УДК: 681.2

МЕТОДЫ ПОВЫШЕНИЯ ЭФФЕКТИВНОСТИ ВЫЯВЛЕНИЯ ЭУНПИ, ВЫПОЛНЕННЫХ НА ОСНОВЕ МОДУЛЕЙ СОТОВОЙ СВЯЗИ СТАНДАРТА GSM900\1800 СРЕДСТВАМИ, РАДИОМОНИТОРИНГА

Белорусов Дмитрий Иванович (Belorusov Dmitry Ivamovich),
ООО «РИКОМ» (г. Москва, ул. Ибрагимова, д. 31\47, email: belorusov@rusmonitor.ru)

В настоящей статье будут рассмотрены особенности обнаружения средствами радиомониторинга электронных устройств негласного получения информации (ЭУНПИ), выполненных на основе модулей сотовой связи стандарта GSM900\1800.
Основной целью настоящей статьи является описание методов активного воздействия радиосигналами специальной формы на приемо-передатчик модуля GSM, входящего в состав ЭУНПИ, с целью повышения эффективности их обнаружения.

1. Актуальность проблемы.

Технические средства ЭУНПИ непрерывно эволюционируют. В 90х годах они, в основном, были представлены аналоговыми радиомикрофонами с ЧМ модуляцией. В начале 2000х появились радиоканалы с цифровыми видами модуляции сигнала, аналоговые радиомикрофоны получили цифровые каналы управления. Примерно в это же время разработчики ЭУНПИ обратили внимание на технологии сотовой связи, в частности на широко распространённую технологию GSM.

Почему именно GSM? Во-первых, сети GSM на то время и по сей день предоставляют наибольшую зону покрытия. Во-вторых, изготовление ЭУНПИ на основе стандартных GSM модулей, не представляет технической сложности. В распоряжении разработчиков ЭУНПИ оказалась технология одновременно позволяющая: повысить скрытность работы ЭУНПИ, за счет использования радиосигнала с псевдослучайной перестройкой рабочей частоты (ППРЧ) и цифровой модуляцией сигнала (GMSK); передавать голосовой трафик и данные (GPRS и EDGE); осуществлять удаленную активацию и управление режимами работы ЭУНПИ (AT-команды и DTMS коды).
Не удивительно, что в настоящее время рынок ЭУНПИ насыщен радиомикрофонами на основе модулей стандарта GSM (рис 1.). Применение таких устройств не требует специальных навыков и не сложнее, чем пользование обычным сотовым телефоном. В то же время выявления таких устройств обычными средствами радиомониторинга оказывается затруднительным.

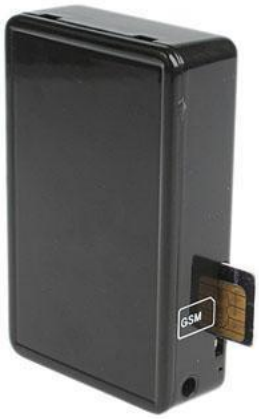

Рис.1
Радиомикрофон на основе GSM модуля

2. Режимы GSM [1].

Рассмотрим состояния, в которых может находиться радиомикрофон, выполненных на основе модуля GSM, и демаскирующие признаки, по которым он может быть обнаружен средствами радимониторинга.

После включение мобильная станция GSM, в том числе и устройство ЭУНПИ, выполненное на основе модуля GSM, должно выполнить процедуру регистрации в сети “registration” (здесь и далее название процедур будут даны в синтаксисе стандарта GSM). В процессе регистрации сеть идентифицирует мобильную станцию по адресам IMEI[1] и IMSI[2], назначает ей рабочие параметры и присваивает статус «idle».

Устройство в состоянии «idle» находится в режиме ожидания вызова. В этом состоянии радиообмен мобильной станции с сетью сведен к минимуму, а именно, мобильная станция лишь должна периодически подтверждать сети свой статус процедурой периодической регистрации «periodic registration» (обычно интервал периодической регистрации составляет около 1 минуты).

При поступлении входящего вызова или при инициировании вызова с мобильной станции устройство переходит в режим активного радиообмена с сетью- «active».

