# ST 500 "PIRANHA"

## MULTIFUNCTIONAL DETECTION DEVICE


## USER MANUAL

**ST Group, Ltd.**
**St. Petersburg, Russia**
**+7 (812) 412-33-21**
**info@smersh.pro**
**www. spymarket.com**

## CONTENTS

# 1. GENERAL INFORMATION

This user manual describes the composition and operation of the multifunctional detection device ST 500 "PIRANHA". The information contained in this manual is cross-referenced with hyperlinks.

## 1.1. PURPOSE AND CAPABILITIES

The multifunctional detection device ST 500 "PIRANHA" is intended for the detection and location of eavesdropping devices.

Functionally, the device consists of four detection channels.

**Channels for the detection of wireless eavesdropping devices:**

- **SELECTIVE HF DETECTOR** is intended for the detection of analog and digital wireless (utilizing GSM, LTE, Bluetooth, or WiFi) eavesdropping devices operating in the frequency range 20 - 6000 MHz.
- **IR DETECTOR** is intended for the detection of IR transmitters (eavesdropping devices using the infrared range for transmissions).

**Channels for the detection of wired eavesdropping devices:**

- **WIRED RECEIVER** is intended for the detection of high-frequency signals from eavesdropping devices that transmit information via electric mains and low current lines in the frequency range 100 kHz – 180 MHz.
- **LOW FREQUENCY AMPLIFIER** is intended for the detection of LF signals from eavesdropping devices.

---

**Each CHANNEL works in certain MODES**
**Each MODE corresponds to a set of search FUNCTIONS**

---

**FUNCTIONALITY OF THE DEVICE:**

1. Detection and location of radio eavesdropping devices:
   - radio microphones, telephone radio repeaters, radio stethoscopes, etc.
   - video cameras with radio transmitters
   - radio beacons of tracking systems.
2. Identification of digital protocols of the detected radio signals: GSM, CDMA, Bluetooth, LTE, WiFi.
3. Identification of signals of base stations and mobile digital communication devices.
4. Detection and location of active wired eavesdropping devices:
   - wired microphones transmitting through permanent and makeshift low current lines
   - detection of signals from eavesdropping devices transmitting over electric mains and low current lines in the frequency range from 0.1 - 180 MHz.
5. Activation of wired electret microphones by applying a bias voltage to the circuit
6. Detection and location of eavesdropping devices that utilize infrared transmissions.

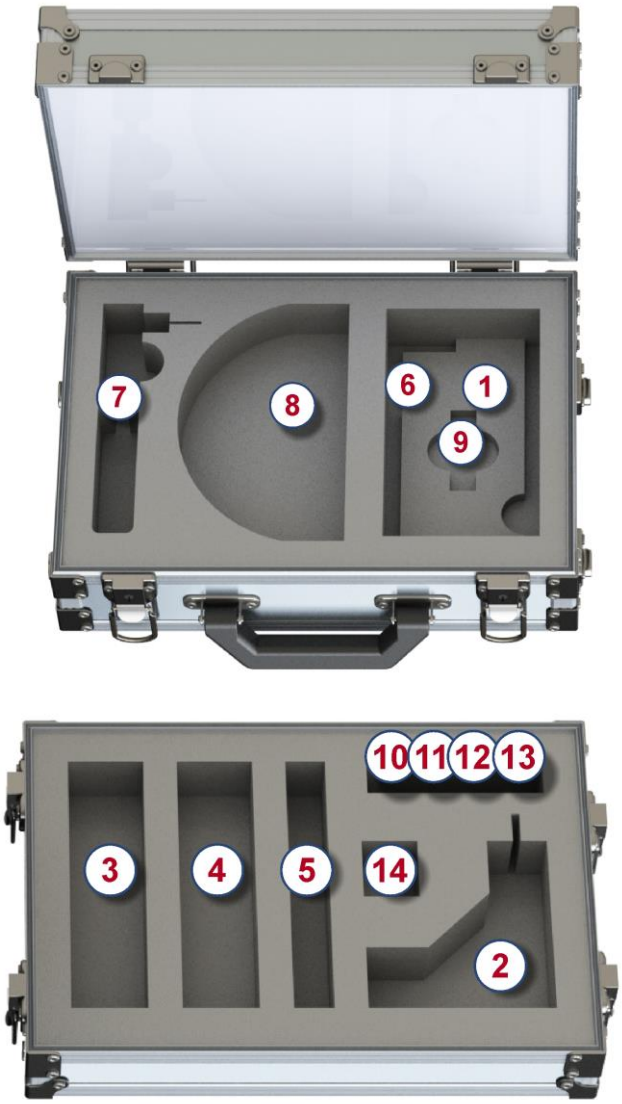
## 1.2. SPECIFICATION

| | | |
|---|---|---|
| 1. | Main Unit | 1 pcs. |
| 2. | Adapter for connecting the main unit to electric mains | 1 pcs. |
| 3. | Cable for connecting the main unit to telephone line sockets | 1 pcs. |
| 4. | Cable for connecting the main unit to low current sockets | 1 pcs. |
| 5. | Cable for connecting the main unit to a PC's USB | 1 pcs. |
| 6. | Telescopic antenna | 1 pcs. |
| 7. | Charger | 1 pcs. |
| 8. | Headphones | 1 pcs. |
| 9. | USB flash drive | 1 pcs. |
| 10. | Coupler (RJ11) | 1 pcs. |
| 11. | Coupler (RJ45) | 1 pcs. |
| 12. | 1x2 splitter (RJ11) | 1 pcs. |
| 13. | 1x2 splitter (RJ45) | 1 pcs. |
| 14. | Adapter for connecting a multicore cable and screwdriver | 1 pcs. |
| 15. | Case | 1 pcs. |

The numbers above correspond to those in fig.1.


**Fig.1**

For transportation and storage of the device, the shock- and moisture-proof plastic case is used. All the items in the bundle are housed in the two panels within the case.




In the placement scheme above, the numbers assigned to items in the ST 500 bundle are the same as in 1.2.1.

## 1.3. DESCRIPTION OF SPECIFICATION ITEMS

### 1.3.1. MAIN UNIT WITH ELECTRONIC SWITCH

**Main unit functions:**

- analysis of the incoming signals,
- control of connection schemes to the tested multiwire lines,
- data display,
- control of operation modes.

**Components of the main unit:**

- signal processing module,
- electronic switch,
- display module,
- power supply module,
- controls.

The appearance of the main unit is shown in fig.2.

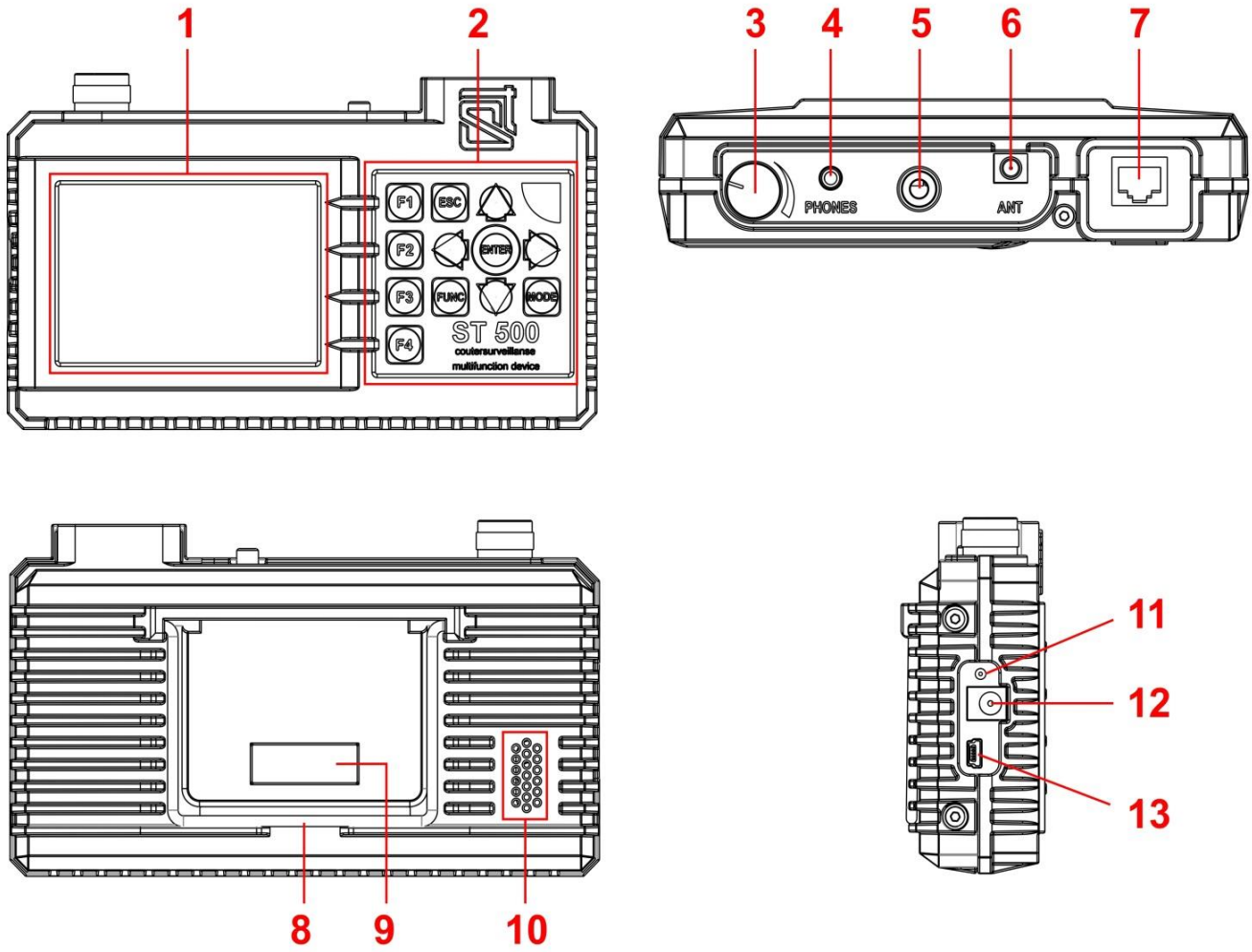



**Fig.2**

| Number in fig.2 | Marking on the device | Element description |
|---|---|---|
| 1 | | Display |
| 2 | | Keyboard |
| | F1-F4 | Hotkeys |
| | ESC | Cancellation (return) key |
| | FUNC | Key to enable additional functions |
| | ENTER | Confirmation key |
| | MODE | Main menu key |
| 3 | | Power switch and volume control |
| 4 | PHONES | Headphone socket |

| Number in fig.2 | Marking on the device | Element description |
|---|---|---|
| 5 | | Sensor of the IR DETECTOR |
| 6 | ANT | Antenna socket of the SELECTIVE HF DETECTOR |
| 7 | INPUT | Electronic switch input |
| 8 | | Prop |
| 9 | | Info shield with serial number |
| 10 | | Inbuilt speaker |
| 11 | | Charger connected indicator |
| 12 | | Charger socket |
| 13 | | Mini-USB for PC connection |

### 1.3.2. ELECTRONIC SWITCH

The device is equipped with an inbuilt electronic switch for a more efficient testing of multiwire cables.

The automated and manual control of the electronic switch allow engaging all possible paired combinations of cores in a multicore cable connected to the electronic switch (via RJ45 socket, fig.2, 7). While testing electric mains, control of the electronic switch is disabled.

### 1.3.3. ADAPTER FOR CONNECTING TO ELECTRIC MAINS

The adapter is intended for connecting the main unit to electric mains equipped with European standard sockets (fig.1, 2). A LED indicator in the plug shows if the line is powered. The adapter cable is equipped with an RJ45 connector, with only the first and second pins are engaged, and the rest are disabled.

### 1.3.4. CABLE FOR CONNECTING TO COMPUTER SOCKETS (RJ45)

The cable is used for connecting the main unit to a computer line equipped with standard RJ45 connectors.

The cable (fig.1, 4) is a standard patch cord.

### 1.3.5. CABLE FOR CONNECTING TO TELEPHONE SOCKETS (RJ11)

The cable is used for testing telephone lines equipped with 6P4C sockets. The cable (fig.1, 3) is equipped with 8P8C (RJ45) and 6P4C connectors. In the RJ45 connector, the four central pins (## 3-6) are engaged, while the four side ones (## 1, 2, 7, 8) have no connections.

### 1.3.6. ADAPTER FOR CONNECTING A MULTICORE CABLE

The adapter (fig.1, 12) is used for connecting to raw-ended (not fitted with connectors) low current cables. While connecting a raw-ended twisted pair cable, it is advised to observe the wiring color scheme (Supplement #3, 12.3.2).

### 1.3.7. MINI-USB CABLE

The cable (fig.1, 5) is used for connecting the main unit to a PC's USB-port.

### 1.3.8. SPLITTERS, ADAPTERS, AND CONNECTOR CABLES

A set of splitters and connecting cables is supplied with ST 500, that are used for testing various types of cabling and circuits. Their use is described in Section 5 of this manual: **CONNECTING ST 500 TO CABLING**

### 1.3.9. USB FLASH DRIVE

The USB flash drive contains pre-recorded test sounds for the test sound source, this Manual, and "ST 500" software.

### 1.3.10. TEST SOUND SOURCE (not included in the package)

A test sound source is required to search for eavesdropping devices. Any portable device equipped with a speaker (smartphone, tablet, voice recorder) can be used.

Purpose of the test sound source:

- creation of an acoustic signal (the correlation of this signal and the information obtained using the ST 500 means that there is an active eavesdropping device with an unencrypted transmission channel in the room);
- forced inclusion of eavesdropping devices equipped with a VOX activation system;
- localization of detected listening devices;
- creation of the "masking noise" during the search operations.

Files with sounds are recorded on a USB drive (fig.1, 9). The user can use their own sound files that are optimally suited to the situation in which the search event is held (noise in the office, people talking, music, etc.).

## 1.4. POWER SUPPLY

The device is only powered from an inbuilt battery whose charge status is shown in the status bar (fig.5, 2). A fully charged battery provides 7 hours of non-stop operation.

