ВОЕННО-КОСМИЧЕСКАЯ АКАДЕМИЯ имени А.Ф.МОЖАЙСКОГО
Кафедра математического и программного обеспечения

УТВЕРЖДАЮ
Начальник 27 кафедры
полковник
С. Войцеховский
«___» _____ 20__ г.

Автор: доцент 27 кафедры
кандидат технических наук
подполковник С.Краснов

Лекция № 8
по учебной дисциплине
«Защита информации»
на тему

Тема: «СТЕГАНОГРАФИЧЕСКИЕ МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ»

по дисциплине: «Защита информации»

Рассмотрено и одобрено
на заседании кафедры № 27
« ___ » августа 202__ г.
протокол № __

Санкт-Петербург 202_

Содержание занятия и время

Введение – 5 мин.

Учебные вопросы (основная часть):

1. Введение в цифровую стеганографию – 30 мин.
2. Стеганографические методы защиты информации – 20 мин.
3. Состав и основные принципы работы стегосистемы ЦВЗ. Области применения стеганографии – 30мин.

Заключение – 3-5 мин.

Литература:

Основная:

1. Войцеховский С.В., Воробьёв Е.Г. Методы и средства защиты компьютерной информации: учебно-методическое пособие. – СПб.: ВКА имени А.Ф. Можайского 2013. – 134 с.
2. Воробьев Е.Г. Защита информации в автоматизированных системах военного назначения. Учебное пособие – СПб, ВКА им.А.Ф. Можайского, 2007. – 252 с.

Дополнительная:

1. Вихорев С.В. Классификация угроз информационной безопасности. - http://www2.cnews.ru/comments/security/elvis_class.shtml
2. Войцеховский С.В., Марковский А.С., Палагушин В.А. Защита информации в автоматизированных системах. / Под ред. профессора Хомоненко А.Д. – Спб.:НТЦ им. Л.Т. Тучкова, 2005. – 149 с.

Материально техническое обеспечение:

1. Технические средства обучения: ПЭВМ, мультимедиа проектор, экран, программное обеспечение.
2. Приложения (слайды).
3. Наглядные средства обучения – доска, мел.

Организационно-методические указания:

Цель лекции: *Дать знания в области стеганографических методов защиты информации.*

Во введении сформулировать тему лекции, цель и название изучаемых вопросов. При этом произвести опрос курсантов по пройденному материалу.

Применяемым методическим приемом является рассказ.

В основной части сконцентрировать внимание курсантов на стеганографических методах ЗИ.

В заключительной части обобщить изложенный материал и осуществить контрольный опрос.

1. Перечислите основные стеганографические методы ЗИ?
2. В чем заключается суть стеганографических методов ЗИ?
3. Что такое контейнер?
4. Что такое стегоключ или просто ключ?

Отвечаю на вопросы по теме занятия, даю задание на самостоятельную подготовку.

Лекция № 8

«Стеганографические методы защиты информации»

В. 1. Введение в цифровую стеганографию.

Суть *стеганографического метода* защиты информации заключается в том, что скрываемое сообщение встраивается в некоторый безобидный, не привлекающий внимания объект, который затем открыто, транспортируется адресату.

Методы стеганографии позволяют скрыть не только смысл хранящейся или передаваемой информации, но и сам факт существования, хранения или передачи закрытой информации. В компьютерных системах практическое использование стеганографии только начинается, но проведенные исследования показывают ее перспективность. В основе всех методов стеганографии лежит маскирование закрытой информации среди открытых файлов. Обработка мультимедийных файлов в АС открыла практически неограниченные возможности перед стеганографией.

Местом зарождения стеганографии многие называют Египет, хотя первыми "стеганографическими сообщениями" можно назвать и наскальные рисунки древних людей.

Само слово «стеганография» имеет греческие корни. 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). Исторически это направление появилось первым, но затем во многом было вытеснено криптографией. Тайнопись осуществляется самыми различными способами. 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! Первое упоминание о стеганографических методах в литературе приписывается Геродоту, который описал случай передачи сообщения Демартом, который соскабливал воск с дощечек, писал письмо прямо на дереве, а потом заново покрывал дощечки воском.

