Литература

1. С.А. Нестеров–Анализ и управление рисками в сфере информационной безопасности [Текст]– М.: Санкт-Петербург, 2007. — 47с.
2. ФСТЭК Р. №31 «Методика определения актуальных угроз безопасности информации в ключевых системах информационной инфраструктуры» [Текст] – Введ. 2014-03-14
3. ОБЗОР МЕТОДИК АНАЛИЗА РИСКОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ИНФОРМАЦИОННОЙ СИСТЕМЫ ПРЕДПРИЯТИЯ / Пугин В. В., Губарева О. Ю. - T-Comm - Телекоммуникации и Транспорт Выпуск № 6 / 2012 – С. 56-57

А.А. Пасюков, Р.И. Баженов

ВНЕДРЕНИЕ СКРЫТЫХ СООБЩЕНИЙ В АУДИО СИГНАЛЫ НА ОСНОВЕ ЭХО-СИГНАЛОВ

(Приамурский государственный университет им. Шолом-Алейхема)

В современном обществе, когда информационные технологии проникают во все сферы жизнедеятельности человека, остро стоит вопрос обеспечения защиты речевой информации и телефонного разговора от угроз неправомерного хищения. В настоящий момент существует достаточно различных средств защиты, которые позволяют защитить такой род информации. И хотя ученые уделяют много времени для совершенствования этой защиты, никому до сих пор не удалось достичь совершенства.

Одним из способов информационной безопасности является защита с помощью стеганографии. Стеганография в отличие от криптографии скрывает сам факт существования информации, которую необходимо защитить от вмешательства посторонних лиц. Скрываемая информация встраивается в некий контейнер, который располагается в безобидном файле любого формата. Это может быть речь, изображение, видео и аудио записи, не привлекающие особого внимания, которые открыто передаются адресату. Нужную информацию может извлечь только получатель.

В ходе работы, планируется разработать способ защиты телефонного разговора по сетевой линии связи IP – телефонию используя спектральные методы.

Многие зарубежные и русские ученые занимались данной проблематикой. В работе Жарких А. А., Пластунов В. Ю. [1] был представлен метод внедрения цифрового водяного знака в аудиосигнал в виде аудиосигнала на основе преобразований конформной алгебры единичного круга. Стародубцев Д. Е., Плашенков В. В. [2] описали алгоритм реализует процедуру интерпретации двоичного потока сообщения как некоторого мелодического контейнера, хранящегося в формате MIDI-файла. Заикин М.А., Гончаров Н.О. [3] описали исследование эффективности метода защиты аудио сигнала при передаче по от-

крытому аналоговому каналу связи с использованием скремблирования. Jayaram P., Ranganatha H. R., Anupama H. S. [4] описали суть стеганографии аудиосигналов, раскрыли плюсы, минусы и произвели анализ наиболее популярных методов сокрытия информации. В работе Zamani M. [5] описал способы повышения надёжности встраивания цифровых водяных знаков в аудио сигналы. В работе Пескова О. Ю., Халабурда Г. Ю. [6] представлены базовые принципы сетевой стеганографии для защиты речи.

Перед началом решения данной проблемы требуется использовать спектральный метод. Спектральный метод – один из методов обработки аудио сигналов, основан на разложение звука на составляющие с дискретным применением преобразования Фурье. Преобразование Фурье – некая математическая основа, которая описывает восприятие звука человеческом. Данное преобразование помогает разложить функцию, представляя колебательные процессы в виде набора синусоидальных составляющих - волнообразных кривых, переходящих от максимума к минимуму. Другими словами, преобразование Фурье - функция, описывающая амплитуду и фазу каждой синусоиды, соответствующей определённой частоте.

Для реализации данной проблемы было решено использовать метод эхо сигналов. В данном методе данные скрываются благодаря изменению трех составляющих: начальной амплитуды, скорости затухания и задержки. Под контейнером лучше всего использоваться музыкальное произведение. Отличительной особенностью музыкального произведения от речевых данных является наличие большого количество частотных составляющих. Количество частотных составляющих ограничивает пространство внедрения, и определяет пороги внедрения.