The battery is charged with the aid of a charger unit (fig.1, 7) plugged into the socket on the side of the Device (fig.2, 12). The charger is connectable to 220 V/50 Hz mains.

During charging a LED on the side of the Device (fig.2, 11) will be lit red. Full charging time is up to 7 hours. Upon charging, the LED will change its light to green.

**DO NOT ATTEMPT CHARGING THE DEVICE DURING OPERATION!**

## 1.5. TECHNICAL SPECIFICATIONS

| | |
|---|---|
| **Selective HF Detector:** | |
| operative frequency range, MHz | 20-6000 |
| passband, MHz | 1 or 20 |
| impedance, Ohm | 50 |
| rate of scanning, GHz/sec | 18 |
| bandpass flatness, dB | ±6 |
| minimum detection level, dB | -70 |
| dynamic range, dB | 50 |
| **IR Detector:** | |
| spectral range, μm | 0.75…1.1 |
| detection passband, MHz | 5 |
| field-of-view angle, degrees | ±20 |
| minimum detectable power, $W/Hz^{½}$ | $10^{-13}$ |
| **Wired Receiver:** | |
| operative frequency range, MHz | 0.1-180 |
| whole range scanning time, sec | 2 |
| minimum detection level, dBm | -50…-75 |
| dynamic range, dB | 50 |
| impedance, Ohm | 100 |
| demodulation type | AM, FM |
| input filter passband, kHz | 180 |
| maximum voltage on the circuit, V | 250(AC), 60(DC) |
| **Low Frequency Amplifier:** | |
| frequency range, Hz | 20 - 25000 |
| impedance, kOhm | 200 |
| gain, times | 1,2,5,10,20,50,100 |
| max voltage amplitude on the input, V | ±60(DC),<br>±1(AC) |
| noise spectral density, nV/Hz | 3 |
| bias voltage range, V | +30, -30 |
| **Power Supply:** | |
| inbuilt lithium polymer accumulator battery with voltage, V | 3.7 |
| power consumption, W | <1 |
| time of continuous operation at maximum power, hrs | >4 |
| recharging time from a full discharge, hrs | 10 |
| **Weight and Dimensions:** | |
| dimensions of the main unit (length, width, height), mm | 165 x 100 x 40 |
| mass of the main unit, kg | 0.470 |
| case dimensions (length, width, height), mm | 360 x 255 x 195 |
| full package mass (with case), kg | 4,5 |

# 2. INTERFACE OPTIONS

## 2.1. TURNING THE DEVICE ON/OFF

The Device is turned on/off with the power switch and volume control button (fig. 2, 3). When turned on, the display will show a screen (fig.3) with the ST Group Ltd. logo, name of the Device, and firmware version number.


**Fig.3**

Press any key to go to the main menu of device.

## 2.2. MAIN MENU

One of the four operation channels, or the service mode "SETTINGS", can be selected from the main menu. The main menu screen is shown in fig.4.


**Fig.4**

To activate channels "SELECTIVE HF DETECTOR", "IR DETECTOR", "LOW FREQUENCY AMPLIFIER", and "WIRED RECEIVER", with the keys ▽ and △ move the cursor to the corresponding line and press "ENTER", or use the hotkeys ("F1", "F2", "F3", "F4", respectively).

Through the "SETTINGS" menu item, system settings can be accessed.

## 2.3. STATUS BAR

In the upper part of the Device's screen is a status bar shown in fig.5

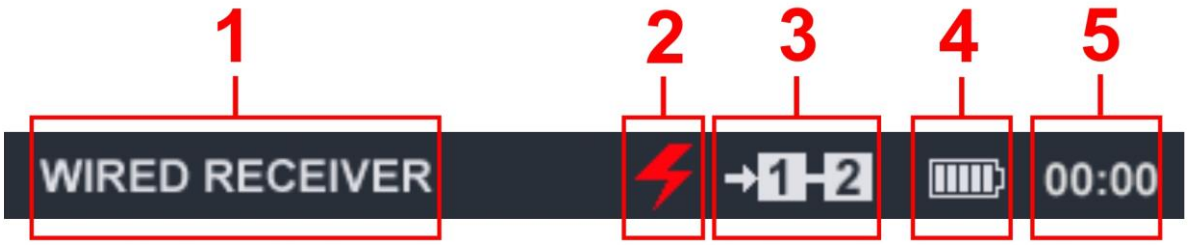



**Fig.5**

**In fig.5:**

1 - active channel
2 - electric mains sign
3 - pair of wires connected
4 - battery charge sign
5 - current time (hh:mm)

## 2.4. "SETTINGS" SERVICE MODE

This SETTINGS mode is intended for setting the date, time and interface language (Russian or English).

To enter the settings mode, using the keys ▽ and △ select "SETTINGS" in the main menu and press "ENTER".

To exit SETTINGS mode to the main menu, press "ESC". Any confirmed changes will be saved upon exiting this mode or deactivating the device. The "SETTINGS" screen is shown in fig.6.

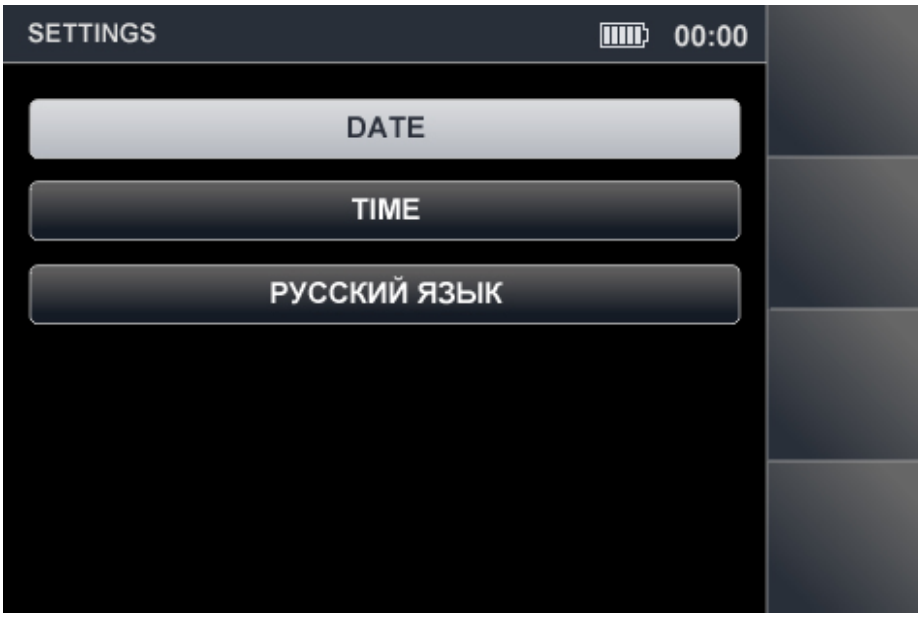



**Fig.6**

### 2.4.1. SETTING THE DATE

In order to set the date, use the keys ▽ and △ to select "DATE" in the menu and press "ENTER". The following screen (fig.7) will appear.


**Fig.7**

The date format is "DD/MM/ YYYY". Use the keys ◁ and ▷ to select "DAY", then use ▽ and △ to set the desired value. Proceed in the same way to set "MONTH" and "YEAR". Use "ENTER" to confirm changes. Use "ESC" to go back to "SETTINGS". To exit the SETTINGS mode without saving changes, press **"**ESC".

### 2.4.2. SETTING THE TIME

In order to set the time, use ▽ or △ to select "TIME" in the "SETTINGS" menu and press "ENTER". The following screen (fig.8) will appear, with time in the format "HH/MM".


**Fig.8**

The time can be set in the same way as the date (3.4.1). Use the "ENTER" to confirm changes. Use "ESC" to go back to "SETTINGS". To exit the SETTINGS mode without saving changes, press **"**ESC".

### 2.4.3. SETTING THE LANGUAGE

In order to set the interface language, using ▽ or △ select "LANGUAGE" in the menu and press "ENTER". The interface language will be changed from Russian to English. To set Russian again, select "РУССКИЙ ЯЗЫК" in the menu and press "ENTER".

## 3. "SELECTIVE HF DETECTOR" CHANNEL

The "SELECTIVE HF DETECTOR" channel is intended for the detection of analog and digital wireless (utilizing GSM, LTE, Bluetooth, or WiFi) eavesdropping devices operating in the frequency range 20 MHz - 6 GHz.

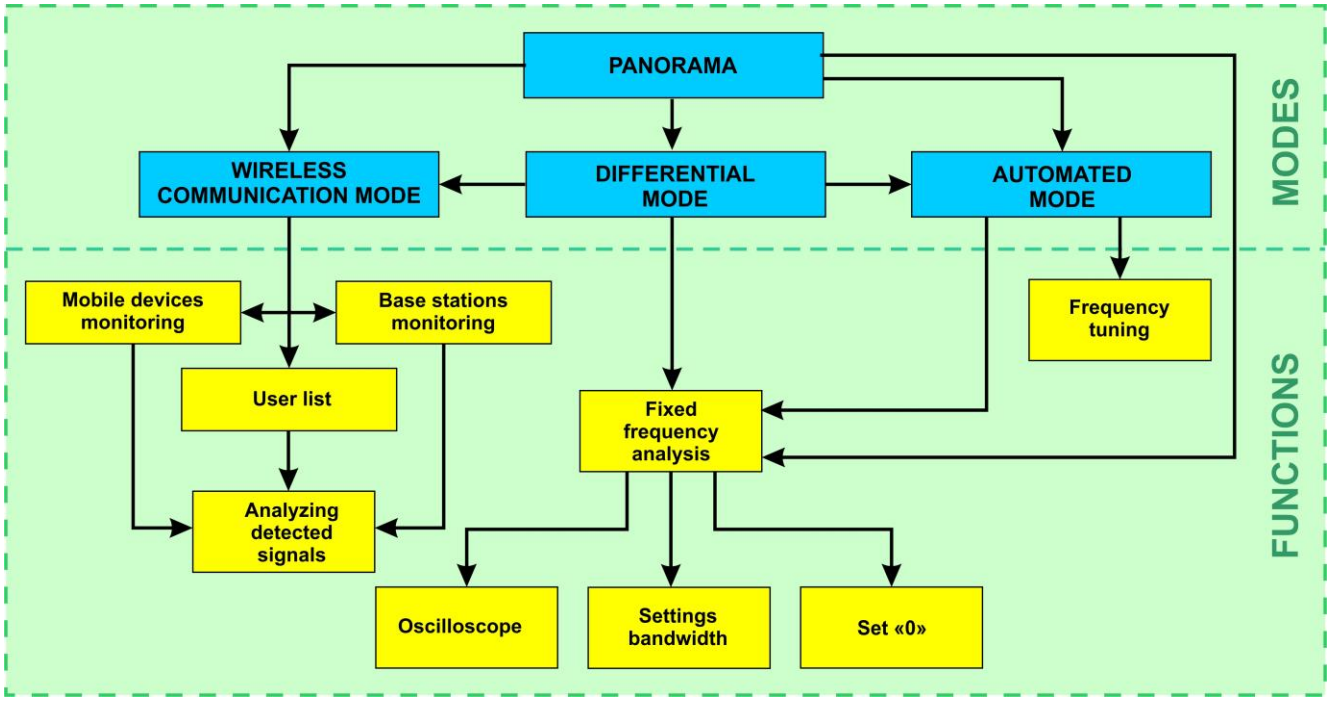
For the reception of radio signals, a telescopic antenna is used (fig.1, 6) that has a spherical radiation pattern. The antenna is connected to a socket on the upper surface of the device (fig.2, 6).

The channel is activated from the main menu.

**The detected signals are analyzed based on:**

- graphic information (spectrogram, oscillogram, table of signals)
- acoustic information (via headphones or inbuilt speaker).

**Functional Scheme of the "SELECTIVE HF DETECTOR" Channel**




### 3.1. "PANORAMA" MODE

The "PANORAMA" mode is started by default when the "SELECTIVE HF DETECTOR" channel is activated. All activity in the frequency band will be shown on the screen (fig. 9).

**Functionality:**

- activating the AUTOMATED mode
- activating the "WIRELESS COMMUNICATION" mode
- activating the DIFFERENTIAL mode
- analyzing the signal at a fixed frequency
- setting the gain
- adjusting the band limits

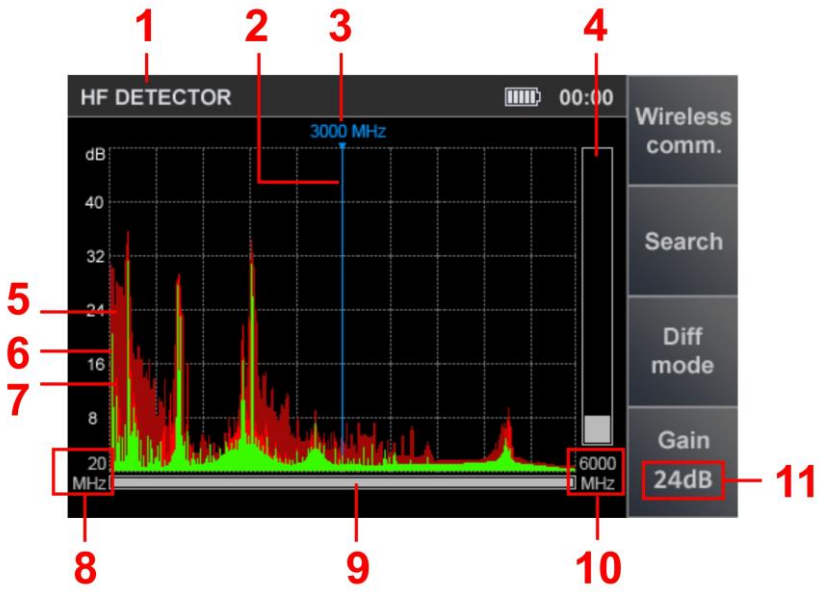



**Fig.9**

**In fig.9:**

1 - active channel
2 - screen cursor
3 - frequency value at the current cursor position
4 - dynamic bar indicating signal level at the selected frequency
5 - peak signal value over all cycles at the selected frequency (maroon)
6 - pulse signals detected in the last measurement cycle (green)
7 - continuous signals detected in the last measurement cycle (red)
8 - lower bound of the set frequency range viewing band
9 - indicator showing the width of the set viewing bar relative to the maximum possible
10 - upper bound of the set frequency range viewing band
11 - gain value

**Controls:**

| Key | Action |
|---|---|
| **ESC, MODE** | switching to main menu of device |
| **ENTER** | turn on "FIXED FREQUENCY ANALYSIS" function |
| ◁ ▷ | screen cursor positioning |
| ▽ △ | panorama scaling relative to frequency on the marker |
| **F1** | activating "WIRELESS COMMUNICATION" mode |
| **F2** | activating AUTOMATED mode |
| **F3** | activating DIFFERENTIAL mode |
| **F4** | gain setting on/off |
| **FUNC** | disabled |

**GAIN SETTING:**

1. Press "F4". The "Gain" field will become lighter.
2. Use the keys ▽ △ ◁ ▷ to set the gain in dB (0, 8, 16, 24, 32, 40). The gain value will be shown in the corresponding screen field (fig.10).
3. Press "F4". The "Gain" field will become darker.