Другой эпизод, который относят к тем же временам - передача послания с использованием головы раба. Для передачи тайного сообщения голову раба обривали, наносили на кожу татуировку, и когда волосы отрастали, отправляли с посланием. В Китае письма писали на полосках щелка. Поэтому для сокрытия сообщений, полоски с текстом письма, сворачивались в шарики, покрывались воском и затем глотались посыльными.

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, например, 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 применявшаяся Германией во время мировых войн. "Крапление карт шулерами - тоже пример стеганографии.

Во время Второй мировой войны правительство США придавало большое значение борьбе против тайных методов передачи информации. Были введены ограничения на почтовые отправления: так, не принимались письма и телеграммы, содержащие кроссворды, ходы шахматных партий, детские рисунки, инструкции по вязанию, 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. Все это делалось для того, чтобы помешать передаче скрытых сообщений.

Развитие средств вычислительной техники в последнее десятилетие дало новый толчок развитию компьютерной стеганографии. Сообщения встраивают теперь в цифровые данные, как правило, имеющие аналоговую природу — речь, аудиозаписи, изображения, видео и даже текстовые файлы и исполняемые файлы программ.

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 скрытие 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 контролировать его использование.

В. 2. Стеганографические методы защиты информации.

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 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 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 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.

Кроме вышеперечисленных методов ряд авторов в своих работах ([3], [11]) называют и другие методы стеганографии. Из них наибольшую известность получили следующие:

- встраивание цифровых водяных знаков (ЦВЗ) (watermarking);
- встраивание идентификационных номеров (fingerprinting);
- встраивание заголовков (captioning).

Методы ЦВЗ 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 так далее. 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.

Одно из наиболее эффективных технических средств защиты мультимедийной информации и заключается во встраивании в защищаемый объект невидимых меток ЦВЗ. Разработки в этой области ведут крупнейшие фирмы во всем мире.

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

Рассмотрим применение этого метода подробнее. В 2003 году на конференции ISDEF 2003 (Independent Software Developers Forum) представителем компании FastReport, Inc. был сделан доклад о разработанной и успешно применяемой системе защиты программ, распространяемых в исходных кодах, методами стеганографии[11].

Основная идея защиты заключается в том, что каждому покупателю передается уникальный набор исходных текстов, но скомпилированные из любого такого набора программы работают совершенно одинаково.

Перед отправкой исходных текстов покупателю в них с помощью специального стеганографического алгоритма добавляется некоторый скрытый идентификатор, связанный с личностью пользователя. Если один из файлов окажется в свободном доступе в Интернете, то с помощью обратного алгоритма разработчики смогут извлечь идентификатор пользователя, а значит, определить и наказать виновного.

Для размещения идентификатора без изменения функциональности программы применяется более 10 различных приемов:

- изменение регистра букв (для языков, не различающих прописные и строчные буквы, например Delphi);
- изменение локальных идентификаторов;
- изменение порядка следования функций;
- взаимная замена пробелов и символов табуляции;
- изменение стиля отступов для блоков кода (begin/end, {/});
- изменение стиля расстановки пробелов до и после скобок;
- вставка пробелов в конце строк;
- вставка пустых строк;
- изменение порядка операторов case внутри switch.

Представитель FastReport в своем докладе отметил, что после введения подобной защиты и лишения поддержки нескольких пользователей, уличенных в нарушении лицензии на использование исходных текстов, новые версии программ перестали появляться в открытом доступе. Также было сказано, что переформатирование исходного текста не приводит к полному разрушению идентификатора, т. е. стеганографическая вставка обладает достаточно высокой живучестью.

Почти все используемые в настоящее время офисные форматы (а именно они преимущественно используются в деловом документообороте) позволяют легко добавлять информацию, которая не повлияет на представление или печать документов.

Метод встраивания идентификационных номеров производителей имеет много общего с технологией ЦВЗ. Отличие заключается в том, что в данном 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.

