Лекция 8. Стеганографическая защита информации

Цель лекции: изучить понятие стеганографии, рассмотреть историю развития стеганографии

План лекции:

1. Понятие стеганографии
2. История развития стеганографии
3. Обзор стеганографических программ

Криптографическая (с греческого *steganos* — "тайный", *graphy* "пишу") **защита информации** (система изменения последней с целью сделать ее непонятной для непосвященных, сокрытие содержания сообщений за счет их шифрования), выражающаяся в наличии шифрованного сообщения, сама по себе привлекает внимание.

Скрытие же самого факта существования секретных данных при их передаче, хранении или обработке является задачей стеганографии (от греческого arcyavog — "скрытый") — науки, которая изучает способы и методы скрытия конфиденциаль-ных сведений. Задача извлечения информации при этом отступает на второй план и решается в большинстве случаев стандартными криптографическими методами.

Стеганография – это искусство и наука передавать сообщения различными способами так, чтобы не было обнаружено наличие самого сообщения, это область знаний о сокрытии информации; это процесс вкрапления представленной в какой-либо форме информации внутрь другой информации.

Цель стеганографии - скрыть от непосвященных лиц сам факт существования сообщений.

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

История развития стеганографии

Стеганография вчера:

- местом зарождения стеганографии многие называют Египет, хотя первыми «стеганографическими сообщениями» можно назвать и наскальные рисунки древних людей;
- общеизвестно, что в древней Греции тексты писались на дощечках, покрытых воском. Во избежание попадания сообщения к противнику, использовали следующее: соскабливали воск с дощечек, писали сообщение прямо на поверхности дерева, потом снова покрывали дощечку воском. Таблички выглядели без изменений и потому не вызывали подозрений;

- греческий историк Геродот упоминает случай применения тайнописи в V веке до н.э.;
- Тиран Гистий, будучи под надзором царя Персии Дария в Сузах, захотел послать сообщение своему родственнику в город Милет в Анатолии. Для этого он побрил наголо раба и вытатуировал сообщение на его голове. Волосы отросли, и раб доставил послание;
- 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;
- в Китае письма писали на полосках щелка. Поэтому для сокрытия сообщений, полоски с текстом письма, сворачивались в шарики, покрывались воском и затем глотались посыльными;
- усиление слежки во времена средневековой инквизиции привело к развитию как криптографии, так и стеганографии. Именно в средние века впервые было применено совместное использование шифров и стеганографических методов;
- В XV веке монах Тритемиус (1462-1516), занимавшийся криптографией и стеганографией, описал много различных методов скрытой передачи сообщений. Позднее, в 1499 году, эти записи были объединены в книгу «Steganographia», которую в настоящее время знающие латынь могут прочитать в Интернет;
- XVII - XVIII века известны как эра «черных кабинетов» - специальных государственных органов по перехвату, перлюстрации и дешифрованию переписки. В штат «черных кабинетов», помимо криптографов и дешифровальщиков, входили и другие специалисты, в том числе и химики. Наличие специалистов-химиков было необходимо из-за активного использования так называемых невидимых чернил;
- Стеганографические методы активно использовались и в годы гражданской войны между южанами и северянами. Так, в 1779 году два агента северян Сэмюэль Вудхулл и Роберт Тоунсенд передавали информацию Джорджу Вашингтону, используя специальные чернила;
- симпатические чернила использовали русские революционеры в начале XX века, что нашло отражение в советской литературе: Куканов в своей повести «У истоков грядущего» описывает применение молока в качестве чернил для написания тайных сообщений. Впрочем, царская охрана тоже знала об этом методе (в архиве хранится документ, в котором описан способ использования

симпатических чернил и приведен текст перехваченного тайного сообщения революционеров);

- особое место в истории стеганографии занимают ***фотографические микроточки***. Те самые микроточки, которые сводили с ума спецслужбы США ***во время второй мировой войны***. Однако микроточки появились намного раньше, сразу же после изобретения Дагером фотографического процесса, и впервые в военном деле были использованы во времена франко-прусской войны (в 1870 году).

Стеганография сегодня:

- 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.

Пример стеганографии:

"КОМПАНИЯ "ЛЮЦИФЕР" ИСПОЛЬЗУЕТ ЕДКИЙ НАТР, ТЯЖЕЛЫЕ ГРУЗИЛА, ОСТРОГУ ТРЕХЗУБУЮ, ОБВЕТШАЛЫЙ ВАТНИК".