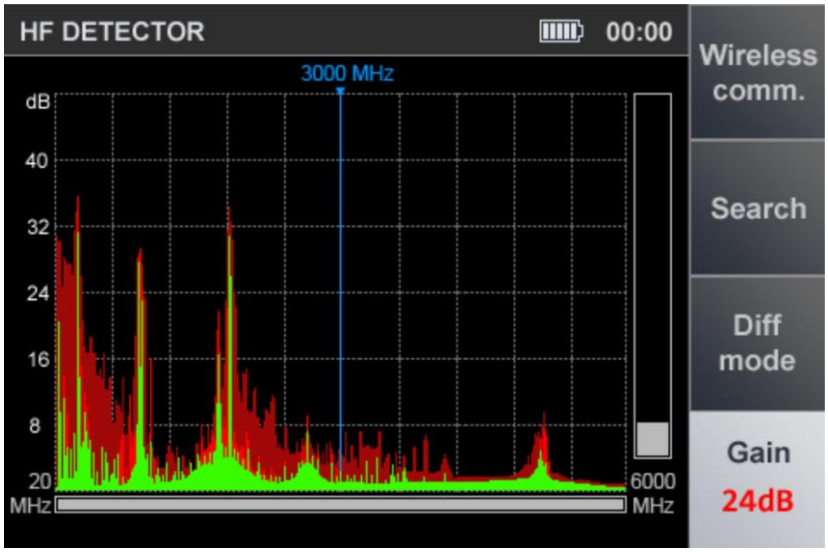



**Fig.10**

**IMPORTANT!** Until the gain setting is completed, other modes and functions are not available, except for switching to the Main Menu of the device (by pressing "MODE").

### 3.2. DIFFERENTIAL MODE

In the DIFFERENTIAL mode, signal levels registered during previous scanning cycles in the "PANORAMA" mode, are set as "0", and only signals in excess of "0" will be shown on the screen (differential spectrum).

The DIFFERENTIAL mode can be used for isolating the signals from sources within the inspected premises, from external signals.

The DIFFERENTIAL mode can be activated from the "PANORAMA" mode (fig.9) by pressing "F3". The "F3" key field will become highlighted.

Upon activating the DIFFERENTIAL mode, the screen will look as shown in fig.11.

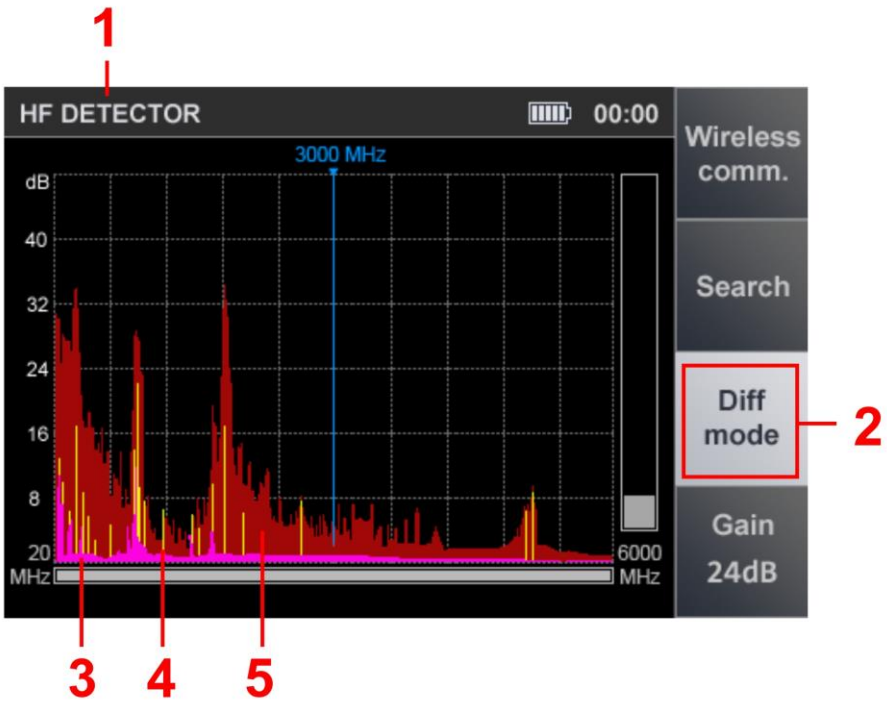



**Fig.11**

**In fig.11:**

1 - active channel
2 - DIFFERENTIAL mode highlighted as currently active
3 - constant differential signal registered during the last scanning cycle (lilac)
4 - pulse differential signal registered during the last scanning cycle (yellow)
5 - peak signal level at the given frequency over all cycles (maroon)

**Functionality:**

- activating the AUTOMATED mode
- activating the "WIRELESS COMMUNICATION" mode
- analyzing the signal at a set frequency
- setting the gain
- adjusting the band limits (zoom)

Switching off the DIFFERENTIAL mode (return to the "PANORAMA" mode) is performed by pressing the "F3". The "F3" key field will become darker. Gain values and span set in DIFFERENTIAL mode are saved.

### 3.2.1. "FIXED FREQUENCY ANALYSIS" FUNCTION

This feature is intended for researching signals detected in the "PANORAMA" or DIFFERENTIAL mode. To activate it from either of said modes, select the signal of interest using ◁ and ▷ and press "ENTER". The screen will look as shown in fig.12 below.

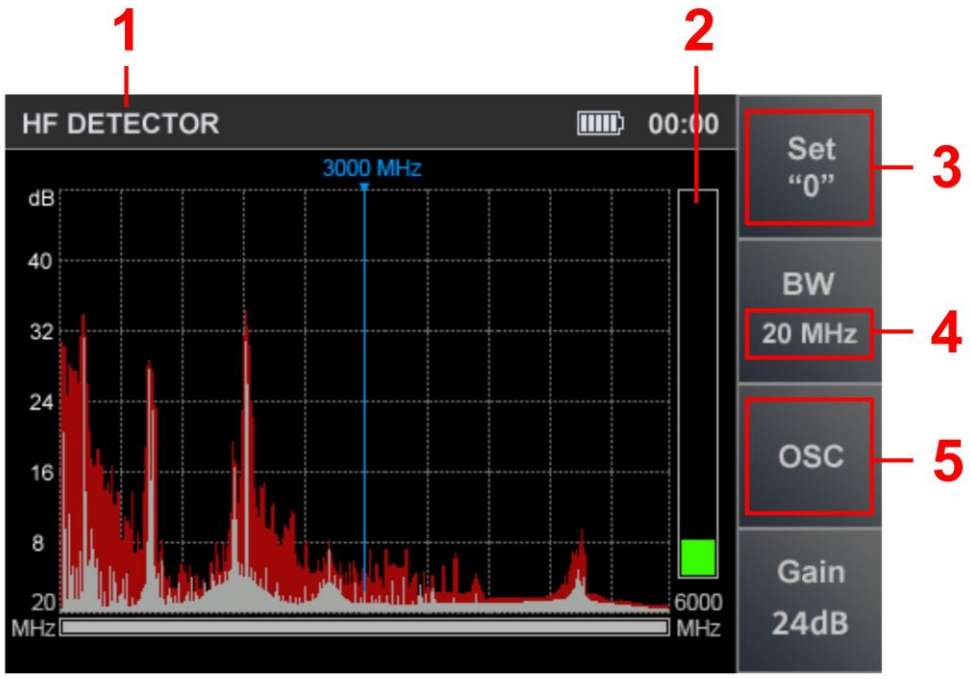



**Fig.12**

**In fig.12:**

1 - active detection channel
2 - signal level at the selected frequency (at cursor position)
3 - "SET "0" active
4 - selected passband (1 MHz or 20 MHz)
5 - OSCILLOSCOPE active

**Functionality:**

- tuning to the frequency of the detected signal
- passband selection (1 MHz or 20 MHz);
- listening to a demodulated signal
- analyzing the signal with oscilloscope
- locating the signal source with power method

**Controls:**

| Key | Action |
|---|---|
| **MODE** | switching to the main menu of device |
| **ENTER, ESC** | turning off "FIXED FREQUENCY ANALYSIS" function |
| ◁ ▷ | screen cursor positioning |
| **F1** | turning on/off "SET "0" function |
| **F2** | passband selection (1 MHz or 20 MHz) |
| **F3** | turning on OSCILLOSCOPE |
| **F4** | turning on/off gain setting |
| **FUNC** ▽ △ | disabled |

To turn off " FIXED FREQUENCY ANALYSIS" function, press "ENTER" or "ESC". The device will switch back to the mode, from which the function was activated ("PANORAMA" or DIFFERENTIAL mode).

### 3.2.2. "SET "0" FUNCTION

This function helps locate the source of a detected signal. It can be especially helpful in finding the sources of powerful signals that make the screen levels go off-scale even at minimum gain. Ways of locating eavesdropping devices are described in more detail in 9.1.4.

When "SET "0" is used, the signal level at current frequency is set as "0", and only the level differences are displayed.

To turn on the "SET "0", press "F1". The "F1" key field will become lighter.

When using the "SET "0" function, it is possible to:

- change the passband ("F2")
- turn on the oscilloscope ("F3")
- change the gain ("F4")

To turn off the "SET "0", press "F1" again. The "F1" field will become darker.

### 3.2.3. OSCILLOSCOPE

To activate the OSCILLOSCOPE, after switching on the "FIXED FREQUENCY ANALYSIS" function, press the "F3". The "OSC" field will become lighter. The screen will look as shown in fig.13 below.

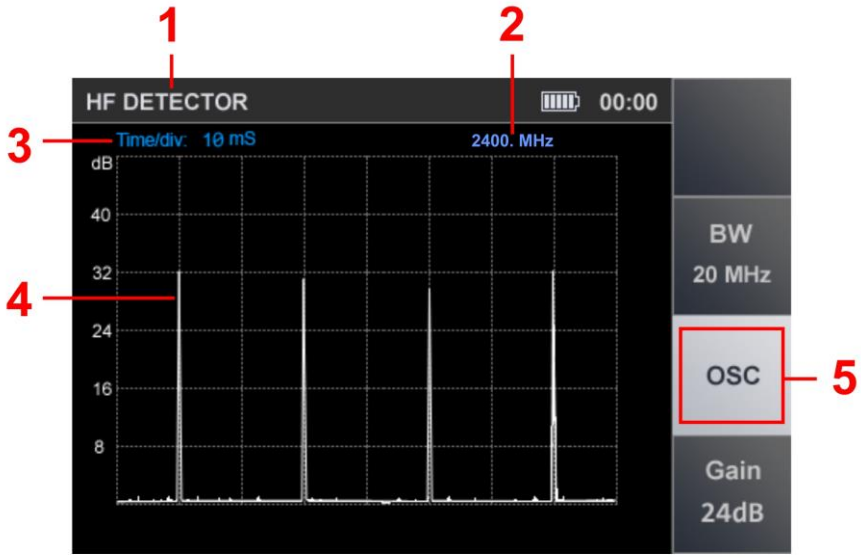



**Fig.13**

**In fig.13:**

1 - active detection channel
2 - selected frequency value
3 - set division value of the time axis
4 - oscillogram of a demodulated signal at the selected frequency
5 - on indication of the inclusion of the OSCILLOSCOPE

**Functionality:**

- determining the time parameters of a demodulated signal
- setting the division value of the time axis
- passband selection
- gain adjustment

**Controls:**

| Key | Action |
|---|---|
| ◁▷ | selecting the division value of the horizontal sweep 100μS/200μS/500μS/1mS/2mS/5mS/10mS |
| **F2** | passband selection (1 MHz or 20 MHz) |
| **F3, ESC** | turning off OSCILLOSCOPE |
| **F4** | activating gain adjustment |
| **MODE** | switching to main menu of device |
| **FUNC ENTER F1** ▽△ | disabled |

To turn off the OSCILLOSCOPE press "F3" or "ESC".

### 3.3. AUTOMATED MODE

The AUTOMATED mode is used to register signals whose amplitudes exceed the adaptive detection threshold. It is activated from the DIFFERENTIAL or "PANORAMA" mode by pressing "F2".

Search for signals is performed within set frequency limits, based on the data obtained in the DIFFERENTIAL mode (if the AUTOMATED mode has been activated from the DIFFERENTIAL mode).

Each detected signal is assigned one of the three categories, "NON-THREAT", "THREAT", or "UNKNOWN". By default, those are:

"NON-THREAT" – signals of base stations of mobile telecommunication networks
"THREAT" – signals of mobile digital communication devices
"UNKNOWN" – all the remaining signals.

With the help of ST 500 ST 500 software (8.6.1), bands can be assigned "THREAT" or "NON-THREAT" status, so that the received signals will be accordingly marked with color, depending on the frequency band they are in. Upon mode activation, the screen will look as shown in fig.14.