Таким образом, можно выделить два основных режима, в которых устройство GSM может быть обнаружено средствами радиомониторинга в произвольный момент времени: режим ожидания и режим активного радиообмена.

Далее рассмотрим особенности организации радиоинтерфейса GSM. В стандарте GSM используется комбинированное частотно-временное (FDMA\TMDA) разделение доступа к ресурсам сети. Каждая мобильная станция передает сигнал в радиоэфир не постоянно, а только в своем временном окне, которое выделено ей сетью в TDMA кадре. Это возможно благодаря тому, что речь сжимается и может быть передана за гораздо меньший промежуток времени, чем она занимала в не сжатом виде. Длительность передачи одного временного окна 576,6 мкс. Вне своего временного окна мобильная станция радиосигнал в эфир не передает. Передача возобновляется в следующем TDMA кадре через 4.63 мс.

Передача радиосигнала мобильной станцией осуществляется на одной из 124 FDMA несущих в диапазоне от 880 до 915 МГц для GSM900 и одной из 374 несущих в диапазоне 1710-1785 МГц для GSM1800. Переключение рабочих частот между несущими осуществляется последовательно в процессе сеанса связи по псевдослучайному закону скоростью 217 скачков в секунду (ППРЧ). Приемник мобильной станции настроен на диапазон частот базовых станций, который расположен выше по частоте на 45МГц (для GSM900) и 95 МГц (для GSM 1800).

Обнаружение радиообмена мобильной станции GSM, находящейся в режиме активного радиообмена с сетью (состояние “active”), может быть успешно реализовано методом панорамного анализа спектра в любом современном средстве радиомониторинга. Для устройств, находящихся в режиме ожидания (состояние “idle”), обнаружение существенно усложняется тем, что длительность радиообмена трубки в режиме регистрации – это единицы миллисекунд, а период периодической регистрации около минуты. Вероятность обнаружения такого короткого сеанса связи в энергетическом спектре, при панорамном обзоре в широкой полосе частот, даже высокоскоростным средством радиомониторинга, стремиться к нулю.

Поскольку обмен в протоколе GSM защищен шифрованием и идентификаторы мобильных устройств передаются в эфир достаточно редко, то очевидно, что метод

---

[1] IMEI — международный идентификатор мобильной станции, уникальный для каждого использующего его аппарата.. IMEI играет роль серийного номера аппарата и передаётся в эфир при регистрации в сети.

[2] IMSI— международный идентификатор мобильного абонента (индивидуальный номер абонента), ассоциированный с каждой SIM картой. Во избежание перехвата, этот номер посылается через сеть настолько редко, насколько это возможно — в тех случаях, когда это возможно, вместо него посылается случайно сгенерированный временный номер- TMSI.

панорамного анализа спектра абсолютно бесполезен для идентификации обнаруженных мобильных станций, в том числе по принципу свой-чужой или для определения количества мобильных станций, обнаруженных в зоне радиовидимости. Локализация обнаруженных устройств, находящихся в режиме ожидания, обычными средствами радиомониторинга не решается в принципе, а в режиме активного радиообмена существенно затруднена ППРЧ.

Таким образом, метод панорамного анализа спектра, достаточный для обнаружения активного радиообмена ЭУНПИ на основе модулей GSM, не может быть эффективно применен для обнаружения этих устройств, находящихся в режиме ожидания и для идентификации и локализации обнаруженных устройств в обоих режимах работы.

3. Методы повышения эффективности обнаружения GSM модулей в режиме ожидания.

Далее рассмотрим специальные методы активного воздействия на приемо-передатчик устройства GSM, позволяющие существенно повысить эффективность обнаружения и\или локализации ЭУНПИ, выполненных на основе модулей GSM: метод подавления базовой станции и метод радиотестера. Суть обоих рассматриваемых методов в принудительном переводе мобильных станций GSM из режима ожидания в режим регистрации или в режим активного радиообмена.

3.1 Метод блокирования сигналов базовой станции.