Первые буквы фразы складываются в предложение: **"Клиент готов".**

Компьютерная стеганография завтра:

- актуальность проблемы информационной безопасности постоянно растет и стимулирует поиск новых методов защиты информации (ЗИ);
- бурное развитие информационных технологий обеспечивает возможность реализации новых методов ЗИ. Сильным катализатором этого процесса является лавинообразное развитие компьютерной сети 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;
- внедрение криптологических методов.

В отличие от криптографии, которая скрывает содержимое тайного сообщения, стеганография скрывает сам факт его существования.

№	Стеганография	Криптография
1.	Защищает информацию о наличии каких-либо сообщений.	Защищает содержание сообщения.
2.	Помещение информации в какой-либо нейтральный объект (контейнер) (текстовый, графический, аудио- или видеофайл) и незаметное распределение в нем информации.	Использование ключа в процессе шифровки и дешифровки и алгоритма обеспечивающего, дешифрование только с помощью ключа.
3.	Определение «гнезд» выступает авторским шифром такого сообщения. В «гнезда» вносится информация, порядок ее внесения, внешняя незаметность изменений контейнера, сохранение различных статистических характеристик контейнера.	Алгоритмы с использованием ключа делятся на два класса: симметричные (или алгоритмы секретным ключом) и ассиметричные (или алгоритмы с открытым ключом). Разница в том, что симметричные алгоритмы используют один и тот же ключ для шифрования и для дешифрования (или же ключ для дешифровки просто вычисляется по ключу шифровки). В то время как асимметричные алгоритмы используют разные ключи, и ключ для дешифровки не может быть вычислен по ключу шифровки.

М.О. Жмакин выражает общий процесс стеганографии простой формулой:

К + СС + СКл = СК

где:

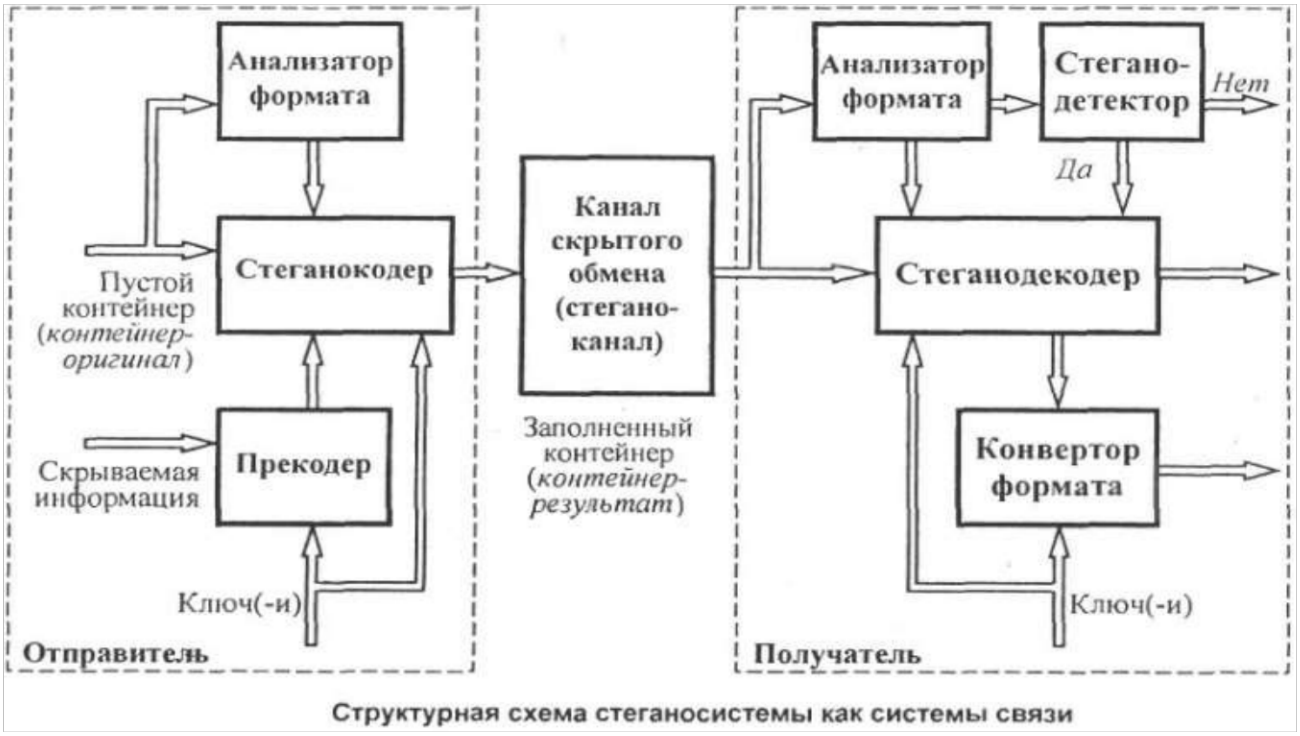
- контейнер (К) – любая информация, предназначенная для встраивания тайных сообщений;
- скрываемое (встраиваемое) сообщение (СС) – тайное сообщение, встраиваемое в контейнер;
- стегоключ (СКл) – секретный ключ, необходимый для скрытия (шифрования) информации. В зависимости от количества уровней защиты (например, встраивание предварительно зашифрованного сообщения) в стегосистеме может быть один или несколько стегоключей;
- стегоконтейнер (СК) – контейнер, содержащий встроенное сообщение;
- стеганографический канал (стегоканал) – канал скрытой передачи информации.

