3. Robinson Ph., Stephenson B. - "TCO-aware provisioning of information security infrastructure" HP Labs, http://www.hpl.hp.com/techreports/2008/HPL-2008-195.pdf
4. Полякова М. - "ИТ и деньги"; http://www.osp.ru/titles/cw/article/article_9491929.html

ОСОБЕННОСТИ ИСПОЛЬЗОВАНИЯ И ПЕРСПЕКТИВЫ КОМПЬЮТЕРНОЙ СТЕГАНОГРАФИИ

Константин Андроник, Василий Власов
Славянский университет (Республика Молдова)

Some modern possibilities of use computer стеганографии for the decision of problems of information safety are considered. Development prospects are defined.

Компьютерные технологии придали новый импульс развитию и совершенствованию стеганографии (от греческого «тайнопись»), 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].

Основными положениями современной компьютерной стеганографии являются следующие [1, 3]:

I. Методы скрытия должны обеспечивать аутентичность и целостность файла.

II. Предполагается, что противнику известны все возможные стеганографические методы.

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

IV. Даже если факт скрытия сообщения стал известен противнику

через сообщника, извлечение самого секретного сообщения представляет сложную вычислительную задачу.

Анализ информационных источников компьютерной сети Internet позволяет сформулировать перечень предметных областей использования стеганографических систем:

1. Защита конфиденциальной информации от несанкционированного доступа. 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 [1].

2. Преодоление систем мониторинга и управления сетевыми ресурсами промышленного шпионажа. Стеганографические методы позволяют противостоять попыткам контроля над информационным пространством при прохождении информации через серверы управления локальных и глобальных вычислительных сетей [2].

3. Камуфлирование программного обеспечения (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) [4 - 8].

4. Защита авторских прав от пиратства - использование стеганографии позволяет наносить на компьютерные графические изображения специальную метку, которая остается невидимой для глаз, но распознается специальным ПО. Такое программное обеспечение уже используется в компьютерных версиях некоторых журналов и предназначено не только для обработки изображений, но и для файлов с аудио- и видеоинформацией и призвано обеспечить защиту интеллектуальной собственности [3].

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 пользо-

вания 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.

В последние годы в связи с интенсивным развитием мультимедийных технологий очень остро встал вопрос защиты авторских прав и интеллектуальной собственности, представленной в цифровом виде. Особенно актуальной эта проблема стала с развитием общедоступных компьютерных сетей, в частности, сети Internet. С учетом этого в настоящее время задачи защиты от копирования и обеспечения аутентификации решаются, помимо мер организационно-юридического характера, с использованием технологий цифровых водяных знаков (ЦВЗ). Необходимо отметить, что наибольшие достижения стеганографии в прошедшем десятилетии были достигнуты именно в области развития цифровых водяных знаков. Эти достижения вызваны реакцией общества на актуальнейшую проблему защиты авторских прав в условиях общедоступных компьютерных сетей.

Проводя подробный анализ стеганографических программ, нельзя не отметить, что в настоящее время на рынке широко представлены следующие программы и приложения: DiSi-Steganograph (DOS-приложение, прячет данные в графических файлах PCX); StegoDOS (DOS, графические форматы); Gif-It-Up (Win95, прячет данные в Gif-файлах); EZStego (Java-приложение, метод LSB для форматов GIF и PICT); Contraband (Win95, формат BMP); FFEncode (DOS, формат ASCII); Isteg (DOS, JPEG); Steganography Tools 4 (шифрует информацию алгоритмами DEA, MPJ2, DES, TripleDES, NSEA и затем прячет ее в графических и звуковых файлах, а также в секторах дисков); Winstorm (DOS, OS/2, PCX) и др. [5 - 8].

Таким образом, в настоящее время одна из наиболее древних наук стеганография становится основой для создания перспективных систем

защиты информации, оперативно-технические характеристики которых определяются новыми информационными технологиями. Сегодня стеганография позволяет не только успешно решать основную задачу – скрытно передавать информацию, но и решать целый ряд других актуальнейших задач, в том числе, помехоустойчивой аутентификации, защиты от несанкционированного копирования, мониторинга информации в сетях связи, поиска информации в мультимедийных базах данных и др.

Литература:

1. Грибунин В.Г. и др. Цифровая стеганография. - М.: СОЛОН-Пресс, 2002. - 299 с.
2. Карасев Андрей. Компьютерная тайнопись – графика и звук приобретают подтекст. – //Мир ПК. - № 1/2007. – С.132-134.
3. Специальная техника//№№ 5/1998, 6/1999, 6/2000, 3/2002.
4. Тигулев Максим. Стегонозавр или тайнопись на компьютере. - //Internet журнал http://www.gagin.ru/internet/8/12.html
5. Privacy Guide: Steganography. http://www.all-nettools.com/privacy/stegano.htm
6. http://www.citforum.ru/internet/securities/stegano.shtml
7. http://www.securitylab.ru/analytics/216270.php
8. http://st.ess.ru/publications/articles/steganos/steganos.htm

ПРОБЛЕМЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ И РОЛЬ ЧЕЛОВЕКА В ИНФОРМАЦИОННОЙ СИСТЕМЕ

Александр Каминский,
эксперт (Республика Молдова)

This work describes the global and local problems of information security, as well as man's role in the common information system.

Централизация знаний и информации происходит на высших уровнях. Идеи и мысли, всё тщательным образом отфильтровывается и обрабатывается, сохраняется и используется для управления низшими звеньями. Тут, применимо высказывание, принадлежащее философу Френсису Бэкону, которое в своё время употребили и приме-