## ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ МЕТОДОМ СТЕГАНОГРАФИИ

*Тимощенко Е.В. (БИП ГФ)*

В основе информационной безопасности лежит деятельность по защите информации – обеспечению её конфиденциальности, доступности и целостности, а также недопущению какой-либо компрометации в критической ситуации.

В последние годы наблюдается активное внедрение цифровых технологий на предприятиях и в организациях. Поэтому, в силу важности и ценности хранящейся информации, вопрос её защиты от несанкционированного доступа, вредоносных атак или перехвата управления внутренними системами является самым важным в политике безопасности любой организации.

Угрозы информационной безопасности могут принимать весьма разнообразные формы. Наиболее серьёзными считаются угрозы связанные с активным внедрением организациями информационных технологий, которые чаще всего спроектированы без учёта требований безопасности, что открывает дополнительные возможности для атаки. Это, в сочетании с нечётко определёнными правовыми нормами и условиями, позволяет организациям использовать собранные персональные данные своих клиентов по собственному усмотрению без их ведома. И хотя правовое регулирование процесса сбора, хранения и обработки персональных данных предполагает в долгосрочной перспективе улучшение информационной безопасности, однако в настоящее время риски организаций всё ещё велики.

Информационная безопасность оказывает непосредственное влияние на понятие неприкосновенности частной жизни. Действительно, активное использование облачных хранилищ, популярность интернет-магазинов, увлечённость разнообразными социальными сетями влекут за собой неизбежную доступность личной информации и персональных данных, которыми могут воспользоваться злоумышленники. Велика вероятность «кражи личности» – действия, в результате которых персональные данные (например, имя, учётная запись в банковской системе или номер кредитной карты) используются для мошенничества и совершения иных преступлений. В конечном итоге человек, от чьего имени мошенники получают незаконные финансовые преимущества, кредиты или совершают иные преступления, зачастую сам становится обвиняемым и несёт финансовые и юридические последствия.

Для защиты информации разработан ряд методов и средств, однако для защиты конфиденциальной информации наиболее эффективным является шифрование. Шифрование – метод защиты информации в коммуникационных каналах путем ее криптографического закрытия. Этот метод защиты широко применяется как для обработки, так и для хранения информации. При передаче информации по коммуникационным каналам большой протяженности этот метод является единственно надежным. Кроме криптографии, скрывающей содержимое секретного сообщения, есть ещё метод шифрования, который, в отличие от предыдущего, скрывает сам факт передачи информации – это стеганография.

Поскольку объемы данных, хранящихся в компьютерах и передаваемых по сетям, с каждым годом растут, популярность стеганографических методов увеличивается. В компьютерах и сетях стеганографические приложения позволяют любому пользователю скрыть любой тип бинарного файла в любом другом бинарном файле. С помощью стеганографии обычное изображение может хранить не только графическую информацию. Поэтому, благодаря большой популярности социальных сетей, именно графические и звуковые файлы являются сегодня самыми распространенными носителями для транспортировки зашифрованной информации.

В зависимости от преследуемых целей могут использоваться различные стеганографические методы. Например, цифровые водяные знаки, которые представляют собой некую цифровую подпись, встраиваемую в мультимедийный объект с целью защиты авторских прав. Внедрение цифровых подписей позволяет определить владельца информации и отслеживать её незаконное распространение. Стеганография также может использоваться с целью встраивания идентификационных номеров – так называемый цифровой отпечаток пальцев – для скрытой аннотации и аутентификации передаваемой конфиденциальной информации.

Актуальность и востребованность темы исследования способствовали решению спроектировать и разработать программное обеспечение, которое будет использовать стеганографические методы сокрытия информации в цифровых изображениях. При этом кодирование будет производиться с помощью метода сокрытия в частотной области изображения. Стоит отметить, что размер и качество изображения, при встраивании в него информации, остается практически неизменным. Следовательно, появляется возможность хранить в открытом доступе или передавать по открытым каналам связи почти любую конфиденциальную информацию.

Метод, который использован при разработке программы для сокрытия информации в изображениях форматов BMP, PNG является одним из наиболее распространенных на сегодня методов скрытия конфиденциальной информации в частотной области изображения. Метод заключается в относительной замене величин коэффициентов дискретно-косинусного преобразования (ДКП) – метод Коха и Жао. Он обладает хорошей устойчивостью к большинству известных стеганоатак, в том числе к атаке сжатием, к аффинным преобразованиям, геометрическим атакам.

Скрытая передача секретного изображения происходит по открытому каналу, где вначале первый пользователь использует предложенную программу для сокрытия информации в изображение, а пользователь-получатель, используя программу, извлекает скрытую информацию из изображения [1].

Дополнительно, кроме непосредственного сокрытия информации разработанное приложение даёт возможность сравнения двух на первый взгляд одинаковых изображений на наличие дополнительных пикселей, отличающих их друг от друга. Также предусмотрена возможность внедрения в изображения случайной информации, благодаря чему скрытая в изображение информация становится недоступной.

Приложение [2] отвечает всем требованиям, предъявляемым к стеганографическому программному обеспечению, и может использоваться для сокрытия данных в графических файлах форматов BMP, PNG. После завершения разработки было проведено тестирование программного средства на ряде фотографий. Результаты тестирования на скрытность встраивания и полезный объем байтов для встраивания являются хорошими.

ЛИТЕРАТУРА

1. Ражков, А. Ф. Использование стеганографического метода Коха и Жао для сокрытия информации в цифровых изображениях / Ражков А. Ф., Тимощенко Е. В. // Первый шаг в науку – 2018: материалы Междунар. форума студ. и учащ. молодежи в рамках Междунар. науч.-практич. инновац. форума «INMAX'18» (Минск, 4–5 декабря 2018 г.). В 4 ч. Часть 4. / ОО «Центр молодежных инноваций», ООО «Минский городской технопарк». – Мн: Лаборатория интеллекта, 2018. – С. 66-68.

2. Программное обеспечение для сокрытия информации в цифровых изображениях с помощью стеганографического метода Коха и Жао // Портал молодых ученых [Электронный ресурс]. – Режим доступа: http://www.student.icm.by/development/programmnoe-obespechenie-dlya-sokrytiya-informacii-v-cifrovykh-izobrazheniyakh-s. – Дата доступа: 14.01.2019.