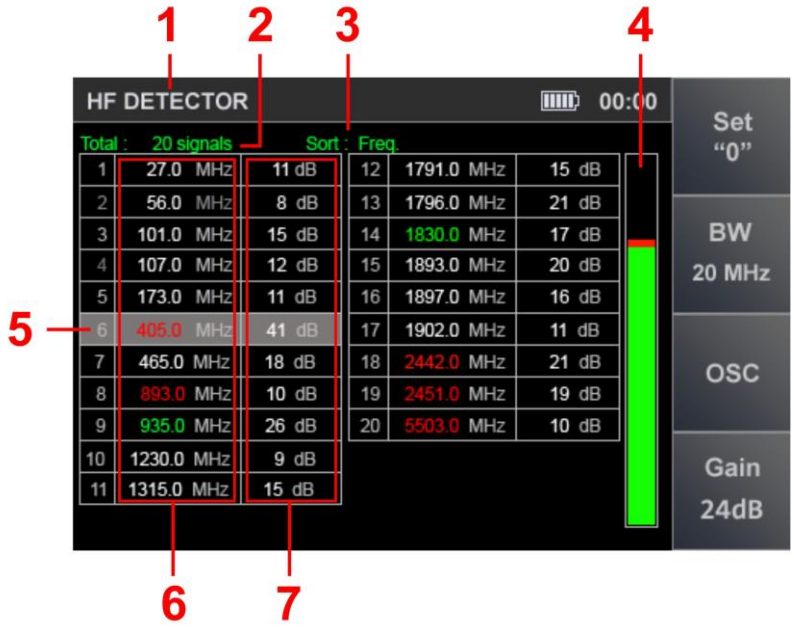



**Fig.14**

**In fig.14:**

1 - active channel
2 - number of the detected signals
3 - data sorting type (by level or frequency)
4 - signal level at the current cursor position
5 - current table row
6 - frequency values of the detected signals
7 - levels of the detected signals

In fig.14 frequency values of the detected signals are marked with different colors:

"THREAT" signals - red
"NON-THREAT" signals - green
"UNKNOWN" signals - white

**Functionality:**

- sorting the detected signals (by frequency or by level)
- quick tuning to the detected signal by selecting it in the table
- fine frequency tuning
- passband selection (1 MHz or 20 MHz)
- activating/turning off "SET "0"
- gain adjustment
- OSCILLOSCOPE activation

**Controls:**

| Key | Action |
|---|---|
| ◁ ▷ ▽ △ | screen cursor positioning |
| **FUNC** | signal sorting |
| **F1** | turning on/off "SET "0" function |
| **F2** | passband selection (1 MHz or 20 MHz) |
| **F3** | turning on OSCILLOSCOPE |
| **F4** | activating gain adjustment |
| **ENTER** | turning on "FREQUENCY TUNING" function |
| **ESC** | returning to "PANORAMA" or DIFFERENTIAL mode |
| **MODE** | switching to main menu of device |

### 3.3.1. "FREQUENCY TUNING" FUNCTION

For fine frequency tuning, select the corresponding table row and press "ENTER". The screen will look as shown in fig.15 below.

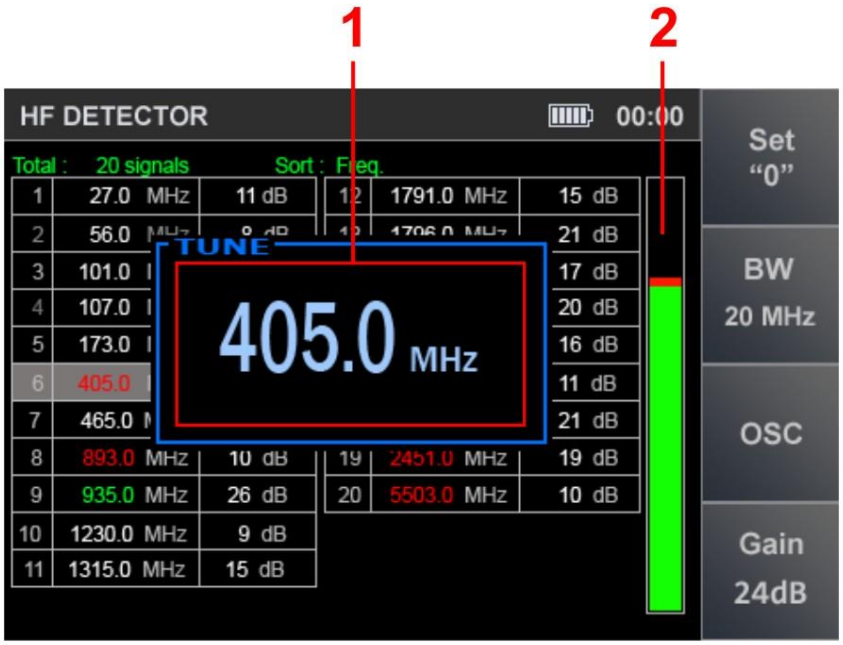



**Fig.15**

A frequency tuning window will appear on the screen (fig.15, 1). Using keys ◁ ▷ set the frequency value at the maximum signal level (fig. 15, 2). The increment is 0.2 MHz.

When finished, press "ENTER" or "ESC".

### 3.3.2. OSCILLOSCOPE

To analyze the demodulated signal with the oscilloscope use the keys ◁ ▷ to select the corresponding table row and press "F3". Functionality and controls described in 3.2.3.

To turn off the OSCILLOSCOPE, press "F3" or "ESC".

## 3.4. "WIRELESS COMMUNICATION" MODE

The "WIRELESS COMMUNICATION" mode is intended for the detection of signals of the common digital communication standards.

ST 500 makes it possible to monitor operative frequency bands of mobile communication devices separately from those of base stations (if such division is specific to the communications standard). The operative frequency bands of Russian mobile communications systems are set by default. The constitution and parameters of these bands can be adjusted using ST 500 software.

The "USER LIST" function allows monitoring pre-defined frequency bands that are the most likely to be utilized by radio eavesdropping devices. The number of these bands, as well as their boundaries, are also set with the aid of ST 500 software.

The "WIRELESS COMMUNICATION" mode is activated from the "PANORAMA" or DIFFERENTIAL mode by pressing "F1". The "MOBILE DEVICES MONITORING" function is launched automatically.

### 3.4.1. "MOBILE DEVICES MONITORING" FUNCTION

This function helps detect active mobile digital communications devices and analyze their signals in the corresponding frequency range. The screen is shown in fig.16.

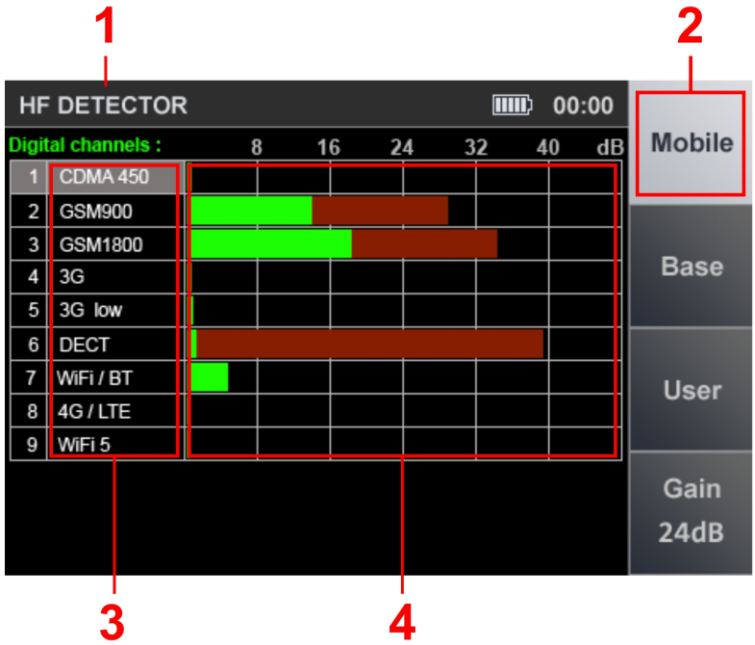



**Fig.16**

**In fig.16:**

1 - active channel
2 - active option (highlighted)
3 - list of digital communication standards
4 - signal levels (green for current level; maroon for peak signal level within the range over the whole monitoring period)

**Controls:**

| Key | Action |
|---|---|
| ▽ △ | table row selection |
| **ENTER** | turning on "ANALYZING DETECTED SIGNALS" function |
| **F2** | turning on "BASE STATIONS MONITORING" function |
| **F3** | turning on "USER LIST" function |
| **F4** | activating gain adjustment |
| **ESC** | returning to "PANORAMA" or DIFFERENTIAL mode (to the previous mode) |
| **MODE** | switching to the main menu of device |
| **F1, FUNC** ◁ ▷ | disabled |

### 3.4.2. "BASE STATIONS MONITORING" FUNCTION

This allows identifying and analyzing the signals from base stations of mobile communications networks in real time. The screen looks as shown in fig.17.

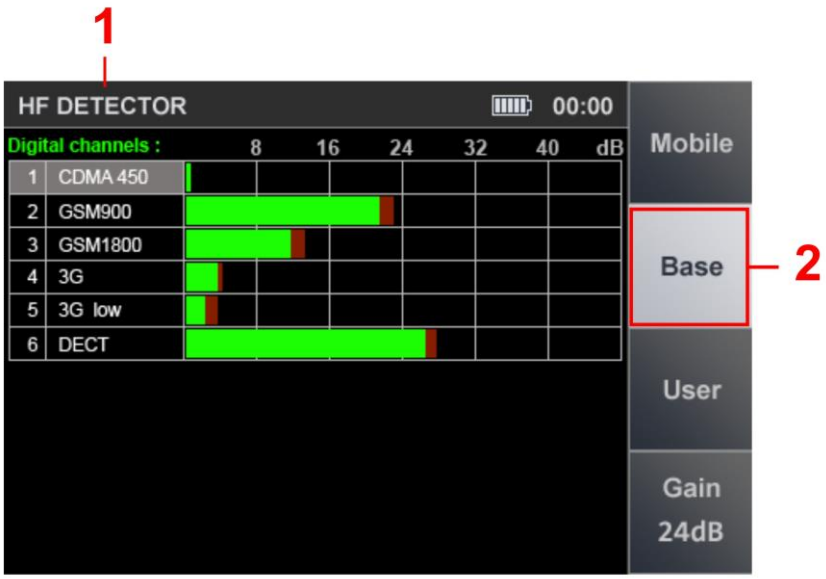



**Fig.17**

**In fig.17:**

1 - active channel
2 - active option (highlighted)

**Controls:**

| Key | Action |
|---|---|
| ▽ △ | table row selection |
| **ENTER** | turning on "ANALYZING DETECTED SIGNALS" function |
| **F1** | turning on "MOBILE DEVICES MONITORING" function |
| **F3** | turning on "USER LIST MONITORING" function |
| **F4** | turning on gain adjustment |
| **ESC** | switching to "PANORAMA" or DIFFERENTIAL mode (to the previous mode) |
| **MODE** | switching to the main menu of device |

### 3.4.3. "USER LIST" FUNCTION

This function allows detecting the activity of radio transmitters in pre-set frequency ranges, and analyze the detected signals.

The screen will look as shown in fig.18.

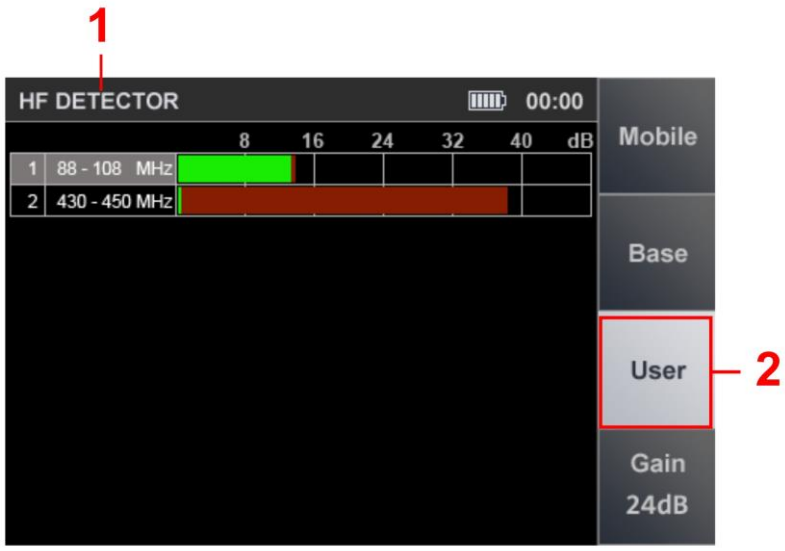



**Fig.18**

**In fig.18:**

1 - active channel
2 - active option (highlighted)

**Controls:**

| Key | Action |
|---|---|
| ▽ △ | table row selection |
| **ENTER** | turning on "ANALYZING DETECTED SIGNALS" function |
| **F1** | turning on "MOBILE DEVICES MONITORING" function |
| **F2** | turning on "BASE STATIONS MONITORING" function |
| **F4** | turning on gain adjustment |
| **ESC** | switching to "PANORAMA" or to the DIFFERENTIAL mode (to the previous mode) |
| **MODE** | switching to the main menu of device |

### 3.4.4. "ANALYZING DETECTED SIGNALS" FUNCTION

The "MOBILE DEVICES MONITORING", "BASE STATIONS MONITORING", and "USER LIST" functions make it possible to detect the presence of signals and estimate their levels; however, it is impossible to determine the number of signals in each range and establish their frequencies with absolute precision.

The "ANALYZING DETECTED SIGNALS" function is intended for a more precise study of the detected signal in a range. It allows determining signal frequencies (in standard bands) and analyzing them with OSCILLOSCOPE

It can be activated from any screen of the "WIRELESS COMMUNICATION" mode. To activate it, use the ▽ △ to select a table row with a detected signal, and press "ENTER".

Upon activation, the screen will look as shown in fig.19.