Данный способ дает возможность внедрять данные в сигнал прикрытия, меняя их характеристики эхо-сигнала. К характеристикам эхо, несущим внедряемые данные, относятся: начальная амплитуда, время спада и сдвиг (время задержки между исходным сигналом и его эхо). При сокращении сдвига два сигнала смешиваются. В конкретной точке человек перестает отличать два сигнала, и эхо воспринимается, равно как дополнительный резонанс.

Таким образов, через полгода планируется реализовать защиту речевых сообщений благодаря встраивания их в контейнер аудио формата, используя эхо-сигналы. После чего планируется активное внедрение метода защиты для безопасности телефонных звонков через IP – телефонию. Данный метод подходит за счет большой пропускной способности и хорошей устойчивости к искажениям.

Литература

1. Жарких А. А., Пластунов В. Ю. Новый метод внедрения водяного знака в аудиосигнал // Вестник МГТУ. 2009. №2 С.206-211.

2. Стародубцев Д. Е., Плашенков В. В. Метод стеганографического преобразования информации в гибридный звуковой контейнер // Вестник Череповецкого государственного университета. 2015. №8 (69) С.29-32.

3. Заикин М.А., Гончаров Н.О. Защита аудио сигнала с использованием скремблирования //Молодежный научно-технический вестник. – 2013. – №. 10. – С. 45.

4. Jayaram P., Ranganatha H. R., Anupama H. S. Information hiding using audio steganography–a survey //The International Journal of Multimedia & Its Applications (IJMA) Vol. – 2011. – Т. 3. – С. 86-96.

5. Zamani M. A secure audio steganography approach //Internet Technology and Secured Transactions, 2009. ICITST 2009. International Conference for. – IEEE, 2009. – С. 1-6.

6. Пескова О. Ю., Халабурда Г. Ю. Применение сетевой стеганографии для защиты данных, передаваемых по открытым каналам Интернет //Материалы научной конференции» Интернет и современное общество. – 2012. – С. 348-354.

Е.В. Пальчевский, А.Р. Халиков

РАЗРАБОТКА СИСТЕМЫ БЛОКИРОВКИ IP-АДРЕСОВ ПО ВНЕШНЕМУ СЕТЕВОМУ ИНТЕРФЕЙСУ

(Уфимский государственный авиационный технический университет)

В современном мире информационная безопасность является одной из ключевых отраслей исследования в области информационной безопасности, в частности, атаки «*DoS*» и «*DDoS*» [1]. Под атакой «*DoS*» понимается направление несанкционированного трафика на внешний сетевой интерфейс ЭВМ с определенным портом [2]. Атака типа «*DDoS*» представляет собой распределенное направление внешнего сетевого трафика на атакуемый сервер (либо ресурса, имеющего выход во внешнюю глобальную сеть) для отказа во внешнем удаленном обслуживании [3]. Зачастую, для выполнения атак типа «*DoS*» и «*DDoS*» используются зараженные вредоносным программным обеспечением персональные компьютеры пользователей [4-7]. Это позволяет генерировать объемные (большие) потоки внешнего сетевого трафика, что приводит к более мощной и усиленной атаке [8-10]. Стандартными методами отличить несанкционированный трафик от легитимного достаточно сложно, так как нет необходимого функционала для данной операции, а также для этого необходимые достаточно большие вычислительные ресурсы [11, 12]. Данные факты обуславливают необходимость разработки специализированной системы для блокировки вредоносного трафика, с последующим снижением нагрузки на ресурсы ЭВМ. Несомненно, разработка системы блокировки *IP*-адресов по внешнему сетевому интерфейсу является актуальной задачей.

Целью работы является разработка системы блокировки *IP*-адресов по внешнему сетевому интерфейсу. Это позволит снижать количество входящих потоков вредоносного трафика, с последующим снижением нагрузки на ресурсы ЭВМ. На первом этапе рассмотрена математическая модель разработанной