Стеганография

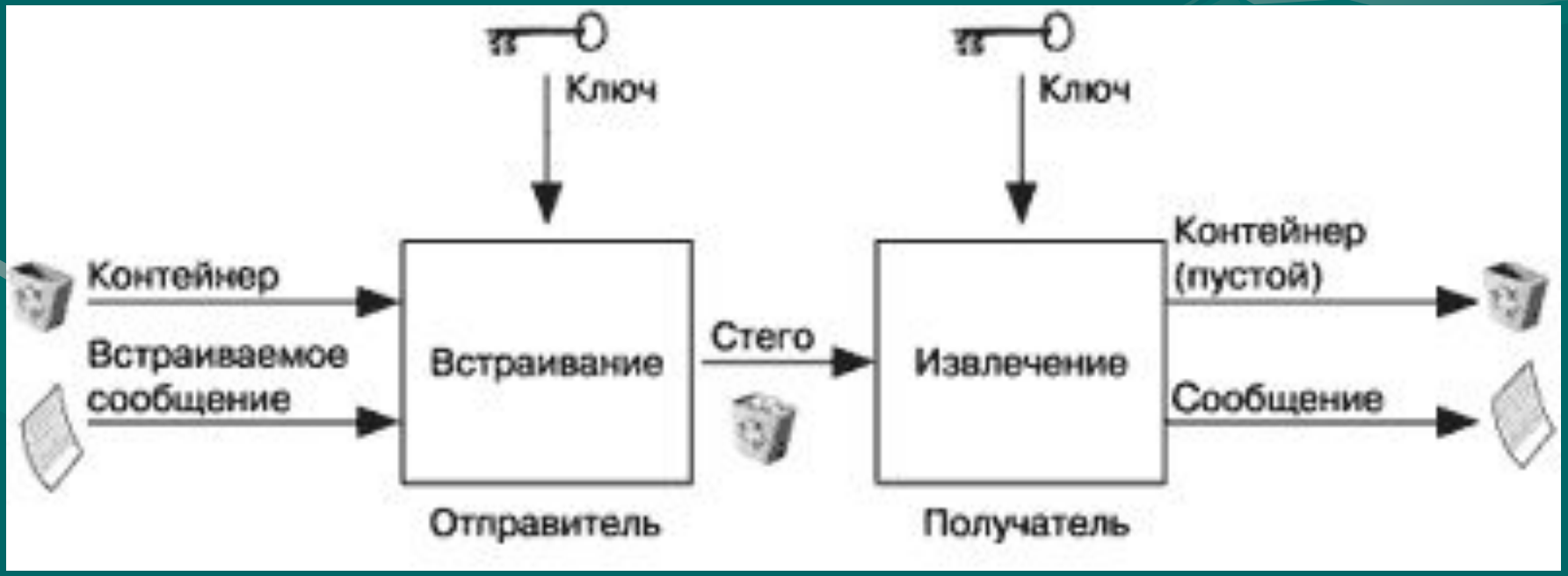
Стеганографическая система

- **Стегосистема** - совокупность средств и методов, которые используются для формирования скрытого канала передачи информации.

Положения и требования стегосистемы:

- аутентичность и целостность файла;
- предположения, что противник знает все стегометоды;
- необходимое сохранение всех свойств открыто передаваемого файла при внесении в него секретного сообщения и ключа;
- сложная вычислительная техника при извлечении сообщения противником.

Обобщенная модель стегосистемы



Содержимое стегосистемы:

- 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

Методы стеганографии

Стеганографические методы	Краткая характеристика методов	Недостатки	Преимущества
1. **Методы использования специальных свойств компьютерных форматов данных**			
1.1. Методы использования зарезервированных для расширения полей компьютерных форматов данных	Поля расширения имеются во многих мультимедийных форматах, они заполняются нулевой информацией и не учитываются программой	Низкая степень скрытности, передача небольших ограниченных объемов информации	Простота использования
1.2. Методы специального форматирования текстовых файлов:			
1.2.1. Методы использования известного смещения слов, предложений, абзацев	Методы основаны на изменении положения строк и расстановки слов в предложении, что обеспечивается вставкой дополнительных пробелов между словами	1. Слабая производительность метода,передача небольших объемов информации 2. Низкая степень скрытности	Простота использования. Имеется опубликованное программное обеспечение реализации данного метода
1.2.2. Методы выбора определенных позиций букв (нулевой шифр)	Акростих - частный случай этого метода (например, начальные буквы каждой строки образуют сообщение)		
1.2.3. Методы использования специальных свойств полей форматов, не отображаемых на экране	Методы основаны на использовании специальных "невидимых", скрытых полей для организации сносок и ссылок (например, использование черного шрифта на черном фоне)		