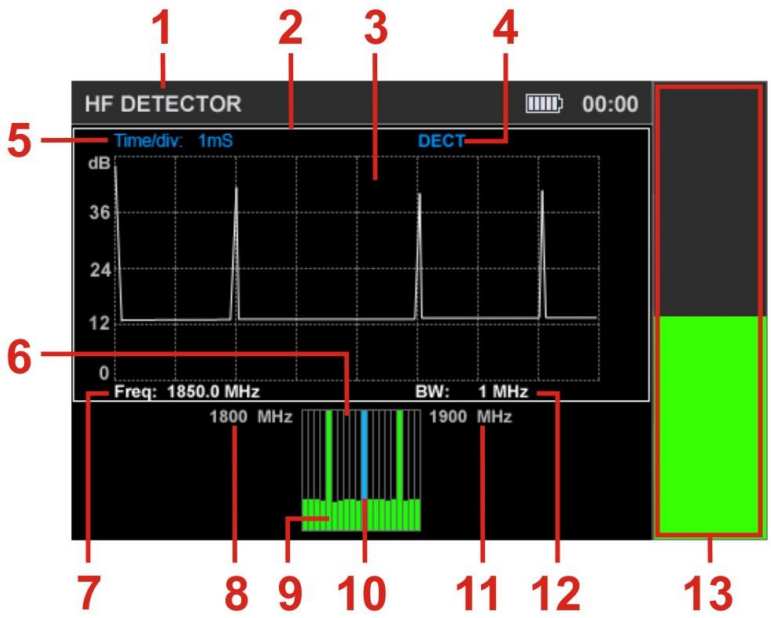



**Fig.19**

**In fig.19:**

1 - active channel
2 - white frame of the active window (OSCILLOSCOPE or SPECTRUM ANALYZER)
3 - OSCILLOSCOPE window
4 - digital communications standard
5 - division value of the oscilloscope time axis
6 - SPECTRUM ANALYZER window
7 - frequency value at SPECTRUM ANALYZER marker position
8 - lower bound of range
9 - spectrum
10 - SPECTRUM ANALYZER marker
11 - upper bound of range
12 - passband width
13 - signal level (at the current frequency)

**The screen is divided into three windows:**

- Signal level bar (fig.19, 13)
- OSCILLOSCOPE (fig.19, 3)
- SPECTRUM ANALYZER (fig.19, 6)

The signal level bar shows signal level at the current frequency (fig.19, 7) as determined by the position of the SPECTRUM ANALYZER marker (fig.19, 10). The oscillogram (fig.19, 3) and the spectrogram (fig.19, 6) are displayed in two other windows. Only one window can be active at a time, highlighted by a white frame (fig.19, 2). To switch between OSCILLOSCOPE and SPECTRUM ANALYZER windows, use the ▽ and △ keys.

For locating the source of the detected signal, the "SET "0" function is implemented. When activated, the detected signal level is set as "0" and the signal level bar will be showing the difference in excess of it (the level bar changes color to lilac).

To turn the "SET "0" function on/off, use "ENTER".

### OSCILLOSCOPE and SPECTRUM ANALYZER controls

| Key | Action |
|---|---|
| **MODE** | switching to the main menu of device |
| **ESC** | switching to the previous mode |
| **ENTER** | turning on/off SET "0" function |
|  | horizontal zoom (OSCILLOSCOPE)<br>cursor positioning (SPECTRUM ANALYZER) |
|  | switching between OSCILLOSCOPE and SPECTRUM ANALYZER |
| **F1 - F4, FUNC** | disabled |

## 4. "INFRARED DETECTOR" CHANNEL ("IR DETECTOR")

The "IR DETECTOR" channel is intended for the detection of eavesdropping devices that utilize the infrared range for transmissions.

The infrared detector sensor is located on the upper surface of the Device (fig.2, 5).

Analysis of the detected signals is carried out using:

- graphic information (oscillogram and signal level bar)
- acoustic information (headphones or built-in speaker).

The channel is activated from the main menu (fig.4). The screen will look as shown in fig.20.

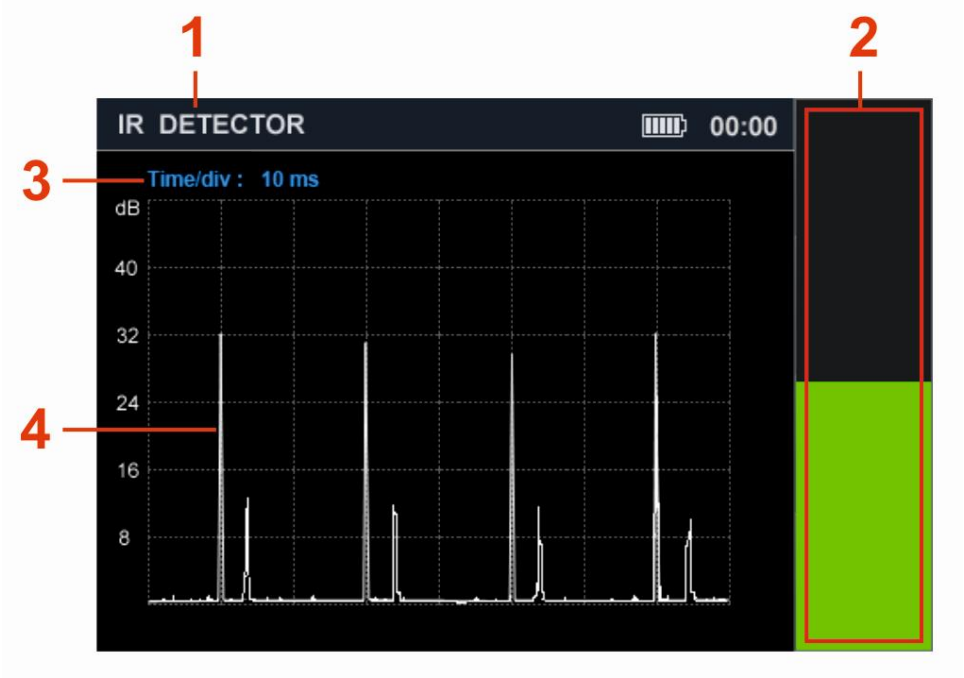



**Fig.20**

**In fig.20:**

1 – active channel
2 – signal level bar
3 – division value of the time axis
4 - oscillogram

**Controls**

| Key | Action |
|---|---|
| **ESC, MODE** | switching to main menu |
| **ENTER** | turning on/off DIFFERENTIAL mode |
| ◁ ▷ | horizontal zoom of the oscilloscope |
| **F1 - F4, FUNC** ▽ △ | disabled |

### 4.1. DIFFERENTIAL MODE

The DIFFERENTIAL mode helps locate the source of a detected IR signal.

Upon activation, the detected signal level will be set as "0" and the signal level bar will be showing the difference in excess of it.

To activate the DIFFERENTIAL mode press "ENTER". The level bar will change color to lilac.

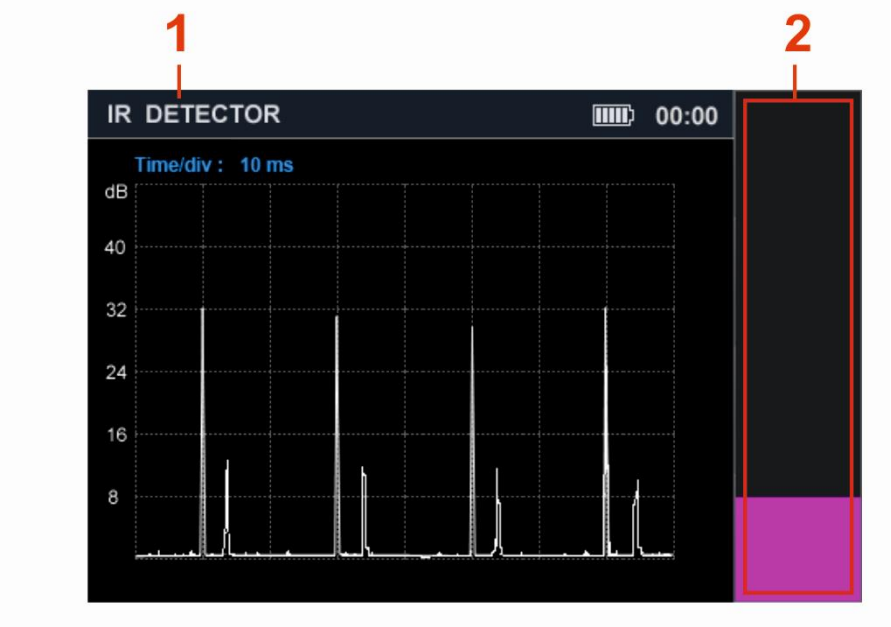



**Fig.21**

To exit DIFFERENTIAL mode, press "ENTER".

# 5. CONNECTING ST 500 TO CABLING

For connecting the Device to the tested circuits, various cables and adapters are supplied with ST 500. They are shown yellow in the figs. 22-27 below.

## 5.1. CONNECTING TO ELECTRIC MAINS

The device is connected to electric mains using an adapter (fig.1, 2), for "WIRED RECEIVER" channel (6.3).

The connection scheme is shown in fig.22.

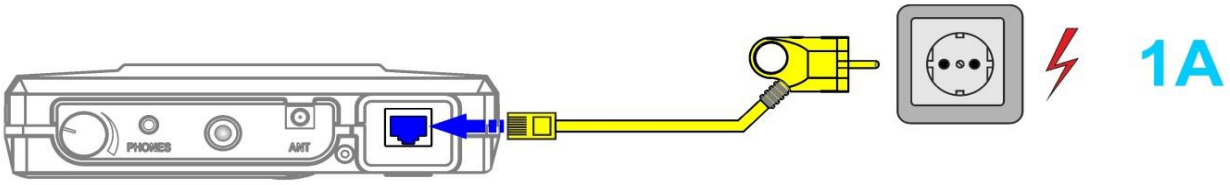



**Fig.22**

The adapter in an electric mains plug is connected to the mains socket, and the other end of the cable is connected to the "INPUT" socket of the main unit (fig.2, 7). A LED on the adapter will indicate if there is voltage on the circuit (lit if present).

## 5.2. CONNECTING TO LAN

### CONNECTING TO LAN CABLES EQUIPPED WITH RJ45 PLUGS

When testing LAN cables without parallel connection of any end user devices (PCs, network printers, VoIP telephones, *etc.*) a LAN cable with RJ45 plug is connected to the "INPUT" socket of the main unit (fig.2, 7).

The connection scheme is illustrated in fig.23, 2A.

If a parallel connection of end user devices is necessary during testing, the following is used:

- cable for connecting the main unit to LAN sockets (fig.1, 4)
- RJ45 splitter (fig.1, 13)
- RJ45 coupler (fig.1, 11).

The connection scheme is shown in fig.23, 2B.

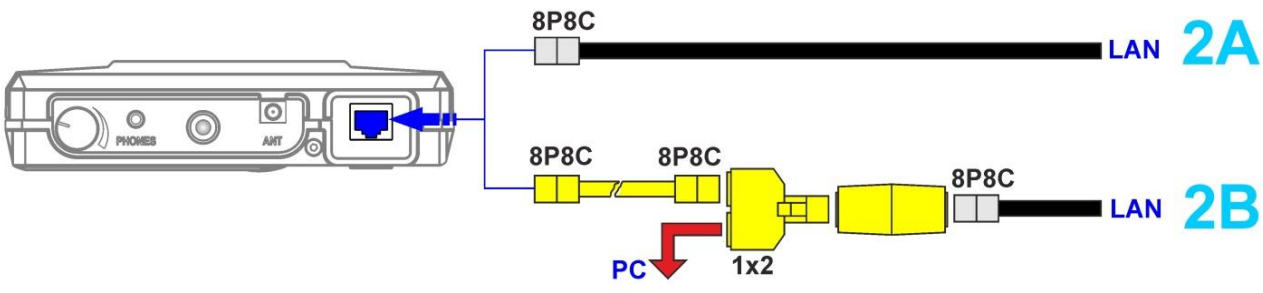



**Fig.23**

### CONNECTING TO A LAN CABLE EQUIPPED WITH AN RJ45 SOCKET

When testing a LAN line without parallel connection of any end user devices, the Device is connected to the computer socket with a patch cord (fig.1, 4). The connection scheme is shown in fig.24, 2C.

If a parallel connection of end user devices is necessary during testing, the following is used:

- cable for connecting the main unit to LAN sockets (fig.1, 4)
- RJ45 splitter (fig.1, 13).

The connection scheme is shown in fig.24, 2D.

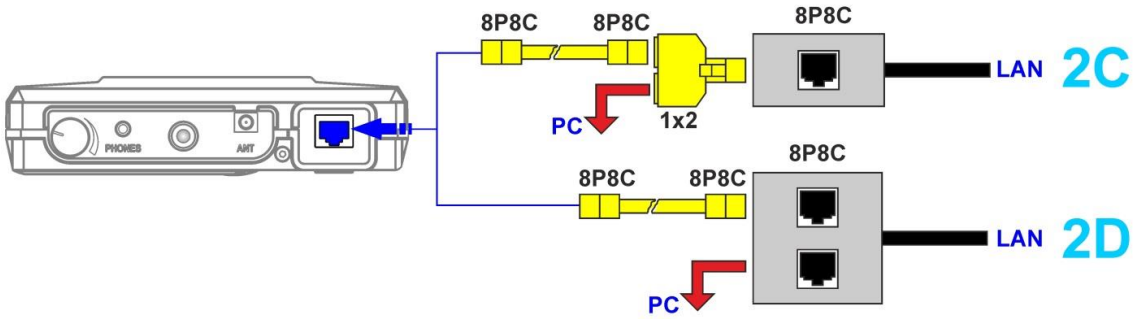



**Fig.24**

## 5.3. CONNECTING TO TELEPHONE LINES

Telephone lines can be equipped with **RJ11 plugs** or **RJ11 sockets.**

### CONNECTING TO TELEPHONE LINE EQUIPPED WITH AN RJ11 PLUG

If there is no necessity in keeping a parallel connection of end user devices (telephone, fax), a cable fitted with an RJ11 plug (fig.1, 3) is connected to the Device through an RJ11 coupler (fig.1, 12). The connection scheme is shown in fig.25, 3A.

