утечки конфиденциальной и корпоративной информации. Защита требует комплексного подхода и учета всех возможных коммуникационных каналов, обеспечение физической безопасности, шифрование резервных копий и информации, покидающей периметр, а также ряда организационных мероприятий. В работе предложено разработать программный модуль анализа сетевого трафика и, таким образом, модифицировать комплексную защиту системы, ее информационную безопасность, предотвратить несанкционированное распространение конфиденциальной информации (на примере филиала ООО "ЮНЛ Солюшнс" г.Гродно). Решены следующие задачи: изучены основные понятия систем предотвращения утечки информации; проанализированы методы анализа информации на предмет содержания конфиденциальных данных; разработан программный модуль анализа информации на языке программирования Ruby; разработана веб-панель управления (с использованием фреймворка Ruby on Rails); развернута система на базе микрокомпьютера Raspberry Pi; проанализирована эффективность программно-аппаратного модуля; даны рекомендации по поддержке, развитию и оптимизации системы защиты от утечек конфиденциальной информации.

Литература

1. Ищейнов, В Организационное и техническое обеспечение информационной безопасности. Защита конфиденциальной информации: учеб. пособие / В. Ищейнов, М. Мецатунян. – М.: Высшее образование, 2014. – 256 с.

2. Росенко, А Внутренние угрозы безопасности конфиденциальной информации. Методология и теоретическое исследование / А. Росенко. – Красанд, 2010. – 160 с.

РАЗРАБОТКА МЕТОДОВ И СРЕДСТВ ДЛЯ ИСПОЛЬЗОВАНИЯ СТЕГАНОКОНТЕЙНЕРОВ В АУДИОФАЙЛАХ

И.А. Сазановец

В докладе представлены исследования автора, отражающие возможности передачи скрытых данных в аудиофайлах, возможность модификации аудосигнала, а также передачи скрытых данных в текстовых компонентах аудиофайла. Стеганография в звуковых файлах может применяться для внедрения цифровых отпечатков, водяных знаков и как инструмент скрытой передачи данных. Все звуковые файлы можно рассматривать во временной или же в частотной области. Для перехода из временной в частотную область используется дискретное преобразование Фурье.

Во временной плоскости работают методы наименьшего значащего бита и кодирования с помощью бита четности. В частотной плоскости работают методы фазового кодирования, эхо кодирования, кодирования с помощью расширения спектра и кодирования с помощью высокочастотного шума.

Методы, работающие в частотной области, не позволяют скрыть большой объем информации, поэтому они больше подходят для внедрения цифровых отпечатков или водяных знаков. Метод наименьшего значащего бита позволяет скрыть значительно больше информации, но при его реализации могут наблюдаться следующие уязвимости: запись бит в промежутки тишины (в звуковых файлах тишина кодируется нулями), левый и правый каналы в стереофайле могут быть побитно одинаковыми и отсутствие шифрования (кроме того, что исходное сообщение шифруется, шифрование усложняет стеганоанализ). Также метод наименьшего значащего бита подвержен статистическому анализу. Также в докладе представлены методы сокрытия данных в метаинформации звуковых контейнеров.

СРАВНЕНИЕ СХЕМ ЦИФРОВОЙ ПОДПИСИ НА ОСНОВЕ СТБ 34.101.45-2013 С РАЗДЕЛЕННЫМ СЕКРЕТОМ ПРИ ИСПОЛЬЗОВАНИИ АЛГОРИТМОВ ХЭШИРОВАНИЯ SHA-2 И SHA-3

С.Б. Саломатин, О.А. Селеня

Использование электронно-цифровой подписи для защиты электронного документооборота предполагает надежность всех алгоритмов в ее составе. В основе любой цифровой подписи лежит алгоритм хэширования для обеспечения существенного изменения конечного значения подписи если подписанный документ при передаче подвергся даже