3. *Борисенко С.Ю., Воробьёв В.И., Давыдов А.Г.* Сравнение некоторых способов анализа фазовых соотношений между квазигармоническими составляющими речевых сигналов. / http:// *radio-technica.ru/wp-content/uploads/.../Секция-АР-Акустика-речи.pdf*. 2014.

4. А.с.1337829 СССР, МКИ[4] G01R29/00. Способ измерения характеристик радиотрактов / *Ю.М. Галаев, Б.В. Жуков* // Бюл. из. 1987. №34. С. 183.

КОНСТРУКТИВНЫЕ ОСОБЕННОСТИ ИМИТАТОРОВ РАДИОЗАКЛАДНЫХ УСТРОЙСТВ ДЛЯ РЕЗОНАНСНО-РЕФЛЕКТОМЕТРИЧЕСКОГО ЛОКАТОРА

В.И. Ворошень

Ранее сообщалось о функциональных особенностях резонансно-рефлектометрического локатора для обнаружения устройств несанкционированного съема информации [1]. Опытный образец локатора укомплектован имитаторами радиозакладных устройств (РЗУ). Имитаторы предназначены для калибровки локатора (проверки работоспособности) в условиях электромагнитной обстановки конкретного помещения непосредственно перед проведением поисковых мероприятий, а также для обучения персонала. В докладе обсуждаются конструктивные характеристики имитаторов РЗУ и некоторые экспериментальные результаты по их обнаружению.

Комплект из пяти имитаторов перекрывает частотный диапазон от 434 МГц до 2,4 ГГц. Конкретные частоты соответствуют диапазонам: ISM, GPS навигации и сотовой связи. Каждый имитатор имеет в своем составе традиционные компоненты беспроводных систем: микросхему приемопередатчика (для GPS-приемника), фильтры, соответствующие антенны. Микросхемы имеют «обвязку» из пассивных компонентов согласно рекомендациям по их применению. Функционально каждый имитатор представляет собой полноценный радио тракт потенциального РЗУ, находящегося в выключенном (дежурном) состоянии.

Конструктивно имитаторы выполнены на печатных платах одинакового размера 74×42×1 мм. Все компоненты (кроме антенн) расположены с одной стороны платы под электромагнитным экраном BMI-S-205-F 38×25×6 мм со съемной перфорированной крышкой. Обратная сторона печатных плат полностью металлизирована.

Указанные конструктивные решения, примененные по назначению, позволили получить ожидаемый результат по снижению эффективности обнаружения имитаторов с помощью нелинейных локаторов. Все пять имитаторов РЗУ не обнаруживаются с минимального расстояния (менее 5 см) следующими моделями локаторов: Катран SEL SP-61M, Лорнет-24, Лорнет-36. Некоторые операторы «диагностируют» имитаторы как коррозионный контакт, что можно непосредственно отнести к прижимному контакту между экранирующей рамкой и крышкой. Со снятой крышкой возможность обнаружения нелинейными локаторами восстанавливается; дальность составляет от 0,3 до 0,5 м.

С помощью резонансно-рефлектометрического локатора все имитаторы РЗУ обнаруживаются с расстояния не менее 1 м.

Литература

1. *Ворошень А.В., Ворошень В.И.* // Тезисы докладов XIII Белорусско-российской научно-технической конференции «Технические средства защиты информации» // Минск, БГУИР. 2015. С. 13.

ТЕХНОЛОГИЯ «INTEL ANTI-THEFT» КАК ИЛЛЮСТРАЦИЯ УГРОЗЫ ДЕСТРУКТИВНОГО ВОЗДЕЙСТВИЯ ПО РАДИОКАНАЛУ

В.И. Ворошень

Компьютер, поддерживающий технологию Intel AT, может быть деактивирован так называемой «таблеткой с ядом» (poison pill). Это зашифрованное SMS сообщение, которое передается через сеть 3G. Кроме того, в режиме блокировки ноутбук через заданные интервалы времени сообщает свои географические координаты. Для этой дополнительной функции отслеживания при покупке нужно заранее проверить наличие совместимого 3G/GPS модуля [1].

