



## **GSM Interceptor**

### **Fast and reliable interception of GSM traffic**

- Maximum accuracy, sensitivity and flexibility
- Total indefectibility
- Support for all frequency bands
- User-friendly operation
- Wide range of antennas for stationary and mobile use

## Content

System Features	3
1. System overview and screen shoots	4
1.1. Main Screen	4
1.2. Receivers window	5
1.3. Target List	7
1.4. Base Stations List	8
1.5. Tape Recorder window	8
1.6. Protocol window	9
2. Operational Modes	10
2.1. Main Operational Modes	10
2.1.1. Random mode	10
2.1.2. Classmark mode	10
2.1.3. IMSI/TMSI mode	11
2.2. Additional Operational Modes	11
2.2.1. Distance mode	11
2.2.2. Reverse Mode	11
2.2.3. Phone Number mode	11
2.2.4. IMEI mode	12
3. Effective radius	12
4. Decryption	13
5. How to choose the right configuration?	13
5.1 Ability not to miss calls	13
5.2 Ability not to miss a more important call than the one currently intercepted	14
5.3 Number of simultaneously intercepted calls	14

## Illustrations

1. Fig.1 Main Screen	4
2. Fig.2 Receivers window	5
3. Fig.3 Receivers setup screen	6
4. Fig.4 Target List	7
5. Fig.5 Target List Edit window	7
6. Fig.6 Base Stations List	8
7. Fig.7 Tape Recorder Window	8
8. Fig.8 Protocol Window	9
9. Fig.9 Toolbar	10
10. Fig.10	13

**System Features:**

Targeting by “Number of Interest”	Yes
Screening GSM communication randomly	Yes
Number of simultaneously monitored duplex channels	From 1 to 8
Voice and data recording on hard disk	Yes
Identities for mobile phone authentication	IMSI, TMSI, IMEI, Mobile System Classmark, Dialed and Dialing phone numbers, Ki
Codec types	LPT-RPE, EFR
Monitoring channels	BCCH, CCCH, SACCH, SDCCH, FACCH, TCH
Outgoing call number determination	Yes
Incoming call number determination	Yes (if caller ID is available)
SMS messages interception	Yes
DTMF tones interception	Yes
Encryption types	A5.1, A5.2



# 1. System overview and screen shoots

GSM INTERCEPTOR is a monitoring system that intercepts traffic in cellular GSM networks.

The Interceptor works with all varieties of GSM networks, with all frequency bands and with any type of encryption. No cooperation from the network operator is needed. The system includes both a hardware device and accompanying software. It is housed in an attaché case.

## 1.1 Main screen

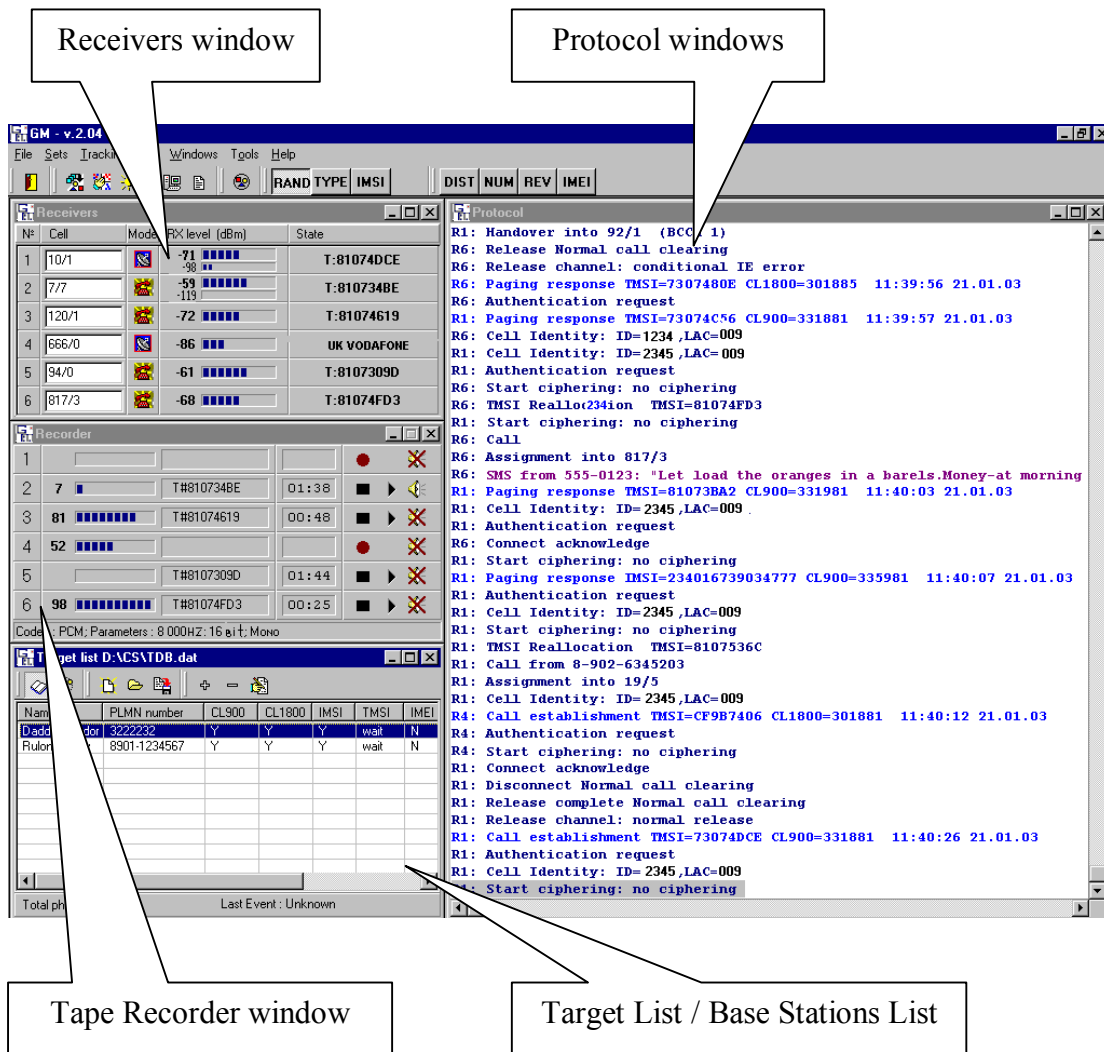









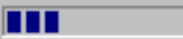






Fig.1 Main Screen

The main operation screen (Fig.1) is divided into 4 main parts:

- receivers window
- tape recorder window
- target list / base stations list
- protocol window


## 1.2 Receivers window

N°	Cell	Mode	RX level (dBm)	State
1	10/1		-71  -98 	T:81074DCE
2	7/7		-59  -119 	T:810734BE
3	120/1		-72 	T:81074619
4	666/0		-86 	UK VODAFONE
5	94/0		-61 	T:8107309D
6	817/3		-68 	T:81074FD3

1 2 3 4 5


Fig.2 Receivers window

1. Receiver number.
2. Channel/Timeslot number
3. Receiver status.

 Traffic channel

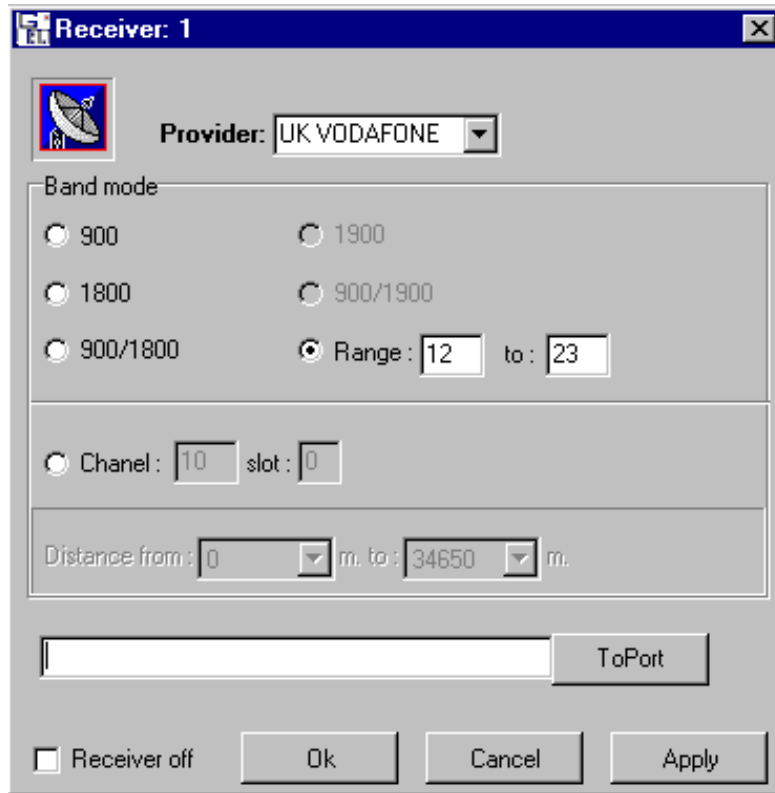
 Control channel

4. Signal level indicator of forward and reverse channels

 - Forward channel  
 - Reverse channel

5. Identity of intercepted call or name of the network operator

A double click on the receiver number will open the Receivers setup screen.



setup screen

Fig.3 Receivers

### 1.3 Target List

Name	PLMN number	CL900	CL1800	IMSI	TMSI	IMEI	Ki	Kc	Last Event
Ted Noi	8901-12345...	Y	Y	Y	wait	N	Y	N	Unknown
Big Boy	3222232	Y	Y	Y	wait	N	N	Y	Paging resp...

Total phones : 2                      Last Event : Unknown

Fig.4 Target List

**Number**

Name: Ted Noi

Number: 8901-1234567

CL900: 1f4b77      CL1800: 1f4e77

**Identification**

IMSI: 230088789776564

TMSI: 123A0B78

Time representation: [ : : ]      Time limit: [ : : ]

**Authentication**

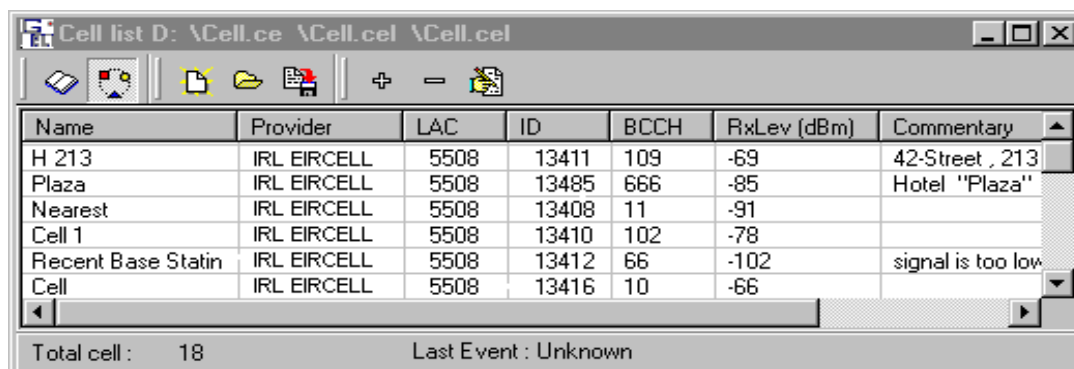
Ki: 123456789ABCDEF0

Kc: [                      ]      Kc\_n: [                      ]

Ok      Cancel

Fig.5 Target List Edit window

## 1.4 Base Stations List



The screenshot shows a window titled 'Cell list D: \Cell.ce \Cell.cel \Cell.cel'. It contains a table with the following data:

Name	Provider	LAC	ID	BCCH	RxLev (dBm)	Commentary
H 213	IRL EIRCELL	5508	13411	109	-69	42-Street , 213
Plaza	IRL EIRCELL	5508	13485	666	-85	Hotel "Plaza"
Nearest	IRL EIRCELL	5508	13408	11	-91	
Cell 1	IRL EIRCELL	5508	13410	102	-78	
Recent Base Statin	IRL EIRCELL	5508	13412	66	-102	signal is too low
Cell	IRL EIRCELL	5508	13416	10	-66	

Below the table, it shows 'Total cell : 18' and 'Last Event : Unknown'.

Fig.6 Base Stations List

## 1.5 Tape Recorder window

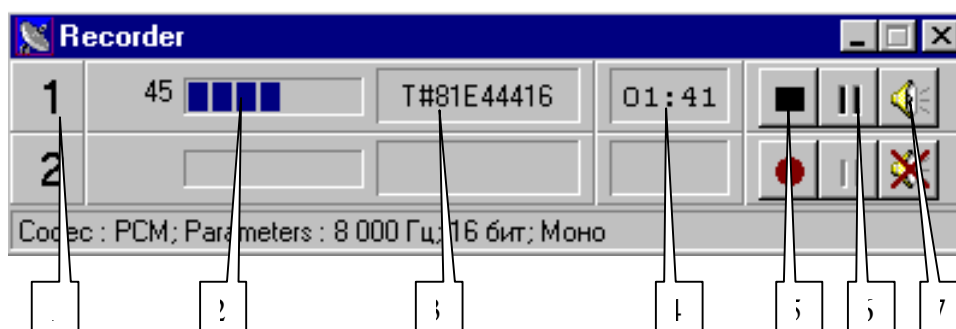


Fig.7 Tape Recorder Window

1. Receiver number
2. Voice Record Level Indicator
3. TMSI or IMSI number
4. Duration
5. Reset Call button
6. Pause button
7. Speaker ON/OFF button

## 1.6 Protocol Window

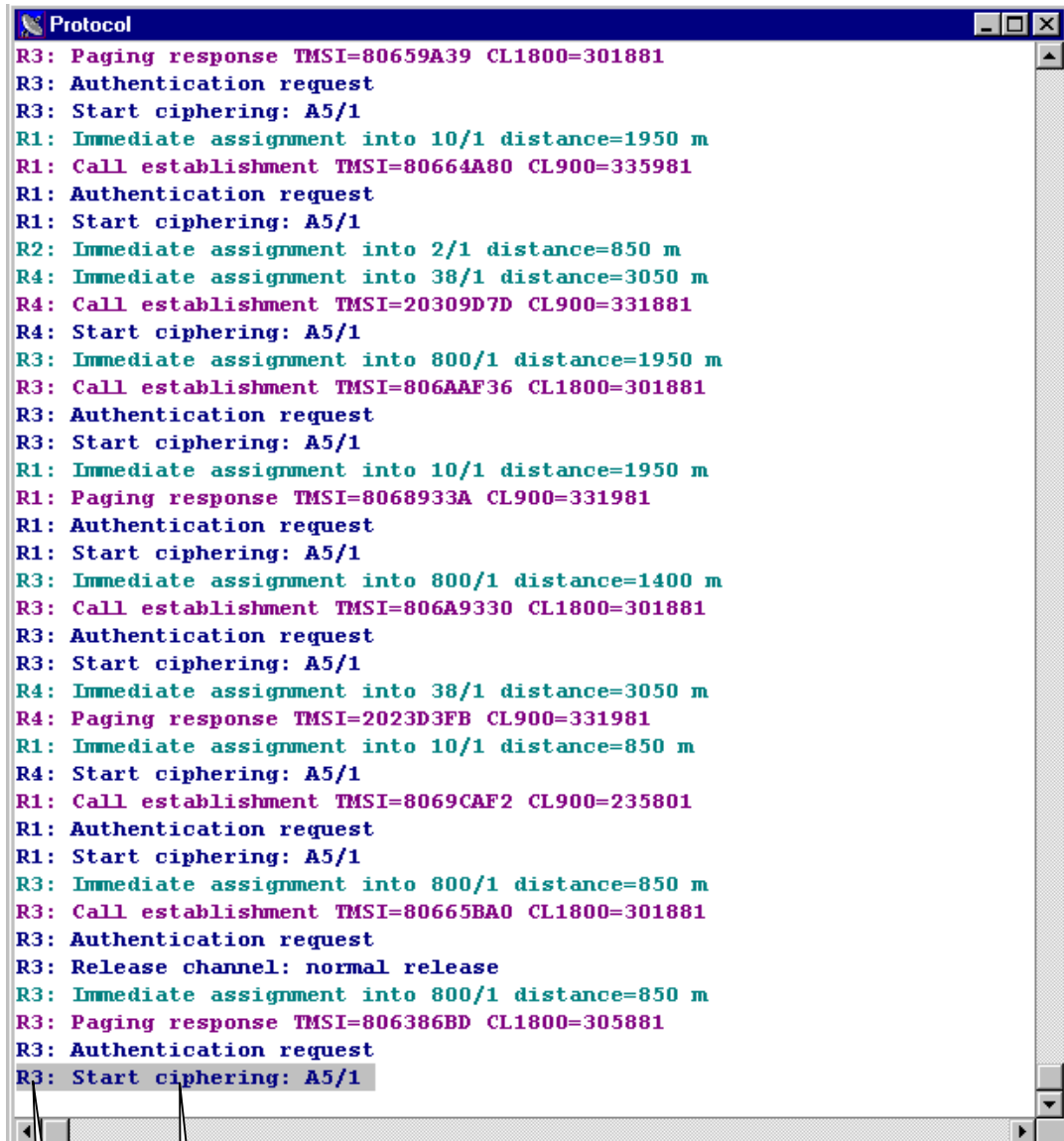


Fig.8 Protocol Window

1. Receiver number
2. GSM network events

## 2. Operational modes

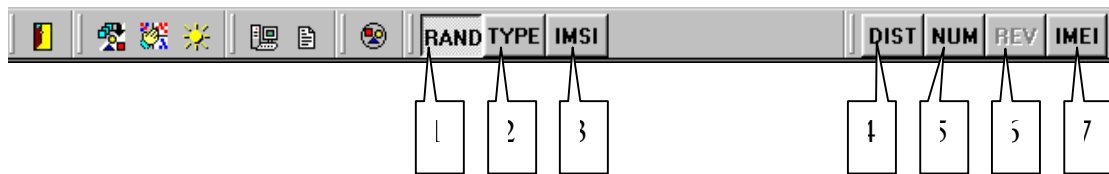


Fig.9 Toolbar

The system has 3 main operational modes:

1. Random Mode
2. Classmark mode
3. IMSI/TMSI mode

Only one of these main modes can be chosen and used at any given time.

In addition, the system has 4 more operational modes:

4. Distance mode
5. Phone number mode
6. Reverse channel mode
7. IMEI mode

The additional operational modes are used together with main modes. The additional modes can be used together in any combination.

### 2.1 Main Operational Modes

#### 2.1.1 Random Mode

This mode is usually used to intercept all calls to or from a given area if the particular phone number is unknown.

#### 2.1.2 Classmark Mode

All mobile phones are distinguished by their classmarks. The classmark is one of the characteristics of mobile phones which is never changed. As soon as some phone conversation is intercepted, the classmark of the active phone is displayed in the protocol window and can be put on the target list. Subsequently, this parameter can be used for monitoring calls made from or to the specific mobile phone.

### **2.1.3 IMSI/TMSI Mode**

The real mobile phone number is never transmitted over the air in GSM networks. Instead of phone numbers, GSM networks use special identities (IMSI or TMSI) for mobile phone authentication.

Using a special technique, the system discovers the identity that corresponds to the particular phone number. These identities are stored in the target list and used for monitoring by specific phone number (see Fig.5).

One of these identities (TMSI) is changed from time to time. The system automatically follows all TMSI modifications and automatically updates them in the Target List without intervention of the system operator.

## **2.2 Additional Operational Modes**

### **2.2.1 Distance mode**

This mode allows interception of those conversations, and only those conversations, being made to or from mobile phones located at a given distance from Base Stations. The distance can be specified in the Receiver Setup Screen (see Fig.3).

This mode may be used effectively when there is some “Place of Interest” and there are no particular phone numbers or other information about mobile phones for that place.

### **2.2.2 Reverse Mode**

When reverse mode is active, only conversations with active reverse channel (i.e. from mobile phones located near the Interceptor) will be intercepted.

This mode can be very useful for interception of calls being made to or from a specific area when the Interceptor is in the area.

Another very effective implementation is a combination of (main) Random Mode and (additional) Distance and Reverse Modes together with a unidirectional antenna. In this case a “Place of Interest” can be defined very closely, in terms of distance from one side and by azimuth from other side.

### **2.2.3 Phone Number Mode**

When this mode is active, the only calls intercepted will be calls made from or to a phone number defined in the Target List (see Fig.5 Target List Edit window).

#### 2.2.4 IMEI mode

Some GSM networks use IMEI identity. This parameter can be very useful as it's a characteristic of mobile phones which is never changed.

In addition, this identity contains the model of the mobile phone. If IMEI is used by the GSM network, Interceptor will display models of mobile phones in the Protocol Window.

### 3. Effective radius

The Interceptor's effective radius may depend on the direction of transmission. In mobile communication there are two directions:

- The direction outward from a base station to a mobile phone is considered the *forward channel*.

Normally the system can intercept traffic in the forward channel at a distance of 3 to 10 km and even more, because a signal in the forward channel is strong.

- The opposite direction, from a mobile phone to a base station, is considered the *reverse channel*.

Normally the system can intercept traffic in the reverse channel at a distance of only 100 to 600 meters, because a signal in the reverse channel is significantly weaker. The exact effective radius for the reverse channel depends on many factors, including walls and their thickness, relative positioning of the system and mobile phone, terrain, and more.

As long as base station transmitters and mobile phone transmitters differ in power, the effective radius of the Interceptor will differ according to channel. But in order to hear both sides of the conversation, the Interceptor needs to be close enough for the weaker channel — normally 600 meters or less.

However, the Interceptor can also be used as a stationary device with unidirectional antennas. In this way, the effective radius for the reverse channel may be increased to as much as 1000 meters.

