

Принцип работы Тог похож на алгоритм передачи данных в VPN. Информация, связанная с запросом, помещается в зашифрованные пакеты. Затем, Тог убирает всю информацию, которая может использоваться для идентификации пользователя. После этого, Тог шифрует всю остальную информацию и все данные пересылаются через множество произвольных серверов. Каждый из серверов просматривает только ту информацию, которая необходима для определения отправителя и дальнейшего пути отправки этого пакета, таким образом обеспечивается анонимность.

SSH-туннелинг. Сетевой протокол, позволяющий производить удалённое управление компьютером и передачу файлов. Использует алгоритмы шифрования передаваемой информации. Данный тип маскировки IP-адреса представлен в виде сторонней программы.

SSH-туннелинг можно рассмотреть в качестве дешёвой замены VPN. При пересылке через SSH-туннель незашифрованный трафик любого протокола шифруется на одном конце SSH-соединения и расшифровывается на другом.

Литература

1. Информационная безопасность в таможенных органах : учебно-методическое пособие для студентов специальности 1-96 01 01 «Таможенное дело» / Г. М. Бровка, И. А. Ковалькова, А. Н. Шавель. – Минск: БНТУ, 2019. – 118 с.
2. Способы сокрытия IP-адреса в сети Internet [Электронный ресурс]. – Режим доступа: <https://habr.com/ru/post/72820/>. – Дата доступа: 27.03.2019.
3. Wikipedia – свободная энциклопедия [Электронный ресурс]. – Режим доступа: <https://ru.wikipedia.org/>. – Дата доступа: 24.03.2019.

Компьютерная стенография и её применение

Алданова Е.А.

Научный руководитель: Ковалькова И.А.

Белорусский национальный технический университет

Задача надёжной защиты информации от несанкционированного доступа является одной из древнейших и не решённых до настоящего времени проблем. Способы и методы сокрытия секретных сообщений известны с давних времён.

В дальнейшем для защиты информации стали использоваться более эффективные методы кодирования и криптографии. От криптографии стенография отличается тем, что с помощью криптографии можно скрыть

содержание сообщения, а, пользуясь стенографией, можно скрыть само существование сообщения.

Компьютерные технологии придали новый импульс развитию и совершенствованию стенографии, появилось новое направление в области защиты информации – компьютерная стенография.

Компьютерная стенография – направление классической стеганографии, основанное на особенностях компьютерной платформы. Примерами компьютерной стенографии являются скрытие данных в неиспользуемых областях форматов [файлов](#), подмена символов в названиях [файлов](#), [текстовая стеганография](#) и т. д.

Компьютерная стенография по сути представляет собой сокрытие сообщения или файла в другом сообщении или файле. Например, стенографы могут спрятать аудио- или видеофайл в другом информационном или даже в большом графическом файле.

Компьютерная стенография базируется на двух основных принципах. Первый принцип заключается в том, что файлы, содержащие оцифрованное изображение или звук, могут быть до некоторой степени видоизменены без потери их функциональности в отличие от других типов данных, требующих абсолютной точности. Второй принцип заключается в неспособности органов чувств человека различать незначительные изменения в цвете изображения или качестве звука.

Этот принцип особенно легко применять к изображению или звуку, несущему избыточную информацию.

Процесс стенографии можно разделить на несколько этапов.

1. Выбор информационного файла.
2. Выбор файла-контейнера. В большинстве известных программ по стеганографии говорится, что для сокрытия информации, объём памяти файла-контейнера должен примерно в восемь раз превышать объём памяти информационного файла. Следовательно, чтобы спрятать файл размером 710КБ, понадобится графика объёмом 5600КБ.
3. Выбор стенографической программы.
4. Кодирование файла.
5. Отправление скрытого сообщения по электронной почте и его декодирование.

