

SPYTEC 3000

The system for GSM communication monitoring

The SPYTEC 3000 system is intended for passive (if system encryption is absent or if A5.2 encryption is used) or semi-active (if A5.1 encryption is used) monitoring of GSM 900 and DCS-1800 standard communication systems.

The system consists of:

- Receivers unit for 8 – 32 channels;
- Control notebook PC of P4 class (with control and A5.2 deciphering software installed);
- Omni-directional antenna system for 900/1800 MHz bands;
- Directed antenna system for 900/1800 MHz bands;
- Carrying case;
- Connection cables set and power cables for power supply from car battery (9–18 V) and from industrial network 220 V;
- User documentation;
- Installation software (HDD image on DVD – for fast system recovery).

Also the delivery pack includes the Operator Workstation software (OW).

OW provides the procession of following types of information:

- Voice records;
- SMS-messages;
- Fax images;
- Fax text;
- Data transmissions.

OW provides:

- Graphic user interface;
- Analysis of records of communication sessions by viewing or listening them;
- Transcribe features (simultaneous listening and typing) with possibility to choose the temp of listening of voice records;
- Generation of reports about communication sessions content after review or listening;
- Forming of the requests to the database and data search;

The system can operate either in stationary or mobile variants.

The quantity of channels received and recorded by the system could be from 8 to 32 for one control computer. The requirements to the control computer are: not worse than Pentium4 2 GHz, RAM 2 Gb, DVD (for operation of A5.2 deciphering software). The system software works in Windows 2000/XP OS environment.

An extensive set of selection parameters enables the interception of certain subscriber with high probability.

Receivers with high dynamical range (80 dB) and special methods of signal procession enable to gain the high quality of reception, high level of computation of session key (Kc), high speech intelligibility, the possibility to control the reverse channel at essential distance from subscriber.

The software enables to use the encryption switch off mode together with software search of encryption key, that provides the high percentage of interception in the networks where encryption is used.

Compactness, light weight and low power consumption of the system (power consumption of 16-channel unit is not more than 15 W without control PC and additional power amplifier) enable carrying the system in small case and long operation using car battery without additional power sources.

The presence of transmitter between the components of the system enables its usage for switching of the encryption (if A5.1 encryption is used), and implementation of such modes as forced cancellation of communication session, definition of subscriber's phone number during the call, substitution of number dialed by the subscriber.

The module structure of the system provides fast repair and the possibility to increase channels quantity easily.

The SPYTEC 3000 system provides the following features:

- Control of forward and reverse voice channels and SMS messages.
- Fast channels scanning in GSM900/1800 MHz band and definition of control channels numbers and appropriate cellular providers.
- Automatic computation of session key (Kc) in real time for A5.2 algorithm, without any disclosing traces for subscriber.
- The possibility to switch off the encryption including both A5.1 and A5.2, if the controlled network supports the operation of the phones without encryption.
- Recording to HDD of voice sessions, SMS messages and call related information.
- Subscriber's location finding relatively to the base station (LAC, BS, sector, distance with accuracy of 550 m) with possibility of its indication on the digital map (optionally).
- Definition of MSISDN – TMSI correlation for the controlled subscriber.
- The possibility of finding of MSISDN number of the controlled subscribed during the call (optionally).
- The possibility to substitute the number, dialled by subscriber without any disclosing traces for subscriber (optionally).
- Proper operation of the system in networks, using Frequency Hopping mode (in contrast to other monitoring systems).
- Tracing of subscriber's movement to another base station coverage area ("handover") if the signal from that base station is strong enough on the receiver input.

The extended set of selection criteria:

- Control of all communications;
- By TMSI (IMSI – if transmitted in the air);
- By phone type (classmark);
- By presence of reverse channel, for control of subscribers within the nearby area (100-1500 m from the system);
- By IMEI (if transmitted in the air) at interception of reverse channel;
- By interlocutor's phone number;
- Selection of communications by distance from the base station;
- Selection of SMS messages only;
- By Ki or Kc of the subscriber (at that the operation in networks, using A5.1 encryption is provided without any disclosing traces);
- Combination of several selection criteria above.

The System Main Application Window

The screenshot shows a software interface for monitoring mobile network activity. It features several panes and a menu bar. Callouts identify key components:

- SelectionWindow:** Located at the top right, it contains a menu with options like RAND TYPE, IMSI, DIST, NUM, REV, IMEI, and SMS.
- Channel control window:** A table below the menu showing details for four channels (1-4), including Cell ID, Rx level, State, IMSI/TMSI, IMEI, CNR/DNR, MSISDN, and Rec qty.
- The list of viewable BS:** A table listing Base Stations (BS) with columns for Name, Provider, LAC, ID, BCCH, RxLev (dBm), and Commentary.
- SMS messages window:** A pane on the right displaying a list of received SMS messages with their timestamps and content.
- Protocol window:** A pane at the bottom showing a detailed protocol log with hex and ASCII data, including error messages and TMSI reallocation events.

