пассивные методы защиты от электромагнитных излучений экранируя их, что позволит значительно увеличить время работы за автоматизированным рабочим местом.

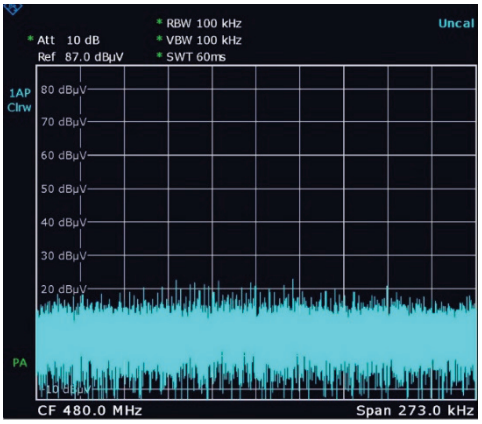

Рис. 4. Спектр излучение
от экранированного USB-flash-носителя

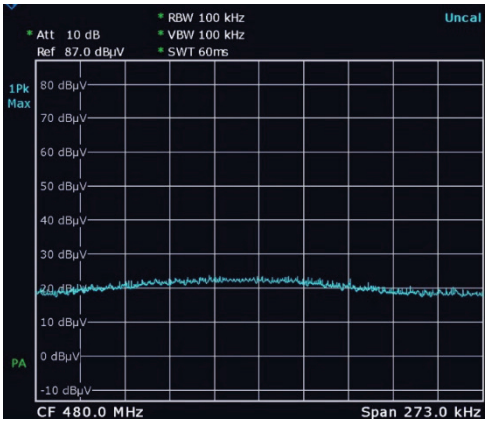

Рис. 5. Спектр излучения от
экранированного USB-flash-накопителя,
собранный в виде накопления
максимальных уровней излучения

Список литературы

1. *Гоноровский И. С.* Радиотехнические цепи и сигналы : учебник для вузов. Изд. 3-е, перераб. и доп. М. : Сов. радио, 1986. С. 25–27.

2. *Кобяков В. Ю., Лучинин А. С.* Обнаружение ПЭМИ проводников и коннекторов при передаче интерфейсу USB // Вестн. УрФО. Безопасность в информационной сфере. 2010. № 4 (14) С. 4–8.

3. Инструкция Соната Р3.1 НПО «АННА».

УДК 004

Е. И. Патраков
Научный руководитель: д-р тех. наук, проф. С. В. Поршнев
Уральский федеральный университет, Екатеринбург

АППАРАТНЫЕ И ПРОГРАММНЫЕ СРЕДСТВА ПЕРЕХВАТА СОТОВОЙ СВЯЗИ

Аннотация. Статья посвящена изучению средств перехвата сотовой связи. Описаны два типа таких систем: аппаратные (активные и пассивные) и программные. Рассмотрены их основные характеристики и принцип работы. Предложены средства и методы противодействия таким системам.

Ключевые слова: аппаратные и программные средства перехвата сотовой связи; мобильный телефон; базовая станция; оператор сотовой связи; данные.

Мобильные телефоны широко применяются для организации связи между несколькими абонентами. Система передачи данных состоит из следующих компонентов: «источника», «приемника» и «канала передачи». Источником является сотовый телефон одного абонента, приемником — мобильное устройство другого абонента, каналом передачи — физическое поле, с помощью которого информация передается от первого абонента ко второму, и наоборот. Стоит отметить, что сотовый канал связи является разновидностью электромагнитного канала, поэтому для него характерен следующий недостаток — несанкционированное прослушивание. Перехват информации может осуществляться с помощью программных и аппаратных комплексов, которые позволяют получить доступ к чужим данным. В настоящее время необходимо иметь представление не только о системах перехвата сотовой связи, но и знать средства и методы противодействия таким устройствам.

Ключевой особенностью сотовой связи является то, что зона покрытия делится на соты, в рамках которых находятся базовые станции. Базовые станции взаимодействуют с несколькими приемопередатчиками, которые обычно располагаются на крышах зданий, либо вышках.

Принцип действия сотовой связи заключается в следующем. Мобильное устройство прослушивает эфир и находит сигнал ближайшей базовой станции, после чего подключается к ней. После установления связи станция и мобильное устройство начинают обмениваться пакетами передачи данных. Если телефон выходит из зоны действия одной станции, он начинает искать связь с другой. Дальше вызов с базовой станции идет по проводным линиям связи на центральный пункт, который называется коммутатором оператора связи. Коммутатор собирает информацию сразу с нескольких станций и перенаправляет другим абонентам. Таким образом, можно выделить три участка, на которых возможно несанкционированное прослушивание и съем информации:

– радиолиния между сотовым телефоном и базовой станцией;
– линия между базовой станцией и коммутатором;
– коммутатор.