If a parallel connecition of end user devices is needed during testing, the following is used:

- cable for connecting the main unit to telephone line sockets (fig.1, 3)
- RJ11 splitter (fig.1, 12)
- RJ11 coupler (fig.1, 10).

The connection scheme is shown in fig.25, 3B.

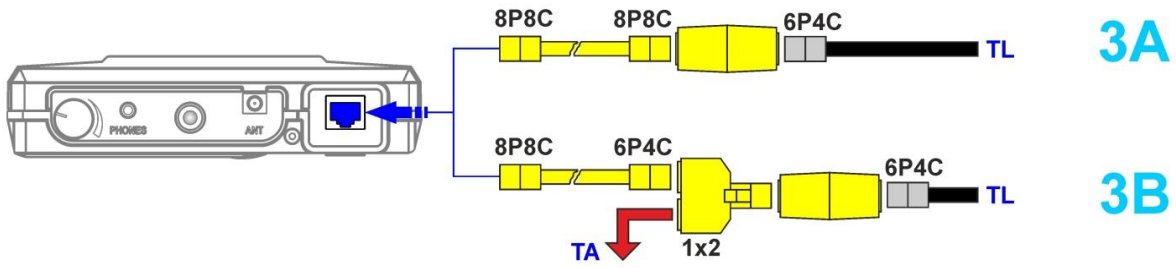



**Fig.25**

### CONNECTING TO A TELEPHONE LINE EQUIPPED WITH AN RJ11 SOCKET

While testing telephone lines, if there is no necessity in a parallel connection of end user devices, a cable fitted with an RJ11 socket is cable-connected to the main unit (fig.1, 3). The connection scheme is shown in fig.26, 3C.

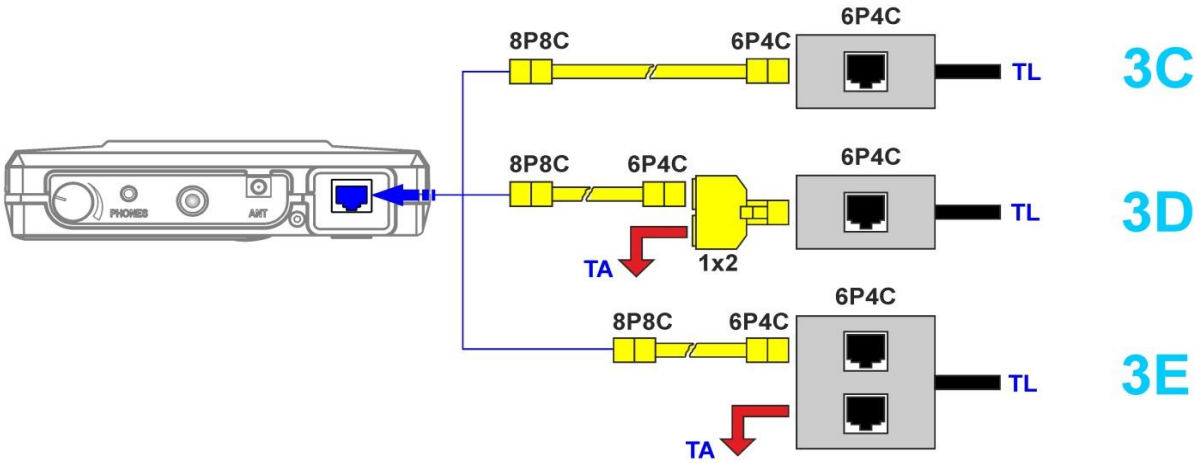



**Fig.26**

Ways of **parallel-connecting** to telephone lines, when end user devices (telephones or facsimile machines) need to be in operation, are shown in fig.26, **3D and 3E.**

The **3D** option is used when the telephone line is fitted with a **singular** RJ11 socket. An RJ11 splitter (fig.1, 12) and cable (fig.1, 3) are to be used in this case, for connecting the main unit.

The **3E** option is used, when telephone line is fitted with a **double** RJ11 socket. In this case, the Main Unit is connected to one of the two socket inlets through a special cable (fig.1, 3), while a telephone or facsimile machine is connected to the other through a standard cable.

## 5.4. CONNECTING TO LOW CURRENT MULTI-CORE CABLES NOT FITTED WITH CONNECTORS

For testing multiwire cables not equipped with either sockets or plugs, a special adapter (fig.1, 16) is used. The connection scheme is shown in fig.27.

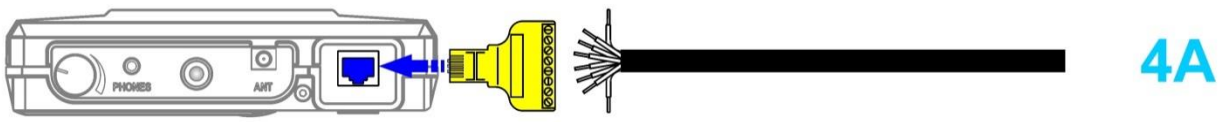



**Fig.27**

When connecting the LAN cable to the adapter, it is advised to observe the wiring color scheme shown in Supplement #3.

# 6. THE "WIRED RECEIVER" CHANNEL

The "WIRED RECEIVER" channel is intended for the detection of signals from eavesdropping devices transmitting over electric mains and low current lines in the frequency range 0.1–180 MHz.

**The detected signals are analyzed with the aid of**

- visual information on the screen
- sounds (through headphones or the inbuilt speaker).

For connecting to electric mains, an adapter (fig.1, 2) is used.
For connecting to low current lines, cables (fig.1, 3, 4) are used.

The mode is activated from the main menu of device, after which it is necessary to determine:

- tested line type (electric mains or low current)
- frequency range (0.1 – 60 MHz or 0.1 – 180 MHz).

## 6.1. CIRCUIT TYPE SELECTION

Upon channel activation use the keys ▽ and △ to select the circuit type ("MAINS" or "LOW CURRENT") and press "ENTER".

**A mains circuit** is connected to the electronic switch through an adapter (fig.1, 2). Control of the electronic switch is disabled: only two cable cores are tested.

**Low current** circuits typically comprise multiwire cabling. Eavesdropping devices can be connected to certain paired combinations of wires. The Device is connected to those by means of the Electronic Switch.

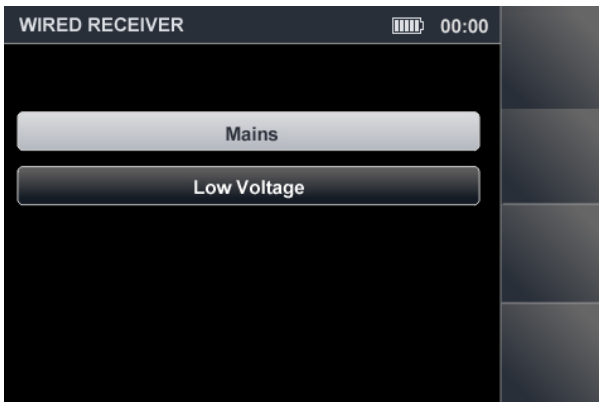



**Fig.28**

## 6.2. FREQUENCY RANGE SELECTION

Using ▽ and △ keys select one of the two frequency bands (0.1 – 60 MHZ or 0.1 – 180 MHz) in which to search for signals, and press "ENTER". Fig.29 shows the frequency range selection menu.

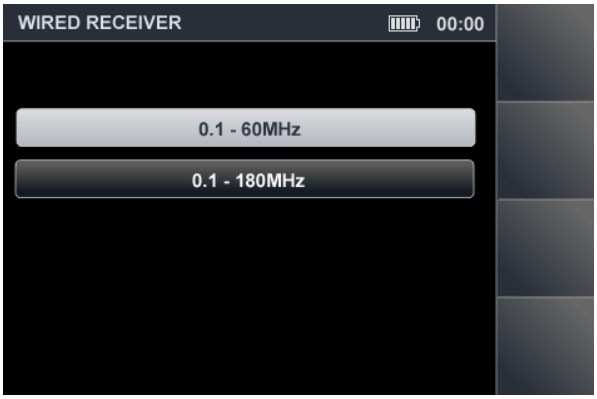
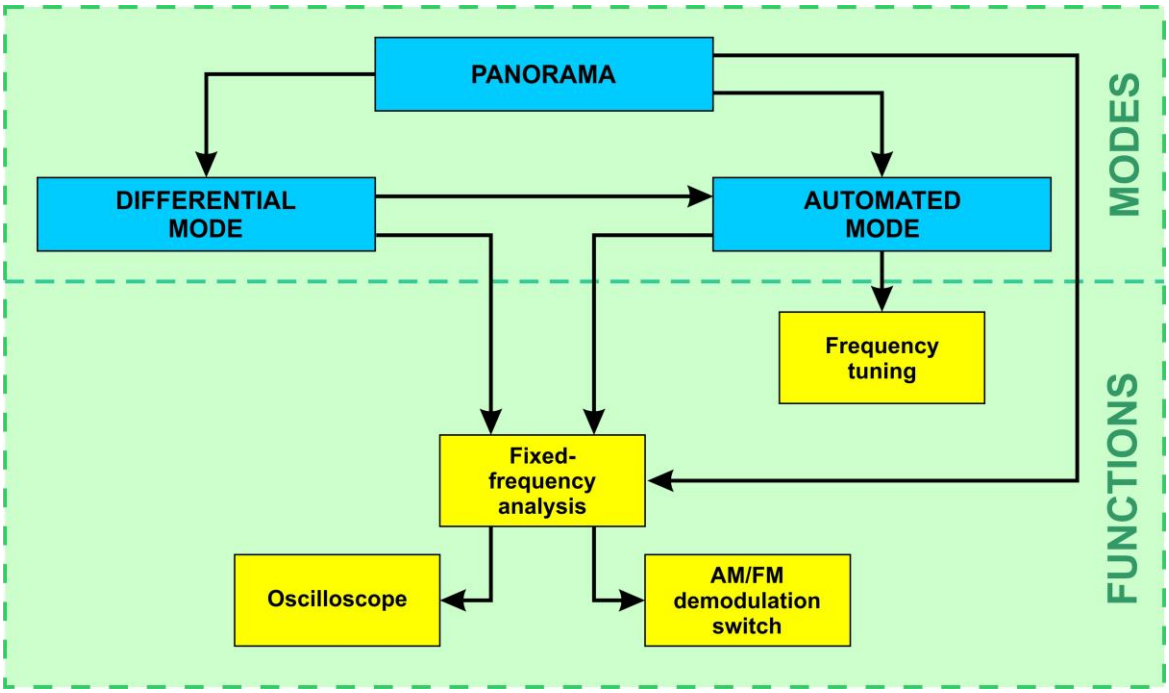



**Fig.29**

## ELECTRIC MAINS TESTING

### FUNCTIONAL SCHEME OF THE "WIRED RECEIVER" CHANNEL (ELECTRIC MAINS TESTING)




### 6.3. "PANORAMA" MODE (ELECTRIC MAINS TESTING)

When "MAINS" is chosen from the menu (fig.28), "PANORAMA" mode turns on, and all the signal activity in the circuit within the selected frequency band is displayed on the screen (fig.30).

**Functionality:**

- analyzing the signal at a set frequency
- obtaining a subtractive representation in the DIFFERENTIAL mode
- searching for signals in the AUTOMATED mode
- activating/deactivating the attenuator (20 dB)
- adjusting the band limits (zoom)

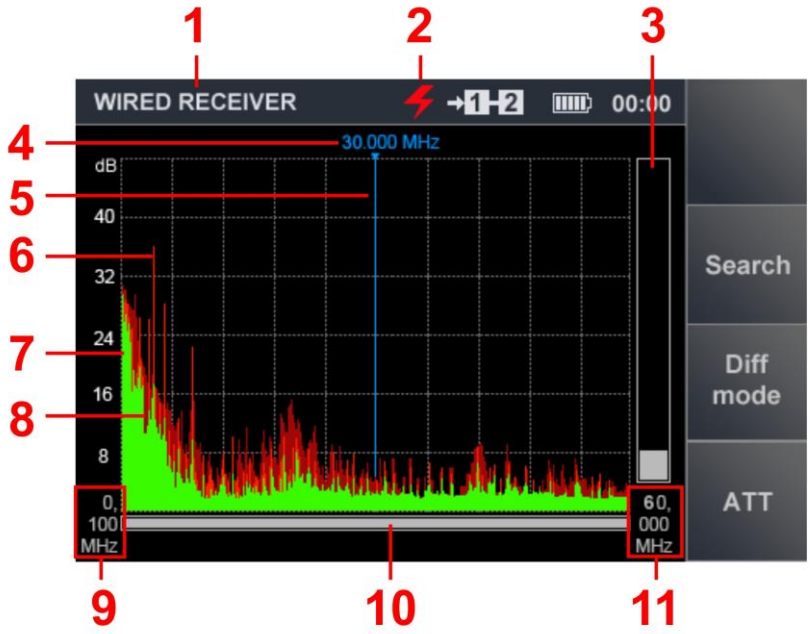



**Fig.30**

**In fig.30:**

1 - active detection channel
2 - electric mains selected
3 - signal level at the selected frequency
4 - frequency value at cursor position
5 - screen cursor
6 - pulse signals detected in the last measurement cycle (red)
7 - steady signals detected in the last measurement cycle (green)
8 - peak signal level at the given frequency over all cycles (maroon)
9 - lower zoom limit
10 - position of the selected band, as against maximum
11 - upper zoom limit

The graphics are periodically refreshed and show the signals received in the range selected for viewing. The constant and pulse components of signals registered during the latest cycle, are shown green and red, respectively.

Maximum signal levels, registered over the whole duration of monitoring the range, are colored maroon.

For more detailed scrutiny of a given segment, use the keys ◁ and ▷ to position the cursor at a signal of interest, or at the center of the segment, and zoom in using the △ key.

The viewed range is displayed in digital (fig.30, 9 and 11) and graphic (fig.30, 10) representations. When the viewed range is changed, any previous data on peak signals (colored maroon) will be discarded. Use ▽ for zooming out.