Метод заключается в кратковременном (около минуты) блокировании сигналов базовых станций на входе приемника модуля GSM. В соответствие протоколом GSM, если мобильная станция вышла за пределы радиочастотного покрытия или в случае разрядки батарей для того, чтобы избежать бесполезного использования ресурсов для вызова, по истечении определенного промежутка времени, сеть изменяет статус мобильной станции на «implicit detach». Мобильные станции, со статусом «implicit detach», для возобновления работы в сети должны снова выполнить процедуру регистрации в сети «registration». Поэтому, если мобильная станция по каким-то причинам не принимает сигналы базовых станций в течение интервала периодической регистрации, она самостоятельно выполняет процедуру регистрации в сети. Используя эту особенность протокола GSM, совмещая подавление диапазона частот приема мобильных станций (передачи базовых станций) и анализ спектра в диапазоне передачи мобильных станций после отключения подавления, удается спровоцировать GSM модуль на радиообмен с сетью для выполнения процедуры регистрации, который может быть зафиксирован, в том числе, методом панорамного анализа спектра.

Очевидно, что метод блокирования сигналов базовой станции, ничего не дает для идентификации обнаруженных устройств и даже для определения их точного количества, поскольку устройства могут регистрироваться в сети на одной или нескольких частотах, а два устройства могут зарегистрироваться на одинаковых частотах в разных временных окнах. Так же этот метод не позволяет локализовать обнаруженные устройства, поскольку длительность регистрации недостаточна для локализации, а возможное автоматическое изменение мощности мобильной станции в процессе регистрации, делает локализацию амплитудным методом бессмысленной.

3.2 Метод радиотестера.

Современной альтернативой методу блокирования базовых станций является метод радиотестера.

Суть метода заключается в формировании радосигнала не отличимого, с точки зрения мобильной станции, от сигнала базовой станции как по радиоинтерфесу, так и по логической структуре обмена.

Особенностью протокола GSM является то, что приемник мобильной станции постоянно сканирует каналы базовых станций в поисках базовой станции с сигналом лучше, чем у той на которой мобильная станция зарегистрирована.

Если качество сигнала радиотестера окажется лучше, чем у реальной базовой станции, мобильная станции выполняет регистрацию на радиотестере автоматически.

После того, как модуль GSM, входящий в состав ЭУНПИ, выполнит регистрацию на радиотестере, становится возможным:
- четко зафиксировать наличие в зоне радиовидимости устройств ЭУНПИ, выполненных на основе модулей GSM;
- точно определить количество обнаруженных устройств;
- получить IMEI адрес GSM модуля и идентифицировать обнаруженные устройства по принципу «свой-чужой»;
- определить адрес SIM-карты GSM модуля и идентифицировать оператора, который выпустил SIM-карту (страну происхождения SIM-карты);
- после принудительной регистрации на радиотестере GSM модуль ЭУНПИ может быть переведен в режим контролируемого радиообмена так, что рабочая частота и мощность передатчика GSM модуля ЭУНПИ будет зафиксирована и известна оператору радиотестера (режим ППРЧ отключен) и при этом GSM модуль будет постоянно обмениваться информаций с радиотестером. В таком режиме местоположение устройства ЭУНПИ может быть локализовано с помощью любой направленной антенны подключенной к радиотестеру.

Важно отметить, что при реализации всех возможностей радиотестера не происходит вмешательство в работу оператора связи и поэтому радиотестер не является, так называемым, средством СТС и не имеет законодательных ограничений по применению.

Выводы.

ЭУНПИ, выполненные на основе модулей GSM, могут быть эффективно обнаружены методом панорамного анализа спектра только в режиме активного радиообмена.

Для обнаружения в режиме ожидания необходимо применение специальных методов активного воздействия на приемо-передатчик GSM модуля, входящего в состав ЭУНПИ, которые приводят к принудительному переводу устройства из режима ожидания в режим радиообмена или регистрации.

Наилучшую эффективность из специальных методов активного воздействия имеет метод радиотестера, который дает полную информацию об обнаруженных устройствах, позволяет их идентифицировать по IMEI и IMSI адресам и локализовать их местоположение.

[1] Обзор Системы GSM. - М.: Вымпелком, 2004