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

В. 3. Состав и основные принципы работы стегосистемы ЦВЗ.

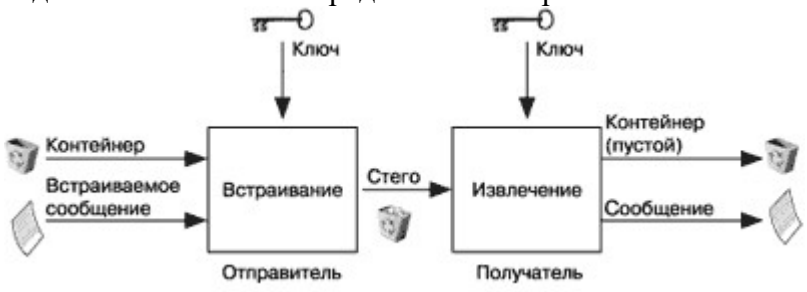
Цифровая стеганография – наука о незаметном и надежном скрытии одних битовых последовательностей в других, имеющих аналоговую природу. В этом определении содержится два главных требования к стеганографическому преобразованию: незаметность и надежность, то есть устойчивость к различного рода искажениям. Упоминание об аналоговой природе цифровых данных подчеркивает тот факт, что встраивание информации производится в оцифрованные непрерывные сигналы. Таким образом, в рамках цифровой стеганографии не рассматриваются вопросы внедрения данных в заголовки IP-пакетов и файлов различных форматов в текстовые сообщения.

Как бы ни были различны направления стеганографии, предъявляемые ими требования во многом совпадают. 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).

Слово «незаметном» в определении цифровой стеганографии подразумевает обязательное включение человека в систему стеганографической передачи данных. Человек здесь может рассматриваться как дополнительный приемник данных, предъявляющий к системе передачи достаточно трудно формализуемые требования.

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.

Обобщенная **модель стегосистемы** представлена на рис. 1.



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. В качестве стеганографического контейнера может выступать почти все что угодно: газетная заметка, точка в конце предложения, картинка и даже лист белой бумаги. Главное — чтобы существовал способ незаметно разместить в этом контейнере некоторый объем информации и чтобы его было очень трудно извлечь или разрушить.

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.

Существенное влияние на надежность стегосистемы и возможность обнаружения факта передачи скрытого сообщения оказывает выбор контейнера.

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

Рассмотрим подробнее понятие «контейнера». Стего должен быть визуально неотличим от пустого контейнера. Различают два основных типа контейнеров: потоковый и фиксированный.

Потоковый контейнер представляет собой непрерывно следующую последовательность бит. Особенностью является то, что невозможно определить его начало или конец. Сообщение вкладывается в него в реальном масштабе времени, так что неизвестно заранее, хватит ли размеров контейнера для передачи всего сообщения. В один контейнер большого размера может быть встроено и несколько сообщений. Интервалы между встраиваемыми битами определяются генератором псевдослучайной последовательности с равномерным распределением интервалов между отсчетами.

Основная трудность заключается в осуществлении синхронизации, определении начала и конца последовательности. Если в данных контейнера имеются биты синхронизации, заголовки пакетов и т. д., то скрываемая информация может идти сразу после них. Трудность обеспечения синхронизации превращается в достоинство с точки зрения обеспечения скрытности передачи. Кроме того, потоковый контейнер имеет большое практическое значение. Например, с помощью стегоприставки к обычному телефону можно было бы передавать другой разговор, данные и т. п., а не зная секретного ключа, нельзя было бы не только узнать содержание скрытой передачи, но и сам факт ее

существования. Не случайно, что открытых работ, посвященных разработке стегосистем с потоковым контейнером, практически не встречается.

У фиксированного контейнера размеры и характеристики заранее известны. Это позволяет осуществлять вложение данных оптимальным в некотором смысле образом.

Контейнер может быть выбранным, случайным или навязанным. Выбранный контейнер зависит от встраиваемого сообщения, а в предельном случае является его функцией. Этот тип контейнера больше характерен для стеганографии. Навязанный контейнер может появиться в сценарии, когда лицо, предоставляющее контейнер, подозревает о возможной скрытой переписке и желает предотвратить ее. На практике же чаще всего сталкиваются со случайным контейнером.

