О МЕТОДАХ СОКРЫТИЯ ИНФОРМАЦИИ

Чухненко М.В.
*Национальный технический университет
"Харьковский политехнический институт",
г. Харьков, ул. Пушкинская, 79/2, тел. 707–63–60*

Под сокрытием информации (Information Hiding) обычно понимают методы, позволяющие скрывать некоторую дополнительную информацию, являющуюся или не являющуюся секретной, в некоторой, не привлекающей внимания информации.

Необходимость скрывать содержание важных сообщений существует уже тысячи лет. Со временем люди находили все более и более сложные способы кодирования сообщений, поскольку простые способы кодировки декодируются с большей легкостью. Коды и шифры не являются синонимами, как многие думают. Код – это совокупность знаков (символов) и система определенных правил, при помощи которых информация может быть представлена (закодирована) в виде набора из таких символов для передачи, обработки и хранения. Шифр – это совокупность условных знаков (условная азбука из цифр или букв) для секретной переписки или для передачи текста секретных данных по техническим средствам связи. Таким образом, при кодировании каждое слово в сообщении заменяется кодовым словом или символом, в то время как при шифровании каждая буква в сообщении заменяется буквой или символом шифра.

Защита информации необходима для уменьшения вероятности утечки (разглашения), модификации (умышленного искажения) или утраты (уничтожения) информации, представляющей определенную ценность для ее владельца. Проблема защиты информации от несанкционированного доступа возникла еще в древние времена, и с тех пор выделилось два основных направления решения этой проблемы, которые существуют и сегодня: криптография и стеганография.

Стеганография является более древней, чем коды и шифры, и обычно её называют тайнописью, искусством скрытой записи. Лучший способ тайнописи – это использование обычных предметов для сокрытия сообщения. В Англии был популярен метод тайнописи, для которого использовали обычную газету с крошечными точками под буквами на первой странице, которые указывали, какие буквы следует читать, чтобы получить сообщение. Некоторые люди могли составить сообщение, используя первые буквы каждого слова в каком-либо тексте или используя невидимые чернила. Стеганографию лучше всего использовать в сочетании с кодом или шифром, так как существует риск, что тайное послание может быть обнаружено.

Среди классических методов стенографии можно выделить следующие: манипуляции с носителем информации (контейнером); симпатические чернила; литературные приемы; семаграммы. Компьютерные технологии придали новый

импульс развитию и совершенствованию стеганографии, появилось новое направление в области защиты информации - компьютерная стеганография.

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).

Криптография - наука о методах обеспечения конфиденциальности (невозможности прочтения информации посторонним) и аутентичности (целостности и подлинности авторства, а также невозможности отказа от авторства) информации. Традиционная криптография образует раздел симметричных криптосистем, в которых шифрование и расшифровка проводится с использованием одного и того же секретного ключа. Помимо этого раздела современная криптография включает в себя асимметричные криптосистемы, системы электронной цифровой подписи, хеш-функции, управление ключами, получение скрытой информации, квантовую криптографию[1].

Шифрование — способ преобразования открытой информации в закрытую и обратно. Применяется для хранения важной информации в ненадёжных источниках или передачи её по незащищённым каналам связи. Существует множество разных шифров. Самые известные шифры это: шифр Атбаш**,** шифр Френсиса Бекона, шифр Блеза Виженера, шифр Лестера Хилла, шифр Тритемиуса, шифр Гронсфельдаза, шифр Цезаря[2].

Современный уровень развития компьютерной техники позволяет обрабатывать информационные потоки в реальном времени. На основе криптографических методов и средств реализуются процедуры шифрования и дешифрования; системы идентификации и аутентификации, реализуемые на основе асимметричных криптографических стандартов (цифровая подпись).

Использование криптографии особенно важно для разработки протоколов передачи информации в глобальных компьютерных сетях для надежной защиты передаваемых данных от незаконного перехвата. Протоколы, разработанные с учетом криптографических методов и средств защиты, позволяют обеспечить требуемую секретность передаваемой информации, т.к. задача расшифровки перехваченных данных потребует от противника высоких вычислительных и материальных затрат, как правило, несоизмеримых с ценностью этих данных.

Список литературы

1. Ященко В.В. Введение в криптографию. [Электронный ресурс] –СПб.: Питер. –2001. ISBN: 5-900916-40-5

2. Аграновский А. В., Хади Р. А. Практическая криптография: алгоритмы и их программирование. [Электронный ресурс] –М.: Солон-Пресс. –2009.