**Controls**

| Key | Action |
|---|---|
| ▽ △ | setting the range (zoom) |
| ◁ ▷ | cursor positioning |
| **F2** | activating the AUTOMATED mode |

| Key | Action |
|---|---|
| **F3** | activating the DIFFERENTIAL mode |
| **F4** | activating/deactivating the attenuator (20 dB) |
| **ENTER** | turning on "FIXED FREQUENCY ANALYSIS" function |
| **ESC, MODE** | switching to the main menu of device |
| **F1, FUNC** | disabled |

### 6.4. DIFFERENTIAL MODE

The DIFFERENTIAL mode is used to reduce the influence of external interference on the information signals, and evaluate changes in the activity within a band upon connecting new technical appliances to the circuit.

When the DIFFERENTIAL mode is activated, signal levels previously registered over the previous scanning cycles, are set as "0". After that only signal levels in excess of "0" will be displayed.

The DIFFERENTIAL mode is activated from "PANORAMA" by pressing "F3" (the key field will become lighter). The screen will look as shown in fig.31.

To deactivate the DIFFERENTIAL mode (return to "PANORAMA"), press "F3" (the key field will become darker). Attenuator and passband settings are saved.

**Functionality:**

- analyzing the signal at a set frequency
- search for signals in the AUTOMATED mode
- activating/deactivating the attenuator (20 dB)
- adjusting the band limits (zoom)

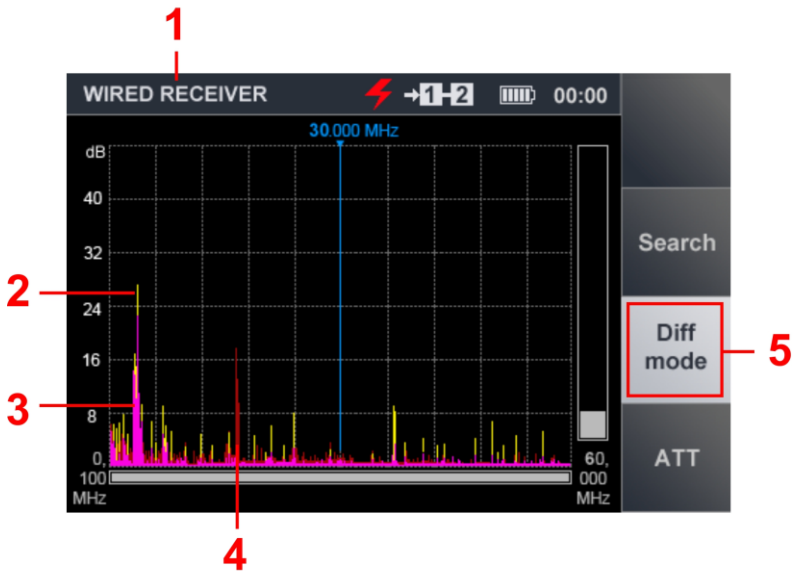



**Fig.31**

**In fig.31:**

1 - active detection channel
2 - differential spectrum of pulse signals obtained in the latest measurement cycle (yellow)
3 - differential spectrum of steady signals obtained in the latest measurement cycle (lilac)
4 - differential spectrum obtained over all previous measurement cycles (maroon)
5 - highlighting that indicates that the DIFFERENTIAL mode is on

**Controls**

| Key | Action |
|---|---|
| ▽ △ | adjusting the band limits (zoom) |
| ◁ ▷ | cursor positioning |
| **F2** | activating the AUTOMATED mode |
| **F3** | deactivating the DIFFERENTIAL mode |
| **F4** | activating/deactivating the attenuator (20 dB) |
| **ENTER** | activating "FIXED FREQUENCY ANALYSIS" function |
| **ESC, MODE** | switching to the main menu of device |
| **F1, FUNC** | disabled |

### 6.4.1. "FIXED FREQUENCY ANALYSIS" FUNCTION

This function is used for studying signals detected in the "PANORAMA" or DIFFERENTIAL mode. It allows listening to a demodulated (AM/FM) signal and researching it with the OSCILLOSCOPE.

The inclusion of the function is carried out from the "PANORAMA" or the DIFFERENTIAL mode. To activate it, use ◁ and ▷ to set the cursor at a given signal, and press "ENTER". The screen will look as shown in fig.32.

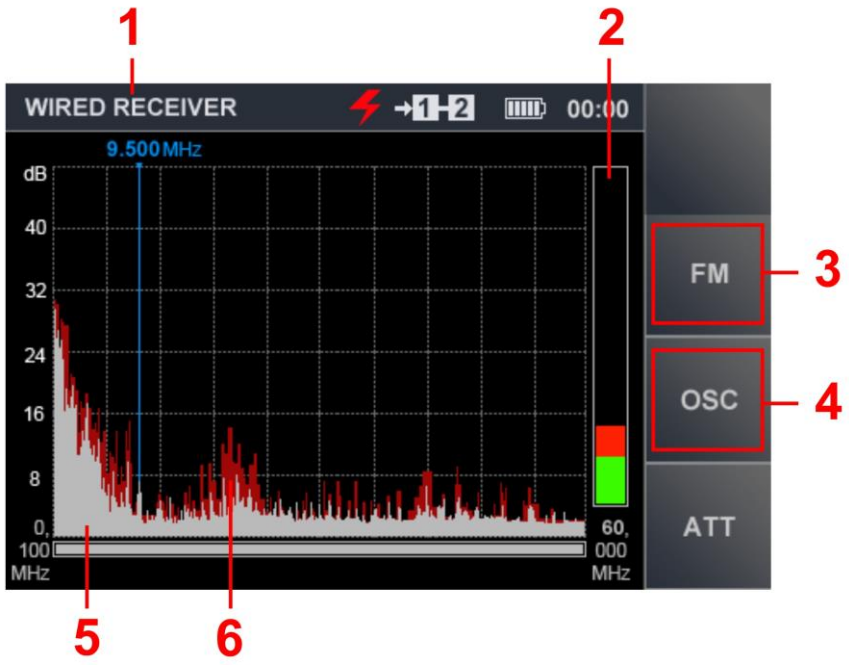



**Fig.32**

**In fig.32:**

1 - active detection channel
2 - signal level at the selected frequency
3 - "F2" (toggling AM/FM demodulation)
4 - "F3" (turn on OSCILLOSCOPE)
5 - spectrum obtained in the latest measurement cycle (grey)
6 - peak signal level at the given frequency over all cycles (maroon)

**Functionality:**

- activating/deactivating the attenuator (20 dB)
- AM/FM demodulation toggling
- researching signals with the OSCILLOSCOPE
- frequency tuning

**Controls:**

| Key | Action |
|---|---|
| ◁▷ | cursor positioning (frequency tuning) |
| **F2** | toggling AM/FM demodulation |
| **F3** | turning on OSCILLOSCOPE |
| **F4** | activating/deactivating the attenuator (20 dB) |
| **ENTER, ESC** | turning on "FIXED FREQUENCY ANALYSIS" function |
| **MODE** | switching to the main menu of device |

### 6.4.2. OSCILLOSCOPE

The OSCILLOSCOPE helps study a signal at a fixed frequency. To do this, press the "F3". After that, the "OSC" key field will become lighter. The screen view of the device is shown in fig.33.

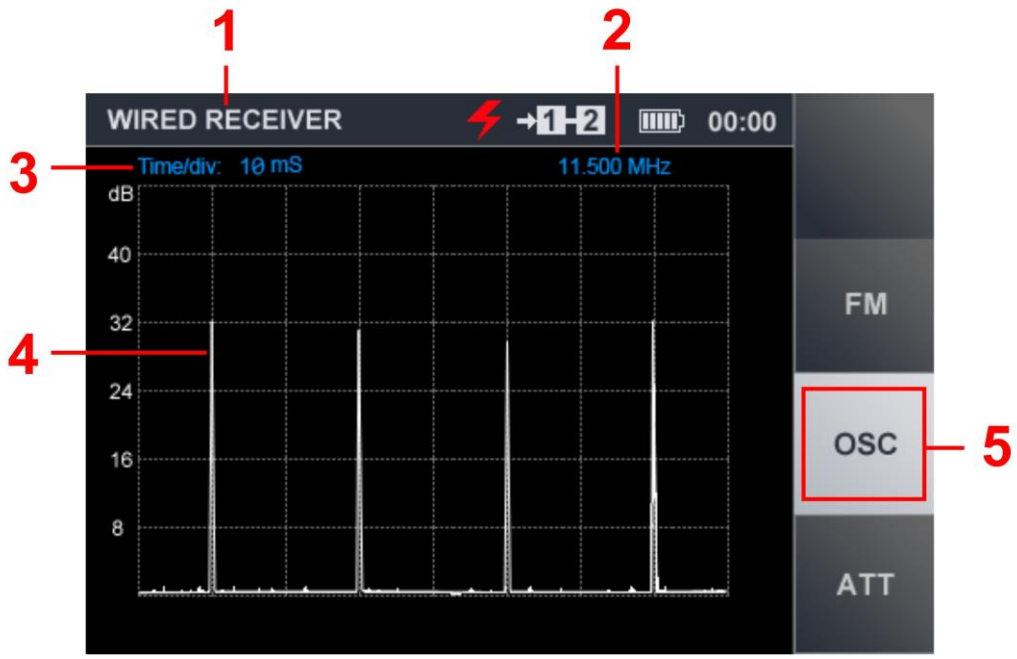



**Fig.33**

**In fig.33:**

1 - active channel
2 - selected frequency value
3 - set division value of the time axis
4 - oscillogram of the signal at the set frequency
5 - indication of the inclusion of the "OSCILLOSCOPE" function

**Functionality:**

- determining the time parameters of the demodulated signal
- setting the division value of the time axis
- listening to a demodulated (AM/FM) signal
- activating/deactivating the attenuator (20 dB)

**Controls:**

| Key | Action |
|---|---|
| ◁▷ | setting the division value of the horizontal sweep<br>100μS/200μS/500μS/1mS/2mS/5mS/10mS |
| **F2** | toggling AM/FM demodulation |
| **F3, ESC** | turning off OSCILLOSCOPE |
| **F4** | activating/deactivating the attenuator (20 dB) |
| **MODE** | switching to main menu of device |

### 6.5. AUTOMATED MODE

In the AUTOMATED mode, the signals are registered whose amplitude exceeds the adaptive detection threshold. Inclusion is made from the "PANORAMA" mode or from the DIFFERENTIAL mode, by pressing "F2". The screen view is shown in fig.34.

**IMPORTANT!** Search for signals is performed within the set boundaries, based on the readings obtained in the DIFFERENTIAL mode (if activated from the DIFFERENTIAL mode).

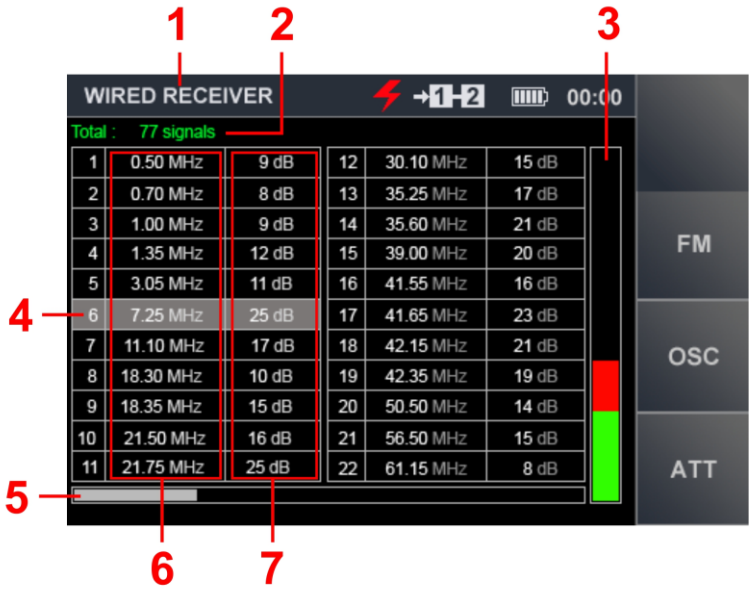



**Fig.34**

**In fig.34:**

1 - active channel
2 - number of the detected signals
3 - signal level, at current cursor position
4 - current table row
5 - current position as related to the total number of rows
6 - frequencies of the detected signals
7 - levels of the detected signals

**Functionality:**

- sorting of the detected signals (by frequency or by level)
- quick tuning to the detected signal by selecting it in the table
- frequency tuning
- activating/deactivating the attenuator (20 dB)
- AM/FM demodulation toggling
- researching signals with OSCILLOSCOPE

**Controls:**

| Key | Action |
|---|---|
| ◁ ▷ ▽ △ | table row selection |
| **FUNC** | sorting signals |
| **F2** | toggling AM/FM demodulation |
| **F3** | turning on OSCILLOSCOPE |
| **F4** | activating/deactivating the attenuator (20 dB) |
| **ENTER** | turning on "FREQUENCY TUNING" function |
| **ESC** | switching to the previous mode |
| **MODE** | switching to main menu of device |

### 6.5.1. "FREQUENCY TUNING" FUNCTION

For tuning to a frequency select the corresponding table row and press "ENTER".

Frequency tuning window (fig.35, 1) will appear. Using the keys ◁ ▷ with a 10 kHz increment, set the frequency to obtain maximum response on the signal strength bar (fig.35, 2).

The function is turned off by pressing "ENTER" or "ESC".

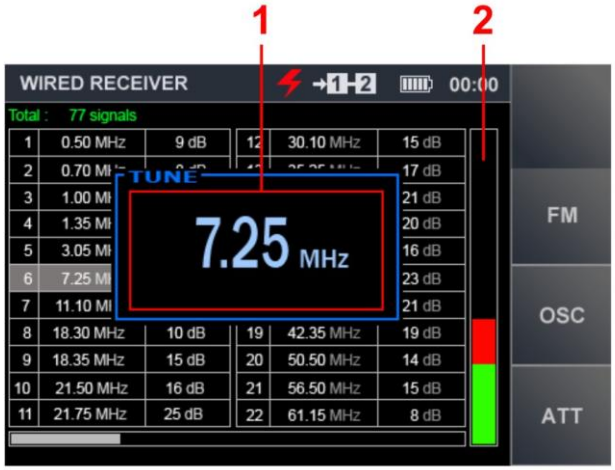



**Fig.35**

### 6.5.2. OSCILLOSCOPE

To analyze a demodulated signal using the "OSCILLOSCOPE" function, in the AUTOMATED mode table, place the cursor on the corresponding row and press "F3".

