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

(ОРА), а доступ к ней получить весьма легко, злоумышленник так же может вывести из строя весь сегмент сети, путем примитивного засвета лазером в линию. Это произойдет в том случае, когда мощность излучаемого в линию сигнала превысит допустимую мощность фотодиода OLT. В xPON используется принцим временного разделения TDM [1], поэтому очевидно, что злоумышленник после некоторых манипуляций с перепрограммированием ONT или подключением ПК с установленным специальным программным обеспечением к ONT может добиться того, что будет получать информацию, адресованную другим пользователям, всего лишь подобрав необходимый интервал. Это можно сделать с каждой оптической розетки (ОРА). Снятие информации нисходящего потока достаточно просто реализуемо, поскольку обычный приемник обеспечивает прием сигнал любого приемника, если использовать другой временной интервал. Более сложна в реализации снятия информации контролируемого абонента с другой абонентской розетки поскольку используется отраженный сигнал от ответвителя или разъемного соединения [2] При использовании отраженного сигнала, необходимо учесть, что в пассивной оптической сети существуют возвратные потери в неоднородностях.

Литература

1. Урядов В.Н., Бунас В.Ю., Глущенко Д.В // Докл. БГУИР. 2012. № 8 (70). С. 81–87.
2. Булавкин И.А. // Технологии и средства связи. 2006. IW2. С. 104–108.

СНЯТИЕ ИНФОРМАЦИИ НИСХОДЯЩЕГО ПОТОКА В ПАССИВНОЙ ОПТИЧЕСКОЙ СЕТИ

Н.Н. Сергеев, В.Н. Урядов

Снятие информации нисходящего потока в пассивных оптических сетях достаточно просто реализуемо, поскольку обычный приемник обеспечивает прием сигнал любого приемника, если использовать другой временной интервал. Более сложна в реализации снятия информации контролируемого абонента с другой абонентской розетки поскольку используется отраженный сигнал от ответвителя или разъемного соединения. В случае передачи информации от ONT-1 к ONT-2 затухание будет весомым, а затухание сигнала на стыках и затухание сигнала в разъемном соединении будут небольшими. Возвратные потери определяют долю оптической мощности, которая возвращается обратно к источнику оптического сигнала. Основным фактором, определяющим возвратные потери, являются многократные френелевские отражения. С этой позиции разветвитель характеризуется затуханием на ближнем конце 50 дБ [1]. Квантовый предел детектирования определяется шумами, связанными с сигналами. Падающий на фотодиод стационарный световой поток генерирует пары носителей заряда как независимые случайные события» Такой процесс преобразования фотонов называется пуассоновским [2]. Таким образом, для того чтобы воспользоваться отраженным сигналом и снять информацию абонента с другой соседней оптической розетки, достаточно, чтобы величина отраженного сигнала была в рамках квантового предела детектируемости [3].

Литература

1. Рекомендация МСЭ-Т G.983.1. Широкополосные оптические сети доступа на базе пассивных оптических сетей.
2. Птицын Г.А. Живучесть динамических сетей телекоммуникаций. М.: МТУСИ. 2008. 48 с.
3. Урядов В.Н., Глущенко Д.В. // Современные средства связи : матер. XIV Междунар. науч.-техн. конф. Минск, 29 сент.–1 окт. 2009 г. С. 23.

ДВУМЕРНЫЕ ХАОТИЧЕСКИЕ ОТОБРАЖЕНИЯ В АЛГОРИТМАХ ХЕШИРОВАНИЯ

А.В. Сидоренко, И.В. Шакинко

На современном этапе развития информационных технологий особое место занимают вопросы, связанные с обеспечением безопасности передаваемых данных. Одной из ключевых задач информационной безопасности является контроль целостности данных. Для обеспечения контроля целостности данных традиционно используются алгоритмы хеширования [1]. Эти