Контейнеры фиксированной длины имеют ограниченный объем и иногда встраиваемое сообщение может не поместиться в файл-контейнер.

В. 4. Области применения стеганографии

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. Камуфлирование программного обеспечения.
4. Защита авторского права на некоторые виды интеллектуальной собственности.

Остановимся подробнее на каждой из перечисленных задач.

1. Защита конфиденциальной информации от несанкционированного доступа

Это область использования является наиболее эффективной при решении проблемы защиты конфиденциальной 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.

2. 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.

3. 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).

4. 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.

Так к каждому продаваемому экземпляру произведения можно добавлять некоторый незаметный водяной знак, позволяющий идентифицировать покупателя. Если конкретный экземпляр окажется в свободном доступе, проанализировав водяной знак, правоохранительным органам гораздо легче будет найти и наказать виновного. Кроме

того, применение стеганографии, в отличие от DRM (Digital Rights Management, управление цифровыми правами), хорошо тем, что если с документа защита снята полностью, в этом очень легко убедиться. Но *абсолютной уверенности в том, что водяной знак полностью удален из произведения, получить практически невозможно*. А в таких условиях распространение документов после удаления водяных знаков становится весьма опасным — гораздо опаснее, чем распространение документов со снятой защитой.

Кроме этого стеганографические системы могут **использоваться для решения следующих задач**:

- скрытая аннотация документов (медицинские снимки, картография, мультимедийные базы данных),
- доказательство аутентичности информации (системы видеонаблюдения, электронной коммерции, голосовой почты, электронное конфиденциальное делопроизводство),
- скрытая связь (военные и разведывательные приложения, применение в случаях когда нельзя использовать криптографию).

Краткий обзор стеганографических программ

В настоящее время существует большое количество различных программ использующих методы стеганографической защиты. Наибольшую известность получили следующие программы.

Steganos Security Suite 2006 v 8.0.4 – программа, которая скрывает сам факт шифрования. Для этого зашифрованные данные "прячутся" в файлах графики (например, рисунке), или музыкальном файле, которые внешне ничем не отличаются от аналогичных файлов, не несущих зашифрованной информации - картинку можно посмотреть, музыку можно послушать. Дело в том, что оцифрованные файлы (те же *.bmp или *.wav) могут быть в определенной степени изменены, и это не повлияет на качество звука или изображения (вернее, эти изменения будут практически не заметны). От аналогичных программ Steganos Security Suite выгодно отличается способностью скрывать данные не только в файлах форматов wav и bmp, но и в html и даже в обычных текстовых. Не будет лишней и имеющаяся функция удаления файлов без возможности их восстановить. Кроме этого, программа поддерживает 128-битное шифрование по стандарту AES, удаление всех следов нахождения в Интернете, имеет модуль шифрования почты, позволяющий вести шифрованную переписку, а также менеджер паролей. Имеется и такая полезная опция, как блокирование компьютера от посторонних.

Stash 1.0 – программа, которая позволяет запрятывать информацию различных форматов (*.txt, *.doc, различные типы архивов) в графические файлы форматов GIF,PNG, PCX, BMP или TIFF с помощью пяти различных методов, что может потребоваться, например, для защиты авторских прав на изображения. При этом визуальных изменений не происходит.

S-Tools 4.0 –программа, позволяющая прятать информацию в графических (форматы bmp и jpg) и аудио-файлах (формат wav). Информация также может быть зашифрована с помощью криптографических алгоритмов.

Однако, существует большое количество и менее известных программ: Contraband 9h, Text to BMP Encoder/Decoder 2.5, Invisible Secrets v. 2.1, Kimage v. 1.0 и другие.

ВЫВОД: Комплексное использование стеганографии и шифрования многократно повышает сложность решения задачи обнаружения и раскрытия конфиденциальной информации.

Ст. преподаватель 27 кафедры
подполковник
С.Краснов