Одним из методов прослушивания сотового телефона является внедрение устройства в радиолинию между мобильным телефоном и базовой станцией. Такой метод чаще всего характерен для аппаратных средств перехвата сотовой связи.

Аппаратные средства перехвата сотовой связи. В настоящее время существует два метода перехвата сотовой связи с помощью аппаратных средств: пассивный и активный методы.

Пассивный метод заключается в получении доступа к каналу связи между абонентом и приемопередающей антенной базовой станции. Злоумышленник для реализации данного метода использует сканирующую аппаратуру с необходимым программным обеспечением. Наблюдение за каналом связи осуществляется посредством радиомониторинга определенного диапазона. Так, например, частотный диапазон для стандарта GSM-900 составляет от 890 до 960 МГц, для стандарта GSM-1800 — от 1710 до 1880 МГц, для стандарта GSM-1900 — от 1900 до 1990 МГц.

В качестве примера можно привести комплекс перехвата сотовой связи GSS Pro-A. Данная система является одной из лучших систем прослушивания GSM канала непосредственно с радиоэфира. Комплекс GSS Pro-A осуществляет многоканальный перехват сотовых телефонов, запись разговоров, обладает функцией по декодированию и дешифрованию данных. Помимо вышеперечисленного, система GSS-ProA имеет возможность перехватывать SMS, определять местоположение абонента с точностью до двух метров, распознавать голос абонента, отслеживать мобильное устройство на расстоянии до 500 метров.

Активный метод перехвата сотовой связи заключается в активном вмешательстве в эфир между сотовым телефоном и базовой станцией. Результатом данного вмешательства является изменение процесса аутентификации и замена протоколов управления. Данные с мобильного средства поступают на устройство перехвата сотовой связи, после чего отправляются на базовую станцию оператора. Для реализации данного метода используются специальные мобильные комплексы.

В качестве примера устройства, реализующего активный метод перехвата сотовой связи, можно привести систему AIBIS-2. Данный комплекс способен перехватывать входящие и исходящие звонки и SMS. Помимо этого, такая система способна записывать разговоры в режиме реального времени, анализировать полученные данные, перехватывать IMSI, выборочно подавлять трафик в некотором диапазоне. Отличительной особенностью данного комплекса является пеленгация положения заданного объекта с точностью до нескольких метров.

Программные средства перехвата сотовой связи. В настоящее время существуют приложения, которые позволяют осуществлять контроль над мобильными телефонами. Контроль над смартфоном заключается в том, что некоторые программы позволяют прослушивать входящие и исходящие звонки, просматривать SMS и письма электронной почты, дистанционно включать диктофон и микрофон на устройстве, определять местоположение абонента и т. д.

Принцип работы таких приложений один и тот же. Программа слежения за пользователем мобильного устройства отправляет данные со смартфона на промежуточный сервер в сети Интернет. Злоумышленник с помощью личного

кабинета получает доступ к серверу, на котором хранятся данные, выгруженные с мобильного телефона жертвы. Стоит отметить, что такие приложения работают незаметно для владельца смартфона, явно не обнаруживаются в файловой системе и в запущенных процессах телефона. Признаком внедрения такого приложения может быть увеличение объема принимаемых и отсылаемых данных посредством сети Интернет или постоянно разряжающийся аккумулятор смартфона.

К популярным программам слежения относятся: FlexiSPY Extreme, Pro-X и Full от компании MobControl. Найти их в свободном обращении в сети Интернет практически невозможно, как и другие программы слежения.

Таким образом, получить и перехватить данные с мобильного устройства можно с помощью специально внедренных аппаратных закладок, без использования сложных технических средств физического перехвата сотовой связи. Для того чтобы защититься от внедрения программных средств перехвата сотовой связи, достаточно придерживаться следующих правил:

– обеспечить противодействие несанкционированному доступу к мобильному устройству;
– предусмотреть меры по защите смартфона от внедрения вредоносных приложений.

Для предотвращения перехвата информации с помощью аппаратных средств можно использовать приложения, которые позволяют выявить ложные базовые станции и отследить любую подозрительную активности в сети, в том числе при использовании SMS.

УДК 004.056.53

И. Ю. Петров
Научный руководитель: д-р тех. наук, проф. С. В. Поршнев
Уральский федеральный университет, Екатеринбург

ОБНАРУЖЕНИЕ ПЭМИ С ПОМОЩЬЮ RTL-SDR-ПРИЕМНИКА

Аннотация. Проведен анализ возможностей ТВ-тюнера на чипе RTL2832U по захвату и оцифровке радиосигнала с целью его использования в составе программно-определяемой радиосистемы.

Ключевые слова: информационная безопасность; побочные электромагнитные излучения; программно-определяемая радиосистема; радиомониторинг эфира.