Барсуков Вячеслав Сергеевич, кандидат технических наук
Романцов Андрей Петрович

КОМПЬЮТЕРНАЯ СТЕГАНОГРАФИЯ ВЧЕРА, СЕГОДНЯ, ЗАВТРА. Технологии информационной безопасности 21 века.

Задача надежной защиты информации от несанкционированного доступа является одной из древнейших и не решенных до настоящего времени проблем. Способы и методы скрытия секретных сообщений известны с давних времен, причем, данная сфера человеческой деятельности получила название **стеганография.** Это слово происходит от греческих слов steganos (секрет, тайна) и graphy (запись) и, таким образом, означает буквально "тайнопись", хотя методы стеганографии появились, вероятно, раньше, чем появилась сама письменность (первоначально использовались условные знаки и обозначения).

В дальнейшем для защиты информации стали использоваться более эффективные на время создания методы кодирования и криптографии.

Как известно, цель криптографии состоит в блокировании несанкционированного доступа к информации путем шифрования содержания секретных сообщений. Стеганография имеет другую задачу, и ее цель — скрыть сам факт существования секретного сообщения. При этом, оба способа могут быть объединены и использованы для повышения эффективности защиты информации (например, для передачи криптографических ключей).

Как и любые инструменты, стеганографические методы требуют к себе внимания и осторожного обращения, так как могут быть использованы как для целей защиты, так и для целей нападения. В данной статье на базе анализа открытых информационных источников рассматриваются возможности стеганографии применительно к проблеме защиты информации.

1. Стеганография вчера

Первые следы стеганографических методов теряются в глубокой древности. Так, например, общеизвестно, что в древней Греции тексты писались на дощечках, покрытых воском. Во избежание попадания сообщения к противнику, использовали следующее ухищрение. Соскабливали воск с дощечек, писали сообщение прямо на поверхности дерева, потом снова покрывали дощечку воском. Таблички выглядели без изменений и потому не вызывали подозрений.

Хорошо известны различные способы скрытого письма между строк обычного не защищаемого письма: от применения молока до использования сложных химических реакций с последующей обработкой при чтении.

Другие методы стеганографии включают использование микрофотоснимков, незначительные различия в написании рукописных символов, маленькие проколы определенных напечатанных символов и множество других способов по скрытию истинного смысла тайного сообщения в открытой переписке.

2. Компьютерная стеганография сегодня

Компьютерные технологии придали новый импульс развитию и совершенствованию стеганографии, появилось новое

Компьютерные технологии придали новый импульс развитию и совершенствованию стеганографии, появилось новое направление в области защиты информации — **компьютерная стеганография** (КС).

Современный прогресс в области глобальных компьютерных сетей и средств мультимедиа привел к разработке новых методов, предназначенных для обеспечения безопасности передачи данных по каналам телекоммуникаций и использования их в необъявленных целях. Эти методы, учитывая естественные неточности устройств оцифровки и избыточность аналогового видео или аудио сигнала, позволяют скрывать сообщения в компьютерных файлах (контейнерах). Причем, в отличие от криптографии, данные методы скрывают сам факт передачи информации.

2.1.Основные принципы компьютерной стеганографии и области её применения

К. Шеннон дал нам общую теорию тайнописи, которая является базисом стеганографии как науки. В современной компьютерной стеганографии существует два основных типа файлов: сообщение— файл, который предназначен для скрытия, и контейнер—файл, который может быть использован для скрытия в нем сообщения. При этом контейнеры бывают двух типов. Контейнер—оригинал (или "Пустой" контейнер) — это контейнер, который не содержит скрытой информации. Контейнер—результат (или "Заполненный" контейнер) — это контейнер, который содержит скрытую информацию. Под ключом понимается секретный элемент, который определяет порядок занесения сообщения в контейнер.

Основными положениями современной компьютерной стеганографии являются следующие:

1. Методы скрытия должны обеспечивать **аутентичность и целостность** файла.

2. Предполагается, что противнику полностью известны возможные стеганографические методы.

3. Безопасность методов основывается на **сохранении** стеганографическим преобразованием основных **свойств** открыто передаваемого файла при внесении в него секретного сообщения и некоторой неизвестной противнику информации — ключа.

4. Даже если факт скрытия сообщения стал известен противнику через сообщника, извлечение самого секретного сообщения представляет сложную вычислительную задачу.

В связи с возрастанием роли глобальных компьютерных сетей становится все более важным значение стеганографии. Анализ информационных источников компьютерной сети Internet позволяет вделать вывод, что в настоящее время стеганографические системы активно используются для решения следующих основных задач:

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.

Остановимся подробнее на каждой из перечисленных задач.

Защита конфиденциальной информации от несанкционированного доступа

Это область использования КС является наиболее эффективной при решении проблемы защиты конфиденциальной информации. Так, например, только одна секунда оцифрованного звука с частотой дискретизации 44100 Гц и уровнем

информации. Так, например, только одна секунда оцифрованного звука с частотой дискретизации 44100 Гц и уровнем отсчета 8 бит в стерео режиме позволяет скрыть за счет замены наименее значимых младших разрядов на скрываемое сообщение около 10 Кбайт информации. При этом, изменение значений отсчетов составляет менее 1 %. Такое изменение практически не обнаруживается при прослушивании файла большинством людей.

Преодоление систем мониторинга и управления сетевыми ресурсами

Стеганографические методы, направленные на противодействие системам мониторинга и управления сетевыми ресурсами промышленного шпионажа, позволяют противостоять попыткам контроля над информационным пространством при прохождении информации через серверы управления локальных и глобальных вычислительных сетей.