Методы: продолжение

1.3. Методы скрытия в неиспользуемых местах гибких дисков	Информация записывается в обычно неиспользуемых местах ГМД (например, в нулевой дорожке)	1. Слабая производительность метода, передача небольших объемов информации 2. Низкая степень скрытности	Простота использования. Имеется опубликованное программное обеспечение реализации данного метода
1.4. Методы использования имитирующих функций (mimic-function)	Метод основан на генерации текстов и является обобщением акростиха. Для тайного сообщения генерируется осмысленный текст, скрывающий само сообщение	1. Слабая производительность метода, передача небольших объемов информации 2. Низкая степень скрытности	Результирующий текст не является подозрительным для систем мониторинга сети
1.5. Методы удаления идентифицирующего файл заголовка	Скрываемое сообщение шифруется и у результата удаляется идентифицирующий заголовок, оставляя только шифрованные данные. Получатель заранее знает о передаче сообщения и имеет недостающий заголовок	Проблема скрытия решается только частично. Необходимо заранее передать часть информации получателю	Простота реализации. Многие средства (White Noise Storm, S-Tools), обеспечивают реализацию этого метода с PGP шифроалгоритмом

Методы: продолжение

2. **Методы использования избыточности аудио и визуальной информации**			
2.1. Методы использования избыточности цифровых фотографии, цифрового звука и цифрового видео	Младшие разряды цифровых отсчетов содержат очень мало полезной информации. Их заполнение дополнительной информацией практически не влияет на качество восприятия, что и дает возможность скрытия конфиденциальной информации	За счет введения дополнительной информации искажаются статистические характеристики цифровых потоков. Для снижения компрометирующих признаков требуется коррекция статистических характеристик	Возможность скрытой передачи большого объема информации. Возможность защиты авторского права, скрытого изображения товарной марки, регистрационных номеров и т.п.

Основные задачи стеганографии

1. Защита конфиденциальной информации от несанкционированного доступа;
2. Преодоление систем мониторинга и управления сетевыми ресурсами;
3. Камуфлирования программного обеспечения;
4. Защита авторского права на некоторые виды интеллектуальной собственности.

обзор стеганографических программ

Операционная среда Windows

- **Steganos for Win95** — является легкой в использовании, но все же мощной программой для шифрования файлов и скрытия их внутри BMP, DIB, VOC, WAV, ASCII, HTML — файлов.
- **Contraband** — программное обеспечение, позволяющее скрывать любые файлы в 24 битовых графических файлах формата BMP.

Операционная среда DOS

- **Jsteg** — программа предназначена для скрытия информации в популярном формате JPG.
- **FFEncode** — интересная программа, которая скрывает данные в текстовом файле. Программа запускается с соответствующими параметрами из командной строки.
- **StegoDos** — пакет программ, позволяющий выбирать изображение, скрывать в нем сообщение, отображать и сохранять изображение в другом графическом формате.
- **Wnstorm** — пакет программ, который позволяет шифровать сообщение и скрывать его внутри графического файла PCX формата.

Операционная среда OS/2

- **Hide4PGP v1.1** — программа позволяет прятать информацию в файлах формата BMP, WAV и VOC, при этом для скрытия можно использовать любое число самых младших битов.
- **Texto** — стеганографическая программа, преобразующая данные в английский текст.
- **Wnstorm** — аналогична программе для DOS. Для ПК Macintosh
- **Stego** — позволяет внедрять данные в файлы формата PICT без изменения внешнего вида и размера PICT -файла.
- **Paranoid** — эта программа позволяет шифровать данные по алгоритмам IDEA и DES, а затем скрывать файл в файле звукового формата.

Дестеганография – метод выявления секретной информации

Простые методы дестеганографии заключаются в следующем: для начала нужно найти все места возможных закладок инородной информации, которые допускает формат файла-контейнера. Далее требуется извлечь данные из этих мест и проанализировать их свойства на соответствие стандартным значениям.

Дестеганографические программы

- **Stegdetect** весьма эффективен против большого числа стеганографических программ: JSTEG, JPHS, Gifshuffle, Hide-and-Seek, Steganos.
- **FTK Imager** позволяет быстро создать образ жесткого диска для последующего изучения, а также на лету просмотреть файлы MS Office, архивов или изображений.
- **Stego Suite- а**втоматический программный сканер, содержащий 9 стеганографических алгоритмов детектирования, рассчитанных на все общие типы файлов цифрового изображения и аудио файлов.
- **File Signature Header** позволяет не только определить принадлежность какого-либо файла, но и зачастую идентифицировать программу, его создавшую, или заострить внимание на каких-либо файлах (в рамках конкретного дела).

А также

- **ProDiscover**
- **Ilook Investigator**
- **Maresware Forensic Suite**
- **Paraben E-mail Examiner**

Последний аккорд

Стеганография – один из самых увлекательных и эффективных методов сокрытия данных, которые использовались за всю историю человечества. В настоящее время компьютерная стеганография продолжает развиваться. Главной причиной этого процесса является лавинообразное развитие компьютерной сети общего пользования Internet, в том числе такие нерешенные противоречивые проблемы Internet, как защита авторского права, защита прав на личную тайну, организация электронной торговли, противоправная деятельность хакеров, террористов, принятые в ряде стран ограничения на использование сильной криптографии.

- Чем больше человек знает о методах стеганографии, тем больше у него шансов не попасть впросак.