**Functionality:**

- determining the time parameters of the demodulated signal
- setting the division value of the time axis
- listening to an AM- or FM-demodulated signal
- on/off attenuator (20 dB).

**Controls:**

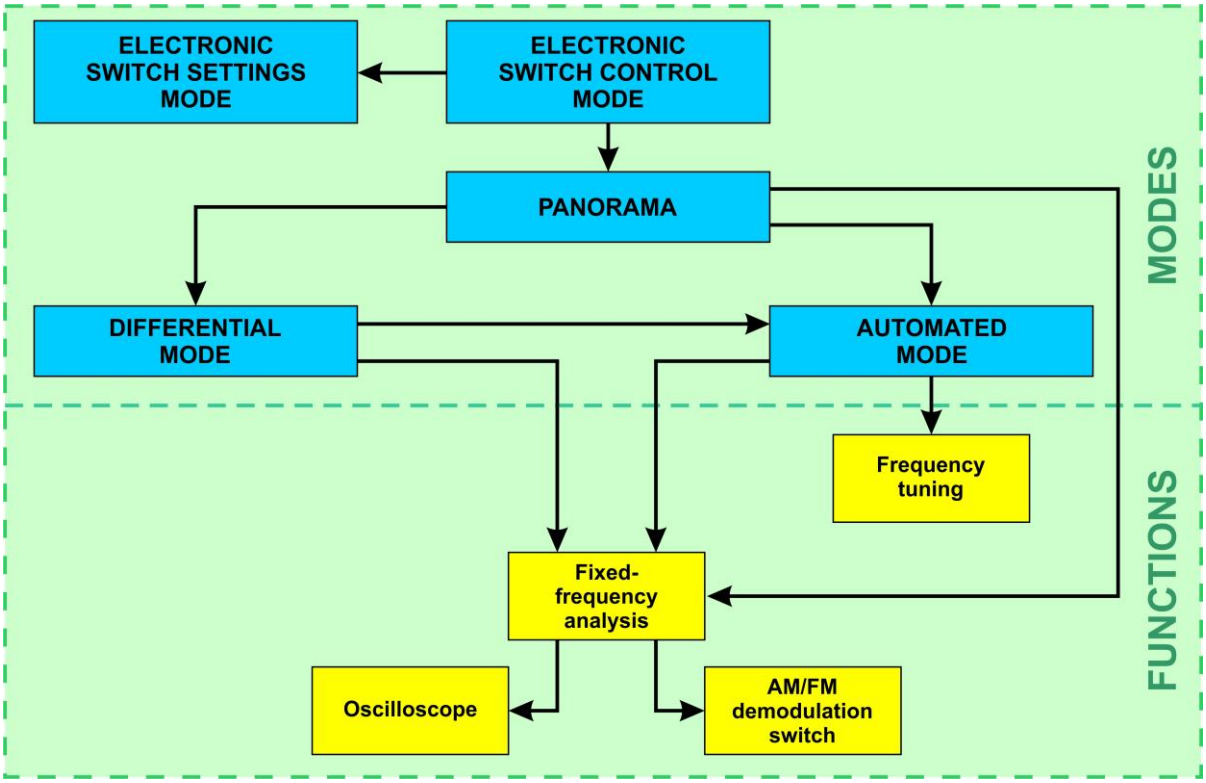
| Key | Action |
|---|---|
| ◁▷ | setting the division value of the horizontal sweep 100μS/200μS/500μS/1mS/2mS/5mS/10mS |
| **F2** | toggling AM/FM demodulation |
| **F3, ESC** | turning off OSCILLOSCOPE |
| **F4** | on/off attenuator (20 dB) |
| **MODE** | switching to the main menu of device |

To turn off the OSCILLOSCOPE, press "F3" or "ESC".

## LOW CURRENT CIRCUIT TESTING

Low current circuits typically utilize multiwire cables. When searching for eavesdropping devices that may be connected to low current circuits, one should test all the possible paired combinations of wires.

**FUNCTIONAL SCHEME OF THE "WIRED RECEIVER" CHANNEL (LOW CURRENT CIRCUITS TESTING)**




### 6.6. "ELECTRONIC SWITCH CONTROL" MODE

Upon selection of the "LOW VOLTAGE" menu item (6.1), the Device will switch to "ELECTRONIC SWITCH CONTROL" mode.

A table is displayed on the screen (fig.36), in which all combinations of wires of a multi-wire cable and measured DC and AC voltage values in each pair are presented.

If the voltage (Vdc) in the connected pair exceeds ± 50 V, the inscription ">50" appears in the corresponding cell.

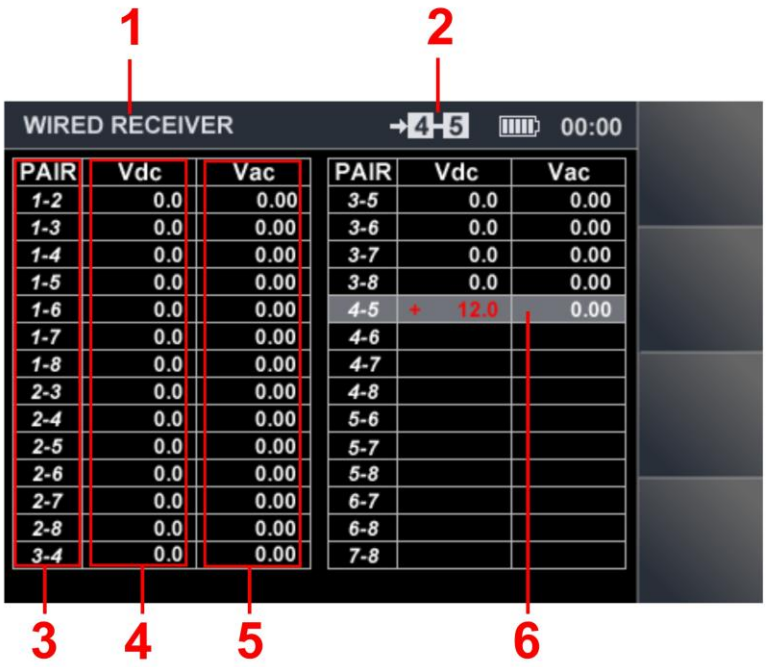



**Fig.36**

**In fig.36:**

1 - active channel
2 - pair of wires connected
3 - pairs of wires
4 - direct voltage on wire pairs
5 - alternating voltage on wire pairs
6 - current table row

**Functionality:**

- selecting a paired combination of wires
- analyzing signals in the selected pair
- electronic switch setup

**Controls:**

| Key | Action |
|---|---|
| ▽ △ ◁ ▷ | table row selection (selecting a pair of wires to be tested) |
| **ENTER** | activating "PANORAMA" mode |
| **ESC, MODE** | switching to the main menu of device |
| **FUNC** | activating "ELECTRONIC SWITCH SETTINGS" mode |
| **F1 - F4** | disabled |

To select a pair of wires, use the ▽ △ ◁ ▷ to set the table cursor to the corresponding row in the table. When the "ENTER" is pressed, the "PANORAMA" mode will be turned on and a panorama of the range loading in the selected pair of wires will be displayed on the screen.

### 6.7. "ELECTRONIC SWITCH SETTINGS" MODE

This mode is intended for setting up the electronic switch before testing low current multiwire cables. The setting-up procedure consists in choosing the pin numbers in the 8-pin socket of the electronic switch, to be connected to the cores of the cable under inspection. One of the four connection options for RJ connectors is thus chosen:

**8P8C** – eight position connector (all 8 pins engaged)
**6P6C** – six position connector (all 6 pins engaged)
**6P4C** – six position connector (4 central pins engaged)
**6P2C** – six position connector (2 central pins engaged)

RJ standard description is given in **Supplement #2**

If the tested cable is not equipped with connectors, or the connectors are non-standard, a **manual setup of the electronic switch** is possible**.**

**Most common custom settings of the electronic switch are shown in Supplement #2**

Electronic switch settings are not changed until switching to the Main menu of the device.
To activate "ELECTRONIC SWITCH SETTINGS" mode, press "FUNC". The screen will look as shown in fig.37 below.

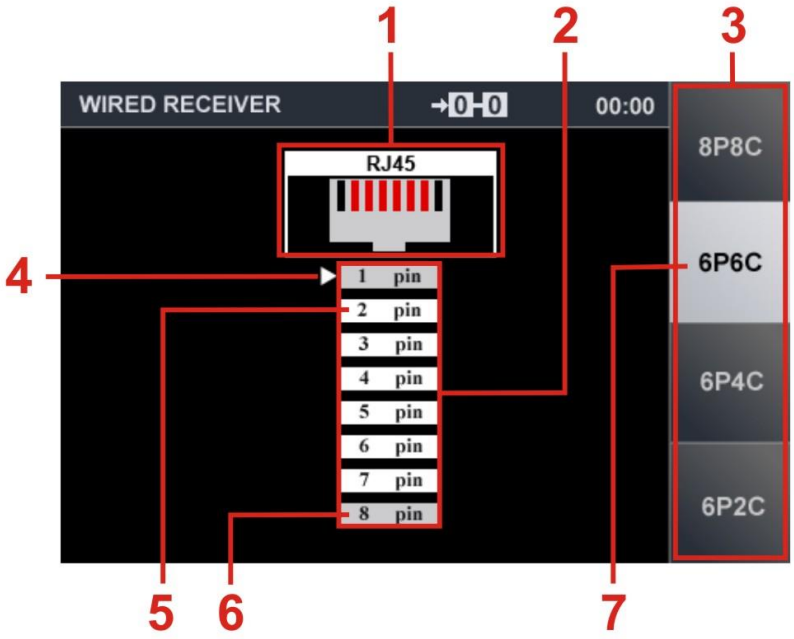



**Fig.37**

**In fig.37:**

1 - graphic representation of the input connector of the electronic switch
2 - adjustable list of electronic switch pins
3 - fields for turning on/off standard connection options
4 - current position marker
5 - connected pin (white background)
6 - disconnected pin (grey background)
7 - active standard connection scheme (highlighted)

**Controls:**

| Key | Action |
|---|---|
| ▽ △ | navigation |
| **ENTER** | connecting/disconnecting the selected pin |
| **F1** | activating/deactivating the standard **8P8C** scheme |
| **F2** | activating/deactivating the standard **6P6C** scheme |
| **F3** | activating/deactivating the standard **6P4C** scheme |
| **F4** | activating/deactivating the standard **6P2C** scheme |
| **ESC, FUNC** | exiting the mode (to the previous screen) |
| ◁ ▷, **MODE** | disabled |

To finish the electronic switch setup and switch to "ELECTRONIC SWITCH CONTROL" mode, press "FUNC" or "ESC".

If any pins have been disengaged in the setting-up stage, upon switching back to "ELECTRONIC SWITCH CONTROL" mode, the table will look different.

Fig.38 shows the table, when the standard 6P6C connection scheme is used on the electronic switch: pins #1 and #8 are off, and no paired combinations that include these wire connections will be tested.


**Fig.38**

## 6.8. "PANORAMA" MODE (LOW CURRENT CIRCUIT TESTING)

To activate the "PANORAMA" mode, in "ELECTRONIC SWITCH CONTROL" mode select the pair of wires to be monitored (fig.36, 6) and press "ENTER". Activity in the frequency band will be displayed on the screen (fig.39).

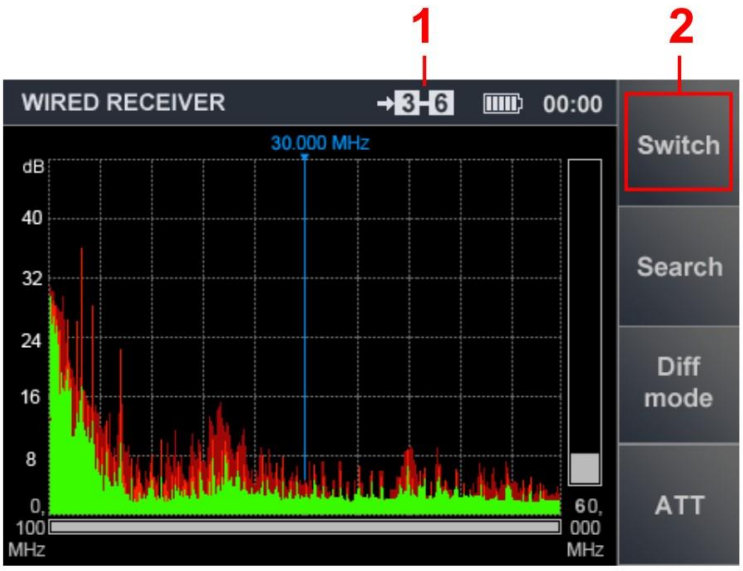



**Fig.39**

**In fig.39:**

1 - pair of wires connected
2 - key for returning to the previous screen

The "Switch" key is used to activate to the "ELECTRONIC SWITCH CONTROL" mode (fig.36) for connecting and analyzing another pair of wires.

**Controls**

| Key | Action |
|---|---|
| ▽ △ | band setting (zoom) |
| ◁ ▷ | cursor positioning |
| **F1** | switching to "ELECTRONIC SWITCH CONTROL" mode |
| **F2** | activating the AUTOMATED mode |
| **F3** | activating the DIFFERENTIAL mode |
| **F4** | activating/deactivating the attenuator (20 dB) |
| **ENTER** | turning on "FIXED FREQUENCY ANALYSIS" function |
| **ESC, MODE** | switching to the main menu of device |
| **FUNC** | disabled |

The operation modes (controls and functions) are similar to those **when testing electric mains.**

The "PANORAMA", DIFFERENTIAL and AUTOMATED modes are described in 6.3, 6.4, and 6.5, respectively.