Камуфлирование программного обеспечения (ПО)

Другой важной задачей стеганографии является камуфлирование ПО. В тех случаях, когда использование ПО незарегистрированными пользователями является нежелательным, оно может быть закамуфлировано под стандартные универсальные программные продукты (например, текстовые редакторы) или скрыто в файлах мультимедиа (например, в звуковом сопровождении компьютерных игр).

Защита авторских прав

Еще одной областью использования стеганографии является защита авторского права от пиратства. На компьютерные графические изображения наносится специальная метка, которая остается невидимой для глаз, но распознается специальным ПО. Такое программное обеспечение уже используется в компьютерных версиях некоторых журналов. Данное направление стеганографии предназначено не только для обработки изображений, но и для файлов с аудио- и видеоинформацией и призвано обеспечить защиту интеллектуальной собственности.

2.2. Обзор известных стеганографическшх методов.

В настоящее время методы компьютерной стеганографии развиваются по двум основным направлениям:

1. Методы, основанные на использовании специальных свойств компьютерных форматов;
2. Методы, основанные на избыточности аудио и визуальной информации.

Сравнительные характеристики существующих стеганографических методов приведены в табл. 1.

Таблица 1. Сравнительные характеристики стеганографических методов

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			

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)		
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
2. Методы использования избыточности аудио и визуальной информации			
2.1. Методы использования	Младшие разряды цифровых отсчетов	За счет введения	Возможность скрытой

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.

Как видно из табл. 1, первое направление основано на использовании специальных свойств компьютерных форматов представления данных, а не на избыточности самих данных. Специальные свойства форматов выбираются с учетом защиты скрываемого сообщения от непосредственного прослушивания, просмотра или прочтения. На основании анализа материалов табл. 1 можно сделать вывод, что основным направлением компьютерной стеганографии является использование избыточности аудио и визуальной информации. Цифровые фотографии, цифровая музыка, цифровое видео — представляются матрицами чисел, которые кодируют интенсивность в дискретные моменты в пространстве и/или во времени. Цифровая фотография — это матрица чисел, представляющих интенсивность света в определенный момент времени. Цифровой звук — это матрица чисел, представляющая интенсивность звукового сигнала в последовательно идущие моменты времени. Все эти числа не точны, т.к. не точны устройства оцифровки аналоговых сигналов, имеются шумы квантования. Младшие разряды цифровых отсчетов содержат очень мало полезной информации о текущих параметрах звука и визуальнного образа. Их заполнение ощутимо не влияет на качество восприятия, что и дает возможность для скрытия дополнительной информации.

Графические цветные файлы со схемой смешения RGB кодируют каждую точку рисунка тремя байтами. Каждая такая точка состоит из аддитивных составляющих: красного, зеленого, синего. Изменение каждого из трех наименее значимых бит приводит к изменению менее 1% интенсивности данной точки. Это позволяет скрывать в стандартной графической картинке объемом 800 Кбайт около 100 Кбайт информации, что не заметно при просмотре изображения.

Другой пример. Только одна секунда оцифрованного звука с частотой дискретизации 44100 Гц и уровнем отсчета 8 бит в стерео режиме позволяет скрыть за счет замены наименее значимых младших разрядов на скрываемое сообщение около 10 Кбайт информации. При этом изменение значений отсчетов составляет менее 1%. Такое изменение практически не обнаруживается при прослушивании файла большинством людей.

2.3. Краткий 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. Для удобства использования программа выполнена в виде мастера. Это 32-разрядное приложение содержит собственный Shredder — программу, которая уничтожает файлы с жесткого диска. С новыми свойствами и дополнительными возможностями Steganos for Win95 является серьезным

с жесткого диска. С новыми свойствами и дополнительными возможностями Steganos for Win95 является серьезным конкурентом на рынке информационной безопасности для скрытия 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. Текстовые файлы-контейнеры после преобразования не содержат какого-либо смысла, но достаточно близки к нормальному тексту, чтобы пройти примитивную проверку.

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.

Информационные источники использованных материалов сети Internet приведены в табл.2.

Таблица 2. Информационные источники материалов по стеганографии в сети Интернет

Программное обеспечение (включая исходные тексты программ):	
1.	www.demcom.com/english/steganos
2.	www.cypher.net
3.	www.rugeley.demon.co.uk
4.	ftp.funet.fi/pub/crypt/steganography
5.	www.stego.com

5.	www.stego.com
6.	www.netlink.co.uk
7.	ftp.crl.com
История развития стеганографии, описание основных принципов, материалы конференций, библиография:	
1.	www.cl.cam.ac.uk (University of Cambridge Computer Laboratory)
2.	www.patriot.net
3.	www.lanl.gov
4.	www.iquest.net
5.	www.cs.hut.fi

3. Компьютерная стеганография завтра

Анализ тенденций развития КС показывает, что в ближайшие годы интерес к развитию методов КС будет усиливаться всё больше и больше. Предпосылки к этому уже сформировались сегодня. В частности, общеизвестно, что актуальность проблемы информационной безопасности постоянно растет и стимулирует поиск новых методов защиты информации (ЗИ). С другой стороны, бурное развитие информационных технологий обеспечивает возможность реализации этих новых методов ЗИ. И/конечно/сильным катализатором 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 и т.п.

Весьма характерной тенденцией в настоящее время в области ЗИ является внедрение криптологических методов. Однако на этом пути много ещё нерешенных проблем, связанных с разрушительным воздействием на криптосредства таких составляющих информационного оружия как компьютерные вирусы, логические бомбы, автономные репликативные программы и т.п. Объединение методов компьютерной стеганографии и криптографии явилось бы хорошим выходом из создавшегося положения. В этом случае удалось бы устранить слабые стороны известных методов защиты информации и разработать более эффективные новые нетрадиционные методы обеспечения информационной безопасности.