ОРГАНИЗАЦИЯ ЗАЩИТЫ ДАННЫХ В СТАНДАРТЕ BLUETOOTH

Горягина Т.М., Трунов И.Л., Серогодский Д.И., Котегов М.Г., Лукьянов С.А.

Южный Федеральный Университет, Таганрогский Технический Институт

В последнее время технологии беспроводной связи применяются в самых разных областях деятельности человека. Это стало возможным благодаря созданию группы стандартов, отвечающих высоким эксплуатационным требованиям. Одним из них является стандарт Bluetooth. Изначально стандарт был разработан для подключения гарнитур к мобильным телефонам, но благодаря сочетанию хорошей пропускной способности (до 10 Мб/сек) и простоты программно-аппаратной реализации, область его применения очень расширилась. Сейчас системы Bluetooth инсталлируются на коммерческие транспортные средства для обеспечения связи с водителями, поддержки устройств «громкой» связи и для сбора данных, беспроводные устройства контроля физических параметров применяются в медицинских учреждениях. Такая популярность технологии накладывает повышенные требования на надежность и безопасность передачи данных. Существуют три основных типа атак на портативные устройства, оснащенные Bluetooth:

Bluejacking - используется способность устройств Bluetooth опознавать другие, расположенные поблизости устройства и посылать на них незапрошенные сообщения.

Bluesnarfing - используя этот прием, злоумышленник может соединиться с устройством, не сообщив об этом его владельцу, и получить доступ к сохраненным на аппарате данным.

Bluebug - атакующие способны установить последовательное соединение с устройством жертвы и использовать его для контроля за службами обмена данными этого аппарата.

Для решения проблемы защиты данных в стандарте Bluetooth, нами предлагается использование систем шифрования, основанных на кодах с иррациональным основанием

$$t = \frac{1+\sqrt{5}}{2},$$

получивших название кодов Фибоначчи. Эти системы обладают рядом свойств, на основе которых можно построить помехоустойчивые коды. Причем корректирующая способность кода будет определяться не длиной кодовой последовательности и вносимой избыточностью, а математическими свойствами предложенной системы счисления. Суть кодирования состоит в том, что каждый символ исходного сообщения может иметь несколько представлений в иррациональном коде. Избыточность закодированного сообщения в этом случае будет переменной. Такой подход, во-первых, позволяет построить помехоустойчивое кодирование и шифрование сообщения на одном математическом аппарате, а во-вторых, как показали экспериментальные исследования, требует очень незначительных вычислительных затрат, вполне допустимых для портативных устройств.