ЗАЩИТА ИНФОРМАЦИИ ОТ УТЕЧКИ ПО КАНАЛАМ СОТОВОЙ СВЯЗИ

Н.С. Вернигоров
ООО «Вихрь»

Современные средства связи — мобильные телефонные аппараты — представляют собой многофункциональные устройства. Они позволяют:

- вести запись аудиоинформации на встроенный микроцифровой диктофон в течение четырех и более часов;
- хранить в памяти до 500 фотоснимков;
- вести видеозапись продолжительностью до одного часа с сохранением;
- осуществлять передачу по радиоэфиру аудио- и видеоинформации в режиме реального времени.

Запись аудио- и видеоинформации, а также ее передача в режиме реального времени могут осуществляться и без маскирующего признака. Достаточно включить мобильный телефон в заданный режим, не производя никаких скрытных действий в присутствии источника информации, и сведения будут автоматически либо записываться во встроенную память, либо сразу транслироваться на заданный адрес. В последнем случае телефон отключается от режима «вызов» и работает только в режиме «передача». При этом источник информации даже не подозревает, что данная конфиденциальная встреча на самом деле является доступной конкурирующей стороне.

Сегодня наиболее распространенными являются два метода нейтрализации сотовых телефонов. Первый метод основан на постановке помехи, препятствующей записи аудиоинформации на цифровой диктофон. Изделия, осуществляющие этот способ, известны как «шумотроны».

Рассмотрим возможности «шумотрона» по нейтрализации диктофона сотового телефона. Изделие проектировалось для блокировки миниатюрных диктофонов старого образца с механической системой кинематики и современных цифровых диктофонов. Безусловно, подавление записи на указанных устройствах осуществляется достаточно эффективно. Однако сведения о статистической вероятности подавления записи для этих примитивных записывающих устройств отсутствуют, то есть нельзя гарантировать эффективность блокировки наиболее распространенных моделей (например, цифровых диктофонов) с помощью постановки СВЧ-помехи.

Следует заметить, что эти записывающие устройства представляют собой весьма крупный объект для СВЧ-излучения. Это означает, что геометрические размеры устройств, предназначенных только для записи аудиоинформации (цифровых диктофонов), сравнимы с длиной волны СВЧ-излучения генератора помех, а также полностью сравнимы с геометрическими размерами современных сотовых телефонов. Именно геометрические размеры цифровых диктофонов позволяют осуществлять подавление (зашумление) записываемой аудиоинформации.

Вернемся к сотовому телефону. Попытка блокировать (поставить помеху) встроенный в сотовый телефон микроцифровой диктофон оказывается безрезультатной. Это связано с тем, что в мобильном телефоне плотность расположения радиоэлементов на один-два порядка выше, чем в любом примитивном цифровом диктофоне. Применяемая в «шумотронах» частота СВЧ-излучения уже не воспринимается внутренним схемотехническим решением сотового телефона с такой же эффективностью, как в цифровом диктофоне. Именно по этой причине ни один из производителей «шумотронов» не упоминает (не берет на себя ответственность) о том, что их устройство способно подавлять цифровой диктофон, встроенный в сотовый телефон. Что касается блокировки сотовых телефонов от передачи информации в режиме реального времени, то в данной ситуации «шумотроны» бессильны. Они не предназначены для выполнения этой задачи.

Второй метод основан на блокировке сотового телефона, которая может осуществляться двумя способами.

Первый способ основан на детектировании вызывного сигнала телефона и постановке акустической помехи для блокировки микрофона. К устройствам данного класса относятся изделия типа «Кокон». Дальность действия этих устройств составляет не более 30 см. Их назначение — защита собственного телефона от несанкционированного дистанционного прослушивания за счет постановки акустической помехи на микрофон сотового телефона. Эти устройства не пригодны для блокировки телефона собеседника.

Второй способ основан на перехвате входящего или исходящего СВЧ-сигнала сотового телефона, его идентификации и генерации такого же типа сигнала на несущей частоте генератора СВЧ-помехи, что позволяет заблокировать приемник телефона от сигнала абонента. Как правило, это устройства стационарного типа (например, серии «Мозаика») с радиусом действия до 15 м. Однако эти изделия не способны блокировать запись информации на внутренний встроенный носитель. Итак, мы имеем два вида изделий, пытающихся препятствовать утечке информации по каналу сотовой связи.

