

ИМИТАТОР БАЗОВОЙ СТАНЦИИ

«МИРАЖ»



Руководство по эксплуатации

2018 г.

1. ВВЕДЕНИЕ

Настоящее руководство предназначено для обеспечения правильной эксплуатации изделия «Имитатор базовой станции Мираж» (далее по тексту – изделие).

Руководство по эксплуатации содержит описание состава изделия, основных принципов работы изделия, использования его по назначению, рекомендации по техническому обслуживанию и ремонту, хранению и транспортировке, а также другие сведения, необходимые для правильной эксплуатации изделия.

2. ОПИСАНИЕ ИЗДЕЛИЯ

2.1. Назначение и область применения

Имитатор базовой станции «Мираж» предназначен для поиска и идентификации электронных устройств негласного получения информации, использующих каналы передачи стандарта цифровой мобильной сотовой связи GSM. Также изделие предназначено для поиска ложных базовых станций, работающих в стандартах E-GSM, DCS1800, GSM850, PCS1900, GSM450, GSM480, GSM-R.

Режим работы изделия круглосуточный, непрерывный.

2.2. Состав изделия

Состав изделия приведен в Таблице 1.

Таблица 1

№ п/п	Наименование	Кол-во, шт.	Примечание
1.	Радиомодуль в переносном кейсе	1	-
2.	Антенны штыревые	2	-
3.	Кабель питания	1	-
4.	Интерфейсный кабель (патч-корд)	1	-
5.	ПЭВМ портативная типа ноутбук	1	опционально
6.	Управляемый подавитель сигналов «Мозаика-НВ»	1	опционально
7.	Специализированное программное обеспечение (СПО)	1	на диске
8.	Комплект эксплуатационной документации	1	комплект

2.3. Технические характеристики

Основные технические характеристики приведены в Таблице 2.

Таблица 2

№ п/п	Наименование параметра	Значение	Примечание
1.	Анализ базовых станций сотовых операторов	Поэтапное сканирование каналов связи операторов с последующим анализом.	-

№ п/п	Наименование параметра	Значение	Примечание
2.	Активный поиск устройств сотовой связи	Работа в режиме работы ложной базовой станции стандартов GSM 900/1800	Для перевода закладных устройств, работающих в нескольких стандартах сотовой связи, рекомендуется осуществлять подавление стандартов UMTS/LTE
3.	Выходная мощность радиопередатчика	100 мВт	Максимальное значение
4.	Габаритные размеры радиомодуля	474x415x149 мм	ШxВxГ, не более
5.	Вес радиомодуля	3 кг	-

2.4. Устройство и работа изделия

Основные функциональные узлы изделия работают следующим образом:

Радиомодуль в переносном кейсе представляет собой дуплексный приемопередатчик. Антенные устройства представляют собой две внешние штыревые антенны. Радиомодуль формирует и излучает в пространство сигналы, идентичные сигналам базовой станции стандарта GSM, и, одновременно, принимает сигналы устройств сотовой связи.

ПЭВМ портативная в комплекте с СПО предназначена для управления имитатором базовой станции, а также для документирования, хранения и обработки результатов поиска.

3. ИСПОЛЬЗОВАНИЕ ПО НАЗНАЧЕНИЮ

3.1. Подготовка изделия к использованию

3.1.1. Перед первым использованием изделия необходимо распаковать, сверить фактическую комплектность с указанной в эксплуатационной документации (паспорте или формуляре), провести внешний осмотр на отсутствие механических повреждений. После транспортирования при отрицательных температурах изделие должно быть выдержано в нормальных климатических условиях в упаковке не менее 2 часов.

3.1.2. Подсоединить антенны к радиомодулю.

3.1.3. Подключить радиомодуль и управляющую ПЭВМ к сети электропитания 220В, 50 Гц.

3.1.4. Соединить радиомодуль с управляющей ПЭВМ с помощью интерфейсного кабеля.

3.2. Порядок включения

3.2.1. Включить ПЭВМ, дождаться загрузки операционной системы.

3.2.2. Нажать на кнопку включения, расположенную на лицевой панели радиомодуля, при этом загорится светодиод, свидетельствующий о запуске изделия.

3.2.3. После загрузки операционной системы запустить СПО, при помощи соответствующего «ярлыка».

3.2.4. Выключение изделия производить в обратном порядке.

Настройка сети


3.3.1. Для работы ИБС необходимо установить сетевые настройки адаптера сети Ethernet.

3.3.2. Для входа в меню настроек сети перейдите: "Пуск" – "Панель управления" – "Сеть и Интернет" – "Центр управления сетями и общим доступом" – "Изменение параметров адаптера". Далее следует выбрать адаптер локальной сети "Подключение по локальной сети", нажать правую кнопку мыши и выбрать "Свойства".

3.3.3. В открывшемся окне выбрать "Протокол Интернета версии 4 (TCP/IPv4)" и нажать кнопку "Свойства". В появившемся окне установить значения:

- **IP-адрес 192.168.1.11;**

- **Маска подсети 255.255.255.0.**

3.3.4. Для работы с подавителем Мозаика-НВ, необходимо наличие второй сетевой карты для управляющей ПЭВМ. Настройки сети производятся в соответствии с инструкцией по эксплуатации на подавитель. В программе управления имитатором базовой станции в меню настройки  необходимо выставить необходимые значения IP-адреса подавителя, номера порта, и пароля для авторизации.

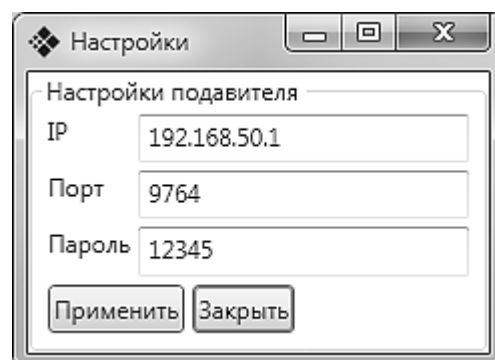


Рисунок 2 – Настройки подавителя

3.3. Использование по назначению

Интерфейс программы управления представлен на Рисунке 2.

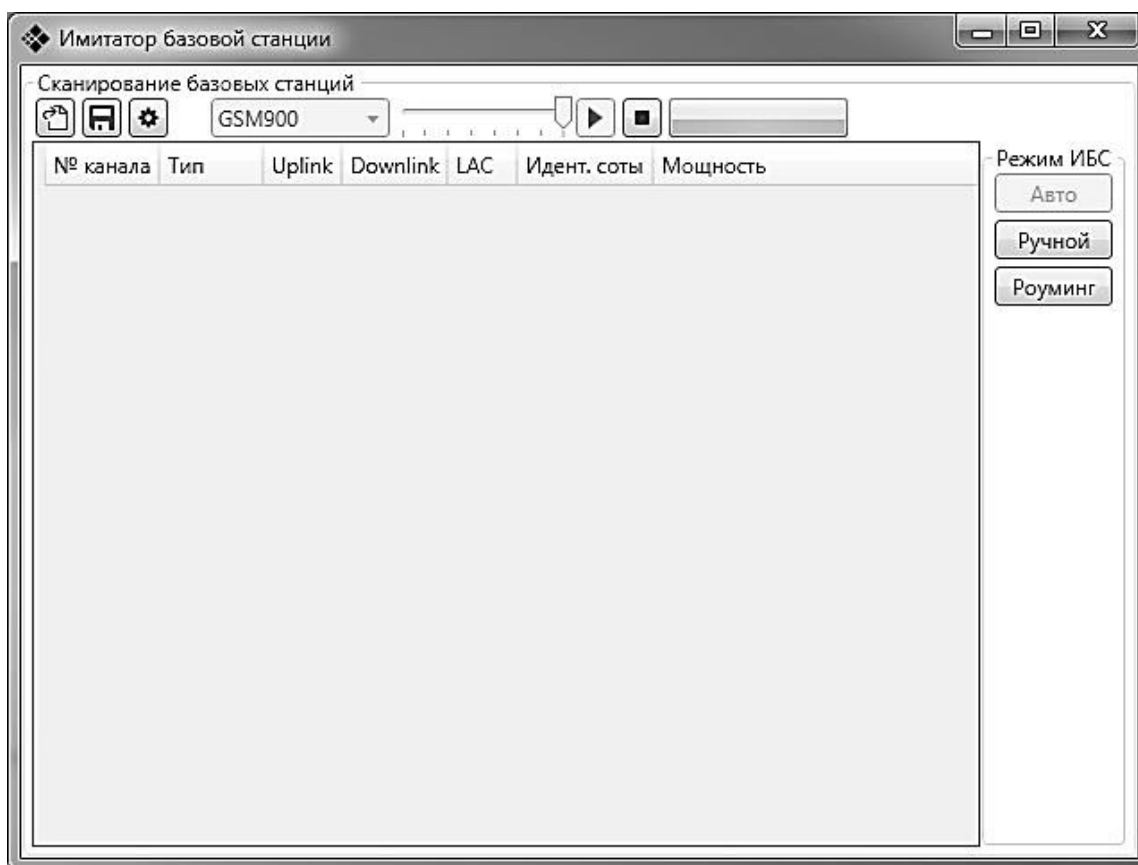


Рисунок 2 – Интерфейс программного обеспечения

Работа имитатора базовой станции (ИБС) состоит из двух базовых режимов. В первом режиме производится анализ каналов связи сети GSM. Второй режим, заключается в имитации базовой станции одного из выбранных операторов сотовой связи.

Анализ каналов связи сети GSM:

1) Выбрать стандарт GSM, для которого необходимо провести анализ. Доступные стандарты сканирования представлены в Таблице 3:

Таблица 3

№ п/п	Стандарт сети GSM	Диапазон частот сканирования	Примечание
1.	E-GSM-900	925.0 – 960.0	Результаты сканирования необходимы для работы ИБС с автоматическими настройками, и для поиска ложных базовых станций
2.	DCS-1800	1805.2 – 1879.8	
3.	GSM-850	869.2 – 893.8	Результаты сканирования необходимы для поиска ложных базовых станций
4.	PCS-1900	1930.2 – 1989.8	
5.	GSM-450	460.6 – 467.6	
6.	GSM-480	489.0 – 496.0	
7.	GSM-R	921.0 – 960.0	

Выбрать диапазон сканирования

Выбрать необходимый коэффициент усиления (по умолчанию 40 дБ)

Выполнить сканирование, нажав на кнопку

2) Сканирование, в зависимости от выбранного диапазона длится 5-15 минут. Результатом сканирования является список активных каналов связи, в которых содержится информация о стандарте, частотах восходящего (ВКС) и нисходящего (НКС) каналов связи, коде страны (MCC), коде оператора (MNC), мощности сигнала базовой станции, имени оператора, а также о доступных каналах, наиболее эффективных для работы имитатора (для стандартов E-GSM-900, DCS-1800). При наведении курсором мыши на строку группировки каналов, выводится информация об операторе. Пример работы представлен на Рисунке 3. Список каналов, доступных для эффективной работы имитатора, представлен на Рисунке 4.

Примечание. Отсутствие информации об операторе, и нулевые значения MCC и MNC, свидетельствует о потере данных в процессе сканирования. При необходимости идентификации данного канала, процедуру сканирования необходимо повторить

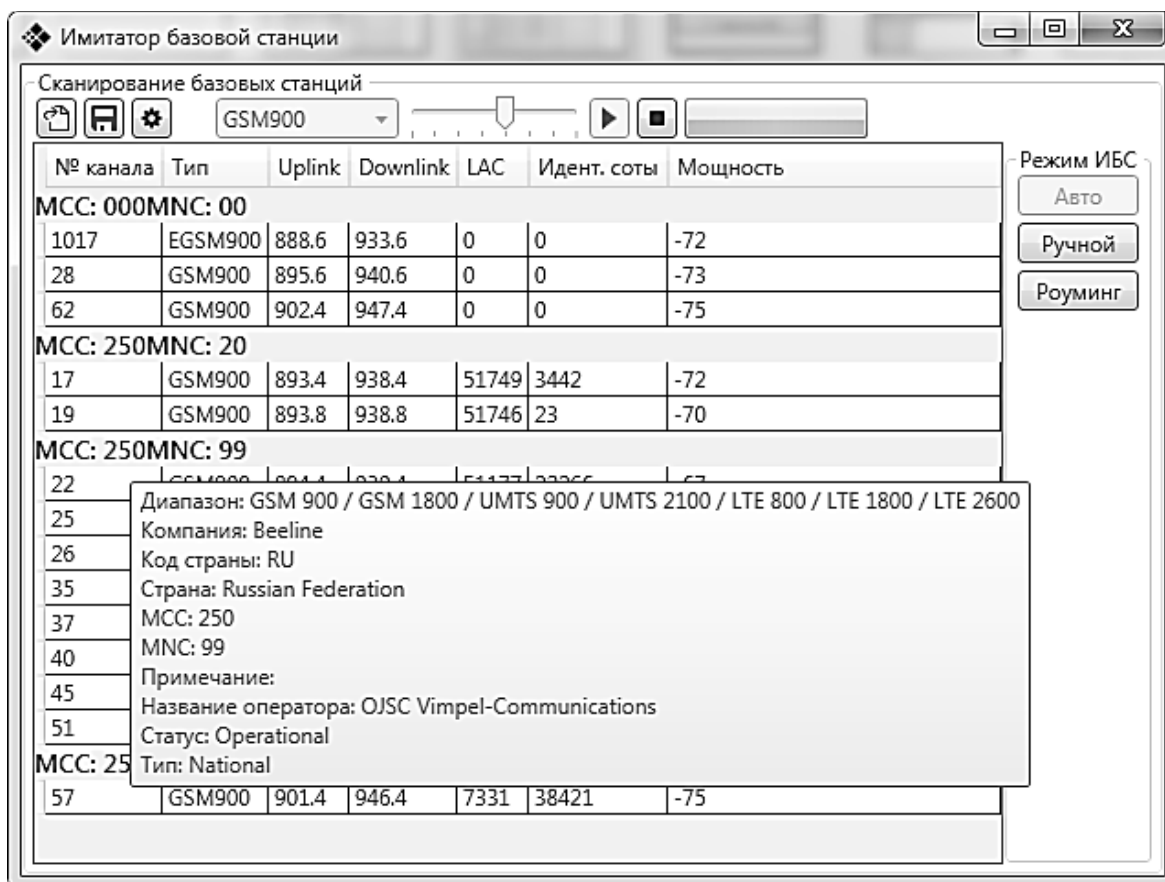


Рисунок 3 – Результат работы сканирования

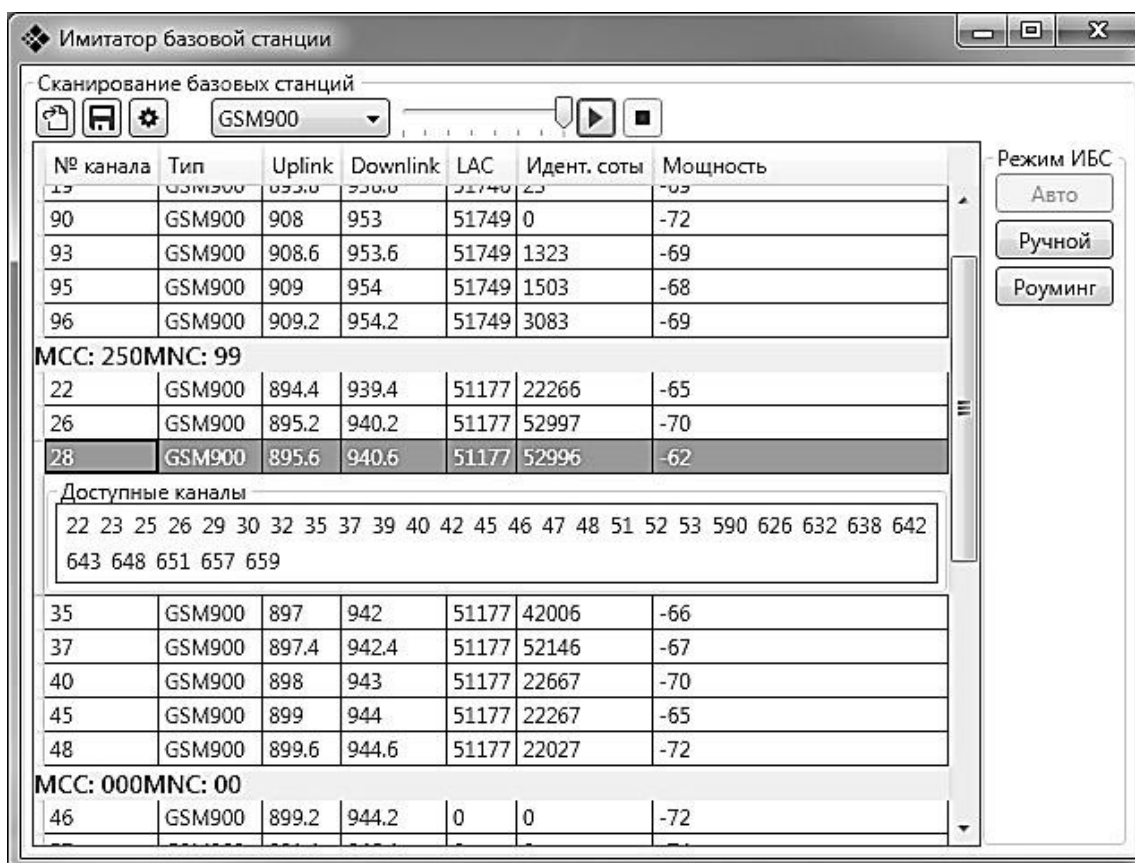


Рисунок 4 – Каналы, доступные для имитации в режиме «Авто»

3) Анализ ложных базовых станций производится оператором по следующим параметрам:

- Код страны (MNC) базовой станции отличается от кода России (250);
- Код оператора (MCC) отличается от кодов операторов сотовой связи России. Актуальный на 2018 год список операторов России представлен в Приложении 1;
- Код локальной зоны (LAC) существенно отличается от LAC-ов базовых станций данного оператора сотовой связи, находящихся в одной локальной территории;
- Возникновение новой, ранее отсутствующей базовой станции с мощным уровнем сигнала;
- Обнаружение сигналов базовых станций на частотах стандартов, отсутствующих в России в целом или в регионе, в частности (например, обнаружение базовых станций, работающих в американских стандартах GSM-850, PCS-1900).

ВНИМАНИЕ!

Не рекомендуется выполнять сканирование, при включенном подавителе сигналов сотовой связи. Это может привести к выходу из строя приемной части комплекса.

Работа имитатора базовой станции:

Правильная работа ИБС осуществляется либо в экранированном помещении, либо в неэкранированном помещении с помощью подавителя сигналов сотовой связи. ИБС имеет три режима работы:

- Режим работы с автоматическими настройками конфигурации ИБС;
- Режим перевода закладных устройств в роуминг;
- Ручной режим работы.

Работа в экранированных помещениях:

Для экранированных помещений, необходимым и достаточным условием правильной работоспособности ИБС (для мультистандартных мобильных устройств) является отсутствие сигналов стандартов UMTS. Проверка выполнения данного условия осуществляется с помощью тестовых мобильных устройств с сим-картами операторов, имеющихся в регионе.

Порядок работы в режиме с автоматическими настройками ИБС:

- 1) По результатам сканирования диапазонов E-GSM-900, DCS-1800, выбрать оператора и канал, доступный для подключения;
- 2) Нажать кнопку «Авто». Появится новое окно с интерфейсом управления имитатором базовой станции (ИБС);
- 3) После включения ИБС, устройства, работающие в стандарте GSM выбранного оператора, переходят под управление комплексом. Рекомендуется выполнять имитацию сигналов в течении 5-10 минут.
- 4) Повторить п. 1-3 для остальных операторов сотовой связи.

Порядок работы в режиме перевода закладных устройств в роуминг:

Данный режим используется в том случае, если в регионе имеется оператор(-ы), не работающий(-ие) в диапазоне частот GSM/DCS, или в зоне действия работы ИБС отсутствуют базовые станции стандартов GSM/DCS оператора(-ов).

- 1) Нажать кнопку «Режим роуминга». Появится новое окно с интерфейсом управления имитатором базовой станции (ИБС);

2) После включения ИБС, устройства, работающие в стандарте GSM, переходят под управление комплексом.

Порядок работы в ручном режиме:

- 1) Нажать кнопку «Ручной». Появится новое окно с интерфейсом управления имитатором базовой станции (ИБС);
- 2) Выставить настройки ИБС вручную. Параметрами для настройки ИБС являются: номер канала, стандарт, MNC, MCC, LAC, CID;
- 3) Запустить ИБС.

Работа с помощью подавителя сигналов:

Для правильной работоспособности ИБС с помощью подавителя необходима возможность подавления стандартов E-GSM-900, DCS-1800, UMTS. Перед работой необходимо определить зону подавления с помощью тестовых мобильных устройств с сим-картами операторов, имеющих в регионе.

Имитатор базовой станции «Мираж» имеет возможность автоматического управления подавителем «Мозаика-НВ» с возможностью автоматизированного включения/выключения диапазонов подавления без участия оператора. Ниже описан порядок работы ИБС, совместно с данным подавителем.

Порядок работы в режиме с автоматическими настройками ИБС:

- 1) По результатам сканирования диапазонов E-GSM-900, DCS-1800, выбрать оператора и канал, доступный для подключения;
- 2) Нажать кнопку «Авто». Появится новое окно с интерфейсом управления имитатором базовой станции (ИБС). При этом рекомендуется подавление стандартов UMTS и кратковременное подавление диапазонов GSM (для устройств с длительным периодом перерегистрации в сети).
- 3) После включения ИБС, устройства, работающие в стандарте GSM выбранного оператора, переходят под управление комплексом. Рекомендуется выполнять имитацию сигналов в течении 5-10 минут.

Порядок работы в режиме перевода закладных устройств в роуминг:

Данный режим используется в том случае, если в регионе имеется оператор(-ы), не работающий(-ие) в диапазоне частот GSM/DCS, или в зоне действия работы ИБС отсутствуют базовые станции стандартов GSM/DCS оператора(-ов).

- 1) Нажать кнопку «Режим роуминга». Появится новое окно с интерфейсом управления имитатором базовой станции (ИБС). При этом необходимо выполнять подавление стандартов связи;
- 2) После включения ИБС, устройства, работающие в стандарте GSM, переходят под управление комплексом.

Порядок работы в ручном режиме:

- 1) Нажать кнопку «Ручной». Появится новое окно с интерфейсом управления имитатором базовой станции (ИБС);
- 2) Выставить настройки ИБС вручную. Параметрами для настройки ИБС являются: номер канала, стандарт, MNC, MCC, LAC, CID;
- 3) Выставить диапазоны,
- 3) Запустить ИБС.

Рекомендуется, использовать тестовые мультистандарт мобилки для проверки результатов работы ИБС

Обнаруженные устройства отображаются в таблице. Информация об устройствах содержит:

- международный идентификатор мобильного абонента (IMSI);
- международный идентификатор мобильного оборудования (IMEI);
- производитель;
- модель.

Результат работы ИБС представлен на рисунке 5

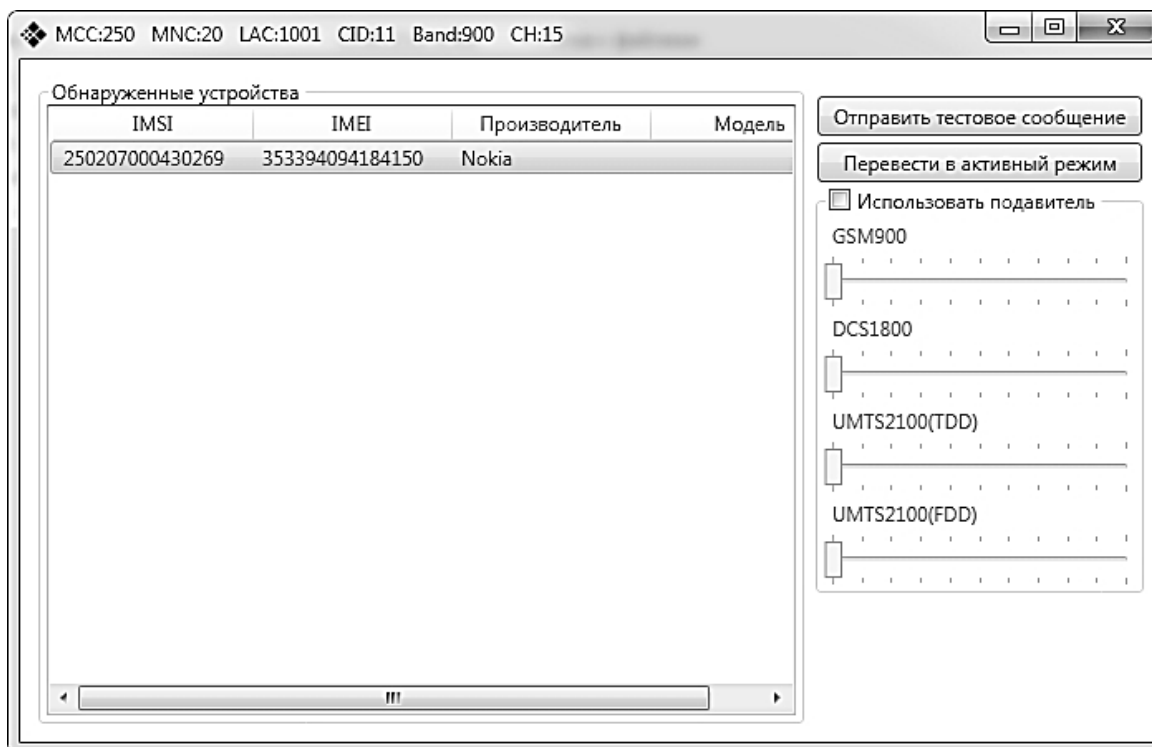


Рисунок 5 – Результат работы ИБС

- 4) С устройствами, переведенными под управление ИБС можно совершать следующие действия:

- отправка тестового сообщения;
- перевод в активный режим работы (необходим для последующей локализации закладных устройств, с помощью индикатора поля).

Примечание. Для проверки эффективности работы ИБС, необходимо использование проверочного устройства, с сим-картой выбранного оператора.

5) Повторить п. 1-5 для остальных операторов сотовой связи.

ПРИЛОЖЕНИЕ 1

СПИСОК КОДОВ ОПЕРАТОРОВ СОТОВОЙ СВЯЗИ РОССИИ

PLMN	MCC	MNC	Наименование оператора
25001	250	1	MTS (Mobile Telesystems)
25002	250	2	Megafon
25003	250	3	NCC (Nizhegorodskaya Cellular Communications)
25004	250	4	Sibchallenge
25005	250	5	Yenisey Telecom (Mobile Comms System)
25006	250	6	Moscow Cellular Comm (Skylink)
25007	250	7	ZAO SMARTS (BM Telecom)
25008	250	8	Personnal Communicational
25009	250	9	Siberian Cellular Systems
25010	250	10	DTC/Don Telecom
25011	250	11	Orensol
25012	250	12	Baykal Westcom
25013	250	13	Kuban GSM
25014	250	14	Megafon
25015	250	15	ZAO SMARTS
25016	250	16	NTC (New Telephone Company)
25017	250	17	JSC/UralTel/U-Tel/Ermak RMS
25019	250	19	Tele2 (INDIGO / OJSC Altaysvyaz / Volgograd Mobile)
25020	250	20	JSC Rostov Cellular Communications
25020	250	20	LLC Personal Communication Systems in the Region
25020	250	20	Tele2/ECC/Volgogr.
25022	250	22	Megafon (JT)
25023	250	23	Mobicon-Nosibirsk
25028	250	28	Bee Line GSM / Extel
25035	250	35	Motiv LLC Ekaterinburg-2000
25038	250	38	Tambov GSM
25039	250	39	UralTel/U-Tel/Ermak RMS
25044	250	44	StavTelesot / Stuvtelesot
25050	250	50	MTS / Bezlimitno.ru
25092	250	92	Printefone
25093	250	93	Telecom XXI
25098	250	98	Baykal Westcom
25099	250	99	Beeline / OJSC Vimpel-Communications (VimpelCom)