В связи с возрастанием роли глобальных компьютерных сетей становится всё более важным значение стенографии. В настоящее время стенографические системы активно используются для решения следующих основных задач:

1. Защита конфиденциальной информации от несанкционированного доступа. Это область использования компьютерной стенографии является наиболее эффективной при решении проблемы защиты конфиденциальной

информации. Так, например, только одна секунда оцифрованного звука с частотой дискретизации 44100 Гц и уровнем отсчёта 8 бит в стереорежиме позволяет скрыть за счёт замены наименее значимых младших разрядов на скрываемое сообщение около 10 Кбайт информации. При этом, изменение значений отсчётов составляет менее 1%. Такое изменение практически не обнаруживается при прослушивании файла большинством людей.

2. Преодоление систем мониторинга и управления сетевыми ресурсами. Стенографические 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). Является одной из важных задач стеганографии. В тех случаях, когда использование ПО незарегистрированными пользователями является нежелательным, оно может быть закомуфлировано под стандартные универсальные программные продукты (например, текстовые редакторы) или скрыто в файлах мультимедиа (например, в звуковом сопровождении компьютерных игр).

4. Защита авторского права на некоторые виды интеллектуальной собственности. Является ещё одной областью использования стенографии, позволяющей осуществлять защиту авторского права от пиратства. На компьютерные графические изображения наносится специальная метка, которая остаётся невидимой для глаз, но распознаётся специальным ПО. Такое программное обеспечение уже используется в компьютерных версиях некоторых журналов. Данное направление стенографии предназначено не только для обработки изображений, но и для файлов с аудио- и видеoinформацией и призвано обеспечить защиту интеллектуальной собственности.

Анализ тенденций развития компьютерной стенографии показывает, что в ближайшие годы интерес к развитию методов компьютерной стеганографии будет усиливаться всё больше и больше. Предпосылки к этому уже сформировались сегодня. В частности, общеизвестно, что актуальность проблемы информационной безопасности постоянно растёт и стимулирует поиск новых методов защиты информации. С другой стороны, бурное развитие информационных технологий обеспечивает возможность реализации этих новых методов защиты информации. И, конечно, сильным катализатором этого процесса является развитие компьютерной сети общего пользования Internet, в том числе такие нерешённые противоречивые проблемы Internet, как защита авторского

права, защита прав на личную тайну, организация электронной торговли, противоправная деятельность хакеров, террористов и т.п.

Литература

1. Грибунин В. Г., Жердин О. А., Мартынов А. П., Николаев Д. Б., Силаев А. Г., Фомченко В. М. Основы стеганографии // Под ред. д-ра техн. наук В. Г. Грибунина, г. Трехгорный, 2012.

2. Конахович Г. Ф., Пузыренко А. Ю. Компьютерная стеганография. Теория и практика. — К.: МК-Пресс, 2006. — 288 с.

Методы и способы обеспечения информационной безопасности таможенных органов Республики Беларусь

Волосенкова Е. Д., Костюкевич В. Ю.

Научный руководитель: Ковалькова И. А.

Белорусский национальный технический университет

В современном мире развитие и применение информационных технологий занимает важное место в любой сфере деятельности. Понятие информации является чрезвычайно ёмким и широко распространённым, особенно в настоящее время, когда информатика, информационные технологии, компьютеры сопровождают человека чуть ли не с рождения.

Развиваются современные информационные технологии, а вместе с ними – преступления и нарушения в этой сфере. При этом негативные последствия от урона, нанесённого информационной безопасности отдельных субъектов, могут иметь международный масштаб. Национальное законодательство совершенствуется, чтобы предотвратить такие информационные угрозы. Новые нормы разрабатываются, а старые корректируются с учётом требований времени.

В свою очередь таможенная деятельность неразделимо связана с возникновением развитием информационных технологий. В настоящее время развитие информационных систем в таможенных службах государств, входящих в Таможенный союз, находится на высоком уровне. В Республике Беларусь внедрение информационных систем, информационных технологий закреплено Таможенным кодексом Республики Беларусь.

Информационные технологии приобрели глобальный трансграничный характер. Это способствует развитию всех сфер деятельности человека, общества и государства.