Классическая стеганография, которая включает в себя все «некомпьютерные методы».

Цифровая стеганография – направление классической стеганографии, основанное на сокрытии или внедрении дополнительной информации в

цифровые объекты, что вызывает некоторые искажения этих объектов. Чаще всего в этих целях используется избыточность аудио и визуальной информации.

Компьютерная стеганография – направление классической стеганографии, основанное на особенностях компьютерной платформы и использовании специальных свойств компьютерных форматов данных.



Структурная схема стеганосистемы как системы связи

Принципы стеганографии:

- файлы, содержащие оцифрованное изображение или звук, могут быть до некоторой степени видоизменены без потери функциональности.
- неспособность органов чувств человека различить незначительные изменения в цвете изображения или качестве звука.
- Методы скрытия должны обеспечивать аутентичность и целостность файла.
- Основные свойства открыто передаваемого файла должны сохраняться при внесении в него секретного сообщения и ключа.
- Предполагается, что противнику известны стеганографические методы, детали их реализации. Единственное, что неизвестно - ключ, с помощью которого только его держатель может установить факт присутствия и содержание скрытого сообщения.

Обзор стеганографических программ

QuickStego позволяет скрывать текст в снимках, чтобы только другие пользователи QuickStego могли извлекать и читать скрытые секретные сообщения. После того, как текст будет скрыт в изображении, сохраненное изображение по-прежнему является «изображением», оно будет загружаться так же, как и любое другое изображение. Изображение можно сохранить, отправить по электронной почте, загрузить в Интернете, как и прежде, единственное различие заключается в том, что оно содержит скрытый текст.

OpenStego. Используя это программное обеспечение, вы можете либо скрыть данные (файл) внутри изображения, либо извлечь данные из изображения.Также, есть и множество других ПО для работы с стеганографией: OpenPuff, Steghide, Stegsolve и другие.

Анализ тенденций развития стеганографии 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).

Список использованной литературы

1. Adam Shostack. “Threat Modeling: Designing for Security”. Published by John Wiley & Sons, Inc., Canada 2014.- 626 p.
2. Richard Bejtlich. “The Practice of Network Security Monitoring”. Published by No Starch Press, Inc., USA 2013. – 380 p.
3. Scott E. Donaldson, Stanley G. Siegel, Chris K. Williams and Abdul Aslam. “Enterprise Cybersecurity: how to build a successful Cyberdefense program against advanced threats”. Published by Apress, 2015. – 508 p.
4. Хорев А. А. Организация защиты конфиденциальной информации в коммерческой структуре // Защита информации. Инсайд : журнал. — 2015. — № 1. — С. 14—17. — ISSN 2413-3582
5. Фред Б. Риксон. Коды, шифры, сигналы и тайная передача информации. — Астрель, 2011. — ISBN 978-5-17-074391-9.
6. Morris J. Dworkin. SHA-3 Standard: Permutation-Based Hash and Extendable-Output Functions (англ.) // Federal Inf. Process. Stds. (NIST FIPS) - 202. — 2015-08-04.