Цитату из рекламного описания продукта от Intel можно рассматривать не только как рекламу предотвращения кражи ноутбука, но и как описание возможности осуществления деструктивного воздействия, в том числе и по отношению к хранящейся информации. Кроме этого тезиса в докладе проводится анализ известных схемотехнических решений приемопередающих устройств, представляющих наибольшую угрозу осуществления подобного сценария.

Собственно обнаружение дополнительного модуля, установленного в ноутбуке или дисплее, возможно при разборке устройства или при проведении рентгенографических исследований. Сложности возникают в случаях с уникальной, дорогостоящей или громоздкой аппаратурой. В таких случаях на первый план выходят методы поиска радиозакладных устройств (РЗУ) по излучению гетеродина — с помощью приемников ближнего поля, например DetectIV. Действительно, практически все современные мобильные телефоны, включая GSM модули, строятся по схеме приемников прямого преобразования (с нулевой промежуточной частотой). Такое решение характеризуется повышенным излучением гетеродина, достигающим на антенном входе (выходе) десятков микроватт, что и является при поиске демаскирующим признаком.

В технике приборов на поверхностных акустических волнах (ПАВ) известна запатентованная архитектура ASH приемопередатчика (Amplifier-Sequenced Hybrid transceiver) [2]. По излучению гетеродина ASH приемник обнаружить практически невозможно даже при работе в непрерывном режиме, так как по принципу действия он является разновидностью приемника прямого усиления. Немаловажно, что габариты этих устройств на ПАВ гораздо меньше в сравнении с GSM модулями. Так размеры гибридной микросхемы ASH приемника RX5000 составляют всего 10×11×2 мм; для ее работы требуется всего несколько внешних конденсаторов.

Методика выявления РЗУ по резонансным явлениям в антеннах и сопутствующих фильтрующих элементах позволяет обнаруживать описанные ASH устройства. Здесь демаскирующим признаком является наличие высокодобротных фильтров на ПАВ на антенном входе. Экспериментально установлено, что приемник RX5000 и приемопередатчик TX3000 диапазона 434 МГц обнаруживаются резонансно-рефлектометрическим локатором с расстояния не менее 1 м.

Литература

1. Intel Anti-Theft — отряд специального назначения. Блог компании Intel. [Электронный ресурс]. Режим доступа: https://habrahabr.ru/company/intel/blog/137529/

2. ASH Transceiver Designer’s Guide. RF Monolithics, Inc. 2000.

КОМПЕНСАЦИЯ ВРЕМЕННОГО ЗАПАЗДЫВАНИЯ ИЗМЕРИТЕЛЬНОГО СИГНАЛА НА ВЫХОДЕ КАНАЛА УТЕЧКИ РЕЧЕВОЙ ИНФОРМАЦИИ

В.К. Железняк, И.Б. Бураченок, Д.С. Рябенко

Важным при оценке защищенности речевой информации является получение на выходе канала утечки (КУИ) параметров измерительного сигнала (ИС) с минимальной среднеквадратичной погрешностью. Случайное временное запаздывание выходного ИС по отношению к входному ИС, обусловленное прохождением через среду распространения, не позволяет получить его оптимальные параметры. Одной из задач является определение с наибольшей точность этого запаздывания.

Для получения значения временного запаздывания и его компенсации используют функцию взаимной корреляции между входным и задержанным выходным ИС. Максимум этой функции, полученный в условиях отсутствия запаздывания, определяет минимальную среднеквадратичную погрешность запаздывания ИС на выходе КУИ и его точку отсчета на временной оси. В точке максимального совпадения входного и выходного ИС производная от функции взаимной корреляции имеет S-образную форму, пересекающую нулевой уровень. Предложенный математический подход позволяет определить запаздывание по производной функции взаимной корреляции, установив положение точки на временной оси, в которой данная производная равна нулю. При наличии задержки, производная от функции взаимной корреляции устанавливает положение точки на временной оси, сдвинутое на величину задержки.

Максимальное значение времени когерентности входного и выходного ИС определяют отношением их комплексных значений функции взаимной корреляции при задержке выходного ИС относительно входного к их функции взаимной корреляции при компенсации задержки. Компенсация временного запаздывания с минимальной среднеквадратичной погрешностью повышает чувствительность и точность оценки защищенности речевой информации в КУИ.