.wikipedia.org/wiki/Usenet) при подготовке [терактов 11 сентября](https://ru.wikipedia.org/wiki/%D0%A2%D0%B5%D1%80%D1%80%D0%BE%D1%80%D0%B8%D1%81%D1%82%D0%B8%D1%87%D0%B5%D1%81%D0%BA%D0%B8%D0%B5_%D0%B0%D0%BA%D1%82%D1%8B_11_%D1%81%D0%B5%D0%BD%D1%82%D1%8F%D0%B1%D1%80%D1%8F_2001_%D0%B3%D0%BE%D0%B4%D0%B0).

В пособии по обучению террориста «Технологичный [муджахид](https://ru.wikipedia.org/wiki/%D0%9C%D1%83%D0%B4%D0%B6%D0%B0%D1%85%D0%B8%D0%B4), учебное пособие для [джихада](https://ru.wikipedia.org/wiki/%D0%94%D0%B6%D0%B8%D1%85%D0%B0%D0%B4)» присутствует глава, посвященная использованию стеганографии.[[16]](https://ru.wikipedia.org/wiki/%D1%F2%E5%E3%E0%ED%EE%E3%F0%E0%F4%E8%FF#cite_note-16)

### Предполагаемое использование спецслужбами

В [2010 году](https://ru.wikipedia.org/wiki/2010_%D0%B3%D0%BE%D0%B4) [Федеральное бюро расследований](https://ru.wikipedia.org/wiki/%D0%A4%D0%B5%D0%B4%D0%B5%D1%80%D0%B0%D0%BB%D1%8C%D0%BD%D0%BE%D0%B5_%D0%B1%D1%8E%D1%80%D0%BE_%D1%80%D0%B0%D1%81%D1%81%D0%BB%D0%B5%D0%B4%D0%BE%D0%B2%D0%B0%D0%BD%D0%B8%D0%B9) выяснило, что [Служба внешней разведки Российской Федерации](https://ru.wikipedia.org/wiki/%D0%A1%D0%BB%D1%83%D0%B6%D0%B1%D0%B0_%D0%B2%D0%BD%D0%B5%D1%88%D0%BD%D0%B5%D0%B9_%D1%80%D0%B0%D0%B7%D0%B2%D0%B5%D0%B4%D0%BA%D0%B8_%D0%A0%D0%BE%D1%81%D1%81%D0%B8%D0%B9%D1%81%D0%BA%D0%BE%D0%B9_%D0%A4%D0%B5%D0%B4%D0%B5%D1%80%D0%B0%D1%86%D0%B8%D0%B8) использовала специальное программное обеспечение для скрытия информации в изображениях. Данный способ использовался для связи с агентами без дипломатического прикрытия за рубежом.