УДК 622

# РАЗРАБОТКА СИСТЕМЫ СТЕГАНОГРАФИЧКСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ

К.Ю. Глебов, студент группы ИТб-122, III курс
Д.В. Замятина, студент группы ИТб-122, III курс
Научный руководитель: И.С. Сыркин, к.т.н., доцент
Кузбасский государственный технический университет имени Т.Ф. Горбачева
филиал в г. Прокопьевск
г. Прокопьевск

*Информация — кислород современного мира.*
*Рональд Рейган*

Кислород важен для жизни человека, информация же важна для целых наций. В одних руках она может принести разрушение, в других же принесет мир и процветание всему человечеству. Главная наша задача - это правильное использование имеющихся у нас знаний, для это и необходима защита информации.

Существует три способа обезопасить информацию. Первый – физический, это самый древнейший способ защиты от противника самого носителя информации (пергамент, секретные документы, проводная линия связи и др.). Самым важным в этом методе является не допустить утечку информации, для этого придумано множество способов скрытия информации, а также в случае необходимости быстрого устранения носителя (выбросить, сжечь, порвать и т.д.).

В своей работе мы будет использовать два других способа и поэтому первостепенной нашей задачей будет подробное изучение особенностей и тонкостей защиты информации. А в дальнейшем уже создание программы, позволяющей передавать сообщения скрытых от посторонних глаз.

Второй способ позволяет скрыть наличие самого факта передачи данных, он называется стеганография. Первое упоминание появилось к 440 г. до нашей эры в трактате Геродота «История». В своих рукописях Геродот рассказывал о двух способах передачи информации, первый это на восковой дощечке писалось сообщение до нанесения самого воска, второй же способ занимал дольше времени для передачи информации, так как оно писалось на бритой голове раба и отправляли только когда волосы отрастали, а там заново сбривали его волосы. Современная стеганография подразделяется на три вида: классическая, компьютерная и цифровая.

К классической стеганографии относятся такие методы как:

- симпатические чернила – главной особенностью является, что при воздействии определенных факторов окружающей среды, их состояние

изменяется (одни при нагревании проявляются, другие же со временем исчезают);

- микроточки-фотографии размером с точку на которых при увеличении можно было увидеть, на пример карту секретной базы;
- запись на боковой колоде карт-только в определенном порядке карт можно прочитать сообщение;
- трафареты- при наложении на текст можно прочитать необходимое сообщение;
- и многое другое.

Компьютерная стеганография - это разновидность классической, но с использованием особенностей современных операционных систем. Примерами этого способа являются:

1. Употребление полей, которые зарезервированы для компьютерных форматов файлов.
2. Скрытие информации в неиспользованных местах сменных носителей.
3. Применение характерных свойств полей форматов, предназначенных для сносок и указателей.
4. Эксплуатация определенных файловых систем.

Цифровая стеганография основывается на внедрении и сокрытии информации в цифровые файлы, тем самым вызывая незначительные искажения самих объектов.

Третьим способом информация защищается с помощью шифрования, основанного на математических функциях, он называется криптография.

Шифрованием пользовались еще в древней Греции, Риме, Египте и даже Индии. Даже великие ученые и философы писали свои работы так, чтобы их смог прочитать только достойный ученик, т.е. более талантливый, способный разгадать шифр. Криптография также широко используется и в наше время, а мы можем даже об этом и не подозревать. Ведь не все задумываются, как банки защищают нашу личную информацию от посторонних.

Криптография в свою очередь делится на симметричное (с закрытым ключом) и ассиметричное (с открытым ключом) шифрование.

Ассиметричное появилось относительно не давно, только в XIX веке, с помощью математических функций начали зашифровывать текст по открытому ключу, и по обратной функции расшифровывать уже по закрытому ключу. Таким образом нет необходимости передавать ключи, и это увеличивает крипто стойкость алгоритмов шифрования, затрудняя дешифровать с помощью украденного ключа во время его передачи.

Симметричное шифрование происходит с древних времен, и это не только математические обратные функции, но это и разнообразные методы замены, подстановки. К ним относятся такие шифры, как книжный шифр, шифр Цезаря, линейка Энея, квадрат Полибея и многие другие.

В современности люди научились комбинировать эти метода, для более качественной и быстрой передачи данных, используя преимущества каждого из них. Так сам текст шифруется симметричным (на пример AES) из-за скорости шифрования, а ключ шифруется ассиметричным алгоритмом (на пример RSA) из-за высокой крипто стойкости, таким образом сообщение шифруется/дешифруется в несколько раз быстрей, но при это ключ защищен.

Проанализировав все способы защиты информации, мы пришли к выводу, что самым лучшим способом защиты информации является комбинирование этих методов. Так если совместить физический и криптографический способ защиты информации, то злоумышленнику нужна не только физическая сила, но и ключ и алгоритм, или опытный крипто аналитик, чтобы расшифровать сообщение. Другой способ - это использовать вместе с криптографией стеганографию. При совмещение всех трех методов защиты нужно быть предельно осторожными ведь физическая защита может вызвать лишнее внимание, но при правильном использование это будет идеальной защитой.

В своей работе мы будем применять несколько методов стеганографии и простой алгоритм симметричного шифрования. В простеньком графическом редакторе при нажатии в определенные места (скрытые label), открываются диалоговые окна, первое окно позволяет зашифровать сообщение и спрятать его в изображение формата *bmp, второе для расшифровки сообщения из изображения, при каждом действии необходим ключ, который генерируется из необходимых данных для шифрования и дешифровки. В зависимости от размера изображения объём передаваемой информации ограничен, размером самого изображения, так как мы заменяем последний пиксель каждого бита. Такое условие позволяет нам искажать изображения так, чтобы человеческий глаз это не заметил.

## Список литературы:

1. Википедия свободная энциклопедия [Электронный ресурс]: Стеганография URL: https://ru.wikipedia.org/wiki/Стеганография, свободный. – Заглавие с экрана. - Язык русский

2. Википедия свободная энциклопедия [Электронный ресурс]: История(Геродод) URL: https://ru.wikipedia.org/wiki/История_%28Геродот%29, свободный. – Заглавие с экрана. - Язык русский

3. Википедия свободная энциклопедия [Электронный ресурс]: Криптография URL: https://ru.wikipedia.org/wiki/%CA%F0%E8%EF%F2%EE%E3%F0%E0%F4%E8%FF, свободный. – Заглавие с экрана. - Язык русский

4. Википедия свободная энциклопедия [Электронный ресурс]: BMP URL: https://ru.wikipedia.org/wiki/BMP, свободный. – Заглавие с экрана. - Язык русский