

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 $\alpha=0.01$, что говорит о том, что обе последовательности носят случайный 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, Эрикссон) 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-Хата 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