А теперь рассмотрим методику, позволяющую обнаружить, а затем и обойти наличие устройств первого типа — «шумотрона» или второго типа — постановщика помехи при передаче информации в режиме реального времени. Для этого заинтересованная в информации сторона устанавливает контрольное время, когда на ее телефон (что предпочтительнее) либо с ее телефона во время встречи производится контрольный звонок. Если в назначенное время, включая небольшой дополнительный интервал для повторного контрольного звонка, соединения не произошло, то, следовательно, работает генератор блокировки телефона для передачи информации в режиме реального времени. Решение — включаем стационарную запись разговоров на встроенный диктофон! Если же связь произошла, значит, постановщик помех, препятствующий передаче информации в режиме реального времени, отсутствует. На глазах у всех присутствующих включаем передачу информации в режиме реального времени. По условной фразе или слову, сказанному во время этого короткого сеанса связи, через некоторое время вновь идет вызов, в котором подтверждается, что информация идет без помех. Этим же способом можно обойти наличие в контролируемом помещении «шумотрона». Таким образом, очевидно, что заблокировать съем информации с помощью сотового телефона известными средствами зашумления невозможно.

Металлодетектор-рамка также не пригоден для этой цели. Несмотря на совершенство этих изделий, которые сегодня позволяют находить металлические предметы по зонам на профиле человеческой фигуры, этот тип обнаружителей не способен выявлять сотовые телефоны.

Существует еще один метод блокировки сотовых телефонов. Это так называемая нелинейная локация. Правда, здесь осуществляется не подавление, а раннее обнаружение сотовых телефонов и запрет на их использование во время конфиденциальных встреч. Если в первых двух случаях по защите информации принимающая сторона не может сказать, что сотовый телефон запрещен на время встречи, дабы не уронить собственное достоинство в глазах собеседников или партнеров, поскольку отношения строятся на взаимном доверии, то нелинейный локатор исключает ситуацию человеческого фактора «верю — не верю». Он просто обнаруживает сотовые телефоны и препятствует их наличию на оговоренной встрече. Не нарушая взаимных обязательств и не унижая достоинства собеседников, с помощью нелинейного локатора удается пресечь возможность утечки информации по каналу сотовой связи.

По нелинейным локаторам имеется много различной информации, в том числе и рекламной, но в основном она касается обнаружения скрытых устройств («жучков»). И только небольшая часть этой информации посвящена вопросу раннего обнаружения радиоэлектронных устройств любого типа, включая сотовые телефоны, с помощью нелинейного локатора, работающего в режиме «рамка».

Известно по крайней мере шесть наиболее популярных моделей локаторов, среди которых и локатор серии NR-900. Однако этот локатор не пригоден для работы в режиме «рамка», и поэтому в его рекламном проспекте отсутствует информация по данной возможности [1].

Единственная модель нелинейного локатора, предназначенного для работы в режиме «рамка», — это известный отечественный локатор серии «Циклон», который был создан для контроля вноса-выноса радиоэлектронных изделий и их компонентов в режиме «рамка» при скрытом досмотре на предприятиях [2]. Эффективность обнаружения радиоэлектронных приборов (в том числе сотовых телефонов) любых типов и размеров данным изделием составляет 95%, как во включенном режиме, так и в выключенном состоянии.

Примером острейшей задачи в мировой практике обнаружения и дальнейшего запрета применения сотовых телефонов во время конфиденциальных встреч является пенциарная система. Это относится к проблеме прав человека, которым в данной ситуации является адвокат, приходящий к своему подзащитному. Никто не имеет права произвести ручной досмотр — обыск адвоката для установления наличия у него сотового телефона. Но если адвокат во время конфиденциальной встречи со своим клиентом совершает действия, способствующие прямой утечке информации либо в режиме реального времени, либо записывая ее на встроенный диктофон по сокрытому сотовому телефону, это часто приводит к закрытию уголовного дела. То же самое имеет место и в предпринимательской деятельности, о чем было сказано выше.

Есть еще один актуальный аспект своевременного обнаружения сотовых телефонов. В умелых руках, особенно в руках террористов, сотовый телефон может использоваться как радиоуправляемый электронный взрыватель, который можно активизировать из любой точки планеты. Даже если удастся определить номер абонента, звонившего на активизацию взрывного устройства, это не означает, что террорист будет установлен. Ведь активация может осуществляться с украденного сотового телефона, бывший владелец которого не имеет никакого отношения к диверсионному акту.

Очевидно, что только применение беспристрастных технических средств, сигнализирующих о наличии у посетителей электронных устройств, позволяет на законном основании, без нарушения прав человека (не применяя ручной обыск) обеспечить запрет применения во время конфиденциальных встреч сотовых телефонов как средства утечки секретной информации и возможного инструмента для террористических акций.

ЛИТЕРАТУРА

1. Вернигоров Н.С. К вопросу о выборе нелинейного локатора для раннего обнаружения устройств звукозаписи и передачи информации по радиоэфиру //Конфидент. — 2001. — № 4.
2. Вернигоров Н.С., Кузнецов Т.В., Усольцев А.А. Некоторые особенности характеристик нелинейных локаторов // Информост. — 2002. — № 5.