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

небольшому изменению. На сегодняшний день самой новым, а значит и самым безопасным считается алгоритм хэширования SHA-3[1]. Его введение было обусловлено нахождением коллизий в семействе алгоритмов SHA-2 индийскими исследователями в 2008 году. Для исследования ЭЦП с использованием этих алгоритмов был применен ряд статистических тестов, опубликованных NIST. За основу была взята модифицированная схема ЭЦП СТБ 34.101.45-2013 с разделенным секретом[2]. Результаты статистических тестов выявили следующее: оба алгоритма прошли тесты с заданным показателем α=0.01, что говорит о том, что обе последовательности носят случайных характер. По результатам побитового теста алгоритм SHA-3 отклоняется от идеального распределения, в то время как SHA-2 показывает близкие к идеалу результаты. Остальные тесты алгоритм с SHA-3 прошел с большей вероятностью, чем его аналог и проявил хорошие показатели по устойчивости, производительности и безопасности. Недостатки SHA-3 из результатов тестирования можно обосновать недостаточной оптимизацией, чем он уступает более ранним версиям, построенным на встроенных библиотеках.

Литература

1. José Luis Gómez Pardo, Carlos Gómez-Rodríguez The SHA-3 family of hash functions and their use for message authentication. [Электронный ресурс]. – Электронные данные. – Режим доступа: https://goo.gl/Cd1hme. – Дата доступа: 19.05.2017.

2. Селеня, О.А. Реализация пороговой схемы электронной цифровой подписи с разделенным секретом на основе СТБ 34.101.45-2013 / О.А. Селеня. – Молодежный сборник научных статей «Научные стремления». 2016. – Вып. № 18. – С. 11–14.

ОЦЕНКА ПРИМЕНИМОСТИ ЭМПИРИЧЕСКИХ МОДЕЛЕЙ РАСПРОСТРАНЕНИЯ РАДИОВОЛН ДЛЯ АНАЛИЗА ЭЛЕКТРОМАГНИТНОЙ БЕЗОПАСНОСТИ СЕТЕЙ СОТОВОЙ СВЯЗИ С МИКРОСОТОВОЙ СТРУКТУРОЙ В ГОРОДСКОЙ ЗАСТРОЙКЕ

А.С. Свистунов

В связи с массовым охватом населения услугами беспроводной связи, сопровождающимся увеличением количества абонентских устройств (АУ) на городской территории и базовых станций (БС) для их обслуживания, наблюдается тенденция уменьшения размеров сайтов сетей сотовой связи до размеров в несколько сотен метров. Проведение анализа электромагнитной безопасности сотовых радиосетей для населения связано с применением моделей условий распространения радиоволн (РРВ) между БС и АУ для определения уровня полезного сигнала. Однако широко используемые эмпирические модели условий распространения радиоволн (РРВ), как правило, определены для расстояний между БС и АУ не менее 1 км и для ограниченной полосы радиочастот, поэтому необходима дополнительная оценка возможности их использования для малых размеров сайтов, характерных для городских сотовых сетей с микросотовой структурой. Для этого выполнено моделирование условий РРВ на расстоянии 0,1…1 км с использованием трехмерного алгоритма РРВ и трехмерной модели участка типовой городской застройки с высотой зданий 6-20 м при размещении АУ вне зданий на земной поверхности, а также выполнено сравнение оценок уровней входного сигнала, полученных с помощью эмпирических моделей (Окамура-Хата, COST231-Хата, COST231-Уолфиш-Икегами, Ли, Эриксон) и трехмерной многолучевой модели РРВ. Результаты оценок уровня сигнала, в наибольшей степени совпадающие с результатами, полученными с помощью трехмерной модели РРВ на рассматриваемой территории городской застройки, могут быть получены с помощью моделей условий РРВ Окамура-Хата, COST231-Хата и COST231-Уолфиш-Икегами; модели Окамура-Хата и COST231-Hata могут быть применены для расстояний между БС и АУ 0,4…1 км.

АКТУАЛЬНАЯ ПРОБЛЕМА БЕЗОПАСНОСТИ xPON

Н.Н. Сергеев, В.Н. Урядов

Наиболее серьезным недостатком xPON является незащищенность обратного канала от действий злоумышленников. На физическом уровне неисправность лазера обратного канала или контроллера этого лазера может вывести из строя всю систему. Такие случаи отслеживаются системами управления терминала. Однако, используя оптическую розетку