Subscriber search and MS-ISDN → TMSI (IMSI) correlation definition window

The screenshot shows a software application window titled "MSISDN" with the following components:

- Search parameters:**
 - MSISDN: 801 3215 5
 - Operator: MC
 - Call count: 5
 - Ack count: 2
 - Duration, ms: 4500
 - Delay, ms: 5000
- Search in:**
 - Tuned channels
 - Visible channels
 - Call
 - Save log
- Search results:**

CNT	IMSI	TMSI	CLM	LAC	CELL	CH
- Buttons:** Start, Stop, Close

Background windows include:

- Receivers:** A list with columns for Cell and R4.
- Target list Config:** A table with columns for Name and PLMN number.
- Event Log:** A list of system events with timestamps and details.

The main technical features of «SPYTEC 3000» system in comparison with other monitoring systems.

№	Parameter	Technical features		
1.	System Name	«GA 900/901»	«Jasmin» / «G-Track»	«SPYTEC 3000»
2.	Interception Method	Active (Base station emulation, the communication goes: subscriber – system – base station)	Passive (the system controls the data exchange between MS and BS if encryption is not used or A5.2 encryption is used)	Passive (the system controls the data exchange between MS and BS if encryption is not used or A5.2 encryption is used) Semi-active (the system controls the data exchange between MS and BS. In strictly defined moments of time it replaces the operation of MS to switch off the encryption mode)
3.	The types of controlled communication systems	GSM 900/1800	GSM-900/1800	GSM900/1800
4.	The information selection criteria for GSM:	- IMSI, IMEI, - The presence of subscriber in certain zone in present time - The phone number of called party	- IMSI (TMSI), - IMEI (by reverse channel) - Ki Definition of MSISDN to IMSI or TMSI correlation	- IMSI (TMSI), - IMEI, - MS Classmark, - distance to BS, - counter party MSISDN - by reverse channel presence, - Ki, - Ks Definition of MSISDN to IMSI or TMSI correlation

5.	The quantity of controlled channels	1 duplex	6 channels for control of service information with possibility of upgrade up to 16 channels, the quantity of channels available for listening is 1(2) duplex.	8 or 16 duplex channels depending on configuration with possibility of expansion. The quantity of channels available for listening is equal to quantity of duplex channels.
6.	Type or information registered	Service information, registered communication session, SMS		
7.	Subscriber's location definition	With accuracy to 550 m or in zone, defined by transmitter power level with possibility to output the information about frequency and time-slot to special direction finder	With accuracy to cell and distance to BS. Additionally: - signal level from MS	With accuracy to cell and distance to BS. Additionally: - signal level from MS, - level of signal, received by MS from neighbour BS.
8.	The possibility of deciphering	The system switches off the encryption in zone of its operation	Provides decryption by A5/2 algorithm in 1-3 sec.	In passive mode provides decryption by A5/2 algorithm in 30 msec. In semi-active mode switches off the A5/1 or A5/2 encryption by short-term transmissions in zone of controlled base stations, if network supports the operation of MS without encryption.
9.	The possibility of operation in mobile variant	Yes, in standing or moving vehicle	Yes, in standing vehicle	Yes, in standing or moving vehicle

10.	The disclosing factors of system's operation	<p style="text-align: center;">Yes</p> <p>1. on some models of mobile phones subscriber can see that encryption is switched off 2. the call receiving party can not see the number of calling party, 3. the bills for communications become smaller, 4. it is impossible to control the incoming calls, only outgoing calls and SMS can be controlled</p>	<p style="text-align: center;">No</p>	<p>In passive mode - no</p> <p>In semi-active mode - yes : - on some models of mobile phones subscriber can see that encryption is switched off</p>
11.	The possibility to block subscriber's communications	<p style="text-align: center;">Yes</p>	<p style="text-align: center;">No</p>	<p style="text-align: center;">Yes</p>

12.	Main disadvantages	<ol style="list-style-type: none"> 1. The necessity of SIM card presence, which will be charged for all calls of controlled subscriber. 2. Impossibility to control the incoming calls. 3. Difficulty of operation near the base station, because the level of signal from original base station is higher the level of signal from the System. 4. Impossibility to control the subscribers of several providers simultaneously. 5. There is no possibility to increase the quantity of TCH (traffic channels), for simultaneous listening of several subscribers. 6. A lot of disclosing factors. 	<ol style="list-style-type: none"> 1. Interception of subscriber in case if TMSI is used and it is changing at each communication session is possible just in case if subscriber did not left the controlled area. 2. The operation in networks, using frequency Hopping is not supported. 3. The system is tuned for operation in certain country (by cellular network identifiers, transferred in the air). 	<ol style="list-style-type: none"> 1. Interception of subscriber in case if TMSI is used and it is changing at each communication session is possible just in case if subscriber did not left the controlled area. 2. In semi-active monitoring mode on some models of mobile phones subscriber can see that encryption is switched off
13.	Additional features	The possibility of integration with direction-finding equipment of DDF series, manufactured by Rohde&Schwarz is implemented	The possibility of simultaneous combined operation with several mobile communications providers	<p>The possibility of simultaneous combined operation with several mobile communications providers</p> <p>Additional features:</p> <ul style="list-style-type: none"> -replacement of phone number, dialled by subscriber; - definition of subscriber's number during the active call;

14.	Power consumption	Main Unit -230 Wt Control computer 20- 50 Wt	<p>«Jasmin» Main Unit (8 channels) – up to 250 Wt</p> <p>«G-Track» Main Unit – up to 50 Wt Control computer 20- 50 Wt.</p>	Main Unit (16-channel) – 20 Wt. Control computer 20- 50 Wt
-----	-------------------	---	--	---