## 4. Decryption

The purpose of security in a cellular telecommunications system is to protect conversations and signaling data from interception. The security and authentication mechanisms incorporated in GSM make it the most secure mobile communication standard currently available. Part of the enhanced security of GSM is due to the fact that it is a digital system using a speech coding algorithm, Gaussian Frequency Shift Keying (GFSK) digital modulation, slow frequency hopping, and Time Division Multiple Access (TDMA) time slot architecture. To intercept and reconstruct such a signal requires highly specialized reception, synchronization and decoding equipment.

For traffic in GSM networks, there are three encryption options:

- No encryption
- A5.2 encryption
- A5.1 encryption

## 5. How to choose the right configuration?

Although the obvious answer, and often the best one, is “the more channels, the better,” still various factors such as budget may make this guideline less useful in practice. For choosing a price/performance level, there are three main performance considerations:

1. Ability not to miss calls
2. Ability not to miss a more important call than the one currently being intercepted
3. Ability to simultaneously intercept numerous calls

Let's analyze each of those.

### 5.1 Ability not to miss calls

At the beginning of interception, all existing receivers dedicated to forward channels must be tuned to the nearest-to-target-phone base stations. Depending on its environment, a mobile phone can communicate with a GSM network via one of several preferred base stations located nearby.

In a rural environment or in a small town, there may be 1–2 preferred base stations. In such a case, a GSM Interceptor with 2 forward receiver channels may be enough. But in a big city, where base stations are close to one another, a mobile phone makes its choice among 2–3 or sometimes even more base stations. Then an Interceptor with at least 3 forward receiver channels will be necessary.

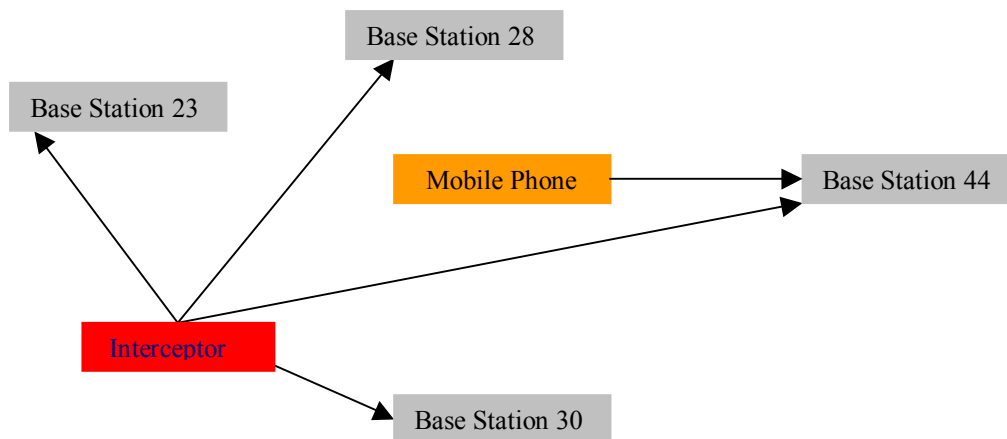


Fig. 10

In Fig. 10 the mobile phone may choose among 4 base stations, so the Interceptor needs at least 4 forward receiver channels. If an Interceptor with 2 forward receiver channels is used in this situation, the chances of missing the call will be around 50%.

### 5.2 Ability not to miss a more important call than the one currently intercepted

This is another important feature of the Interceptor. Suppose some call is intercepted. One of the forward receiver channels is then receiving voice traffic of the one of base stations and, if there are no additional free receivers, cannot monitor other calls of the base station. Therefore one of the preferred base stations is not under surveillance. If at this stage another call occurs that is more important, it can be missed. For that reason, it is very important to have a surplus of forward receiver channels over the number of preferred base stations.

### 5.3 Number of simultaneously intercepted calls

For this model of the Interceptor, the number of reverse channels is usually equal to number of forward channels. One of our standard models has 4 forward and 4 reverse channels. In practice, this means that such an Interceptor can monitor and record four conversations simultaneously (including both sides of each conversation).

**The Interceptors can be produced and supplied in various configurations depending on customer needs and budget.**

**The following system configurations are standard:**

**2+2, 3+3, 4+4, ..., 8+8.**

“8+8” means that the system has 16 receiver channels: 8 forward channels and the other 8 reverse. It means that up to 8 concurrent calls can be intercepted and recorded in the same time. It also means that up to 8 base stations can be covered by the system.

contact - [gsm-interceptor@mail.ru](mailto:gsm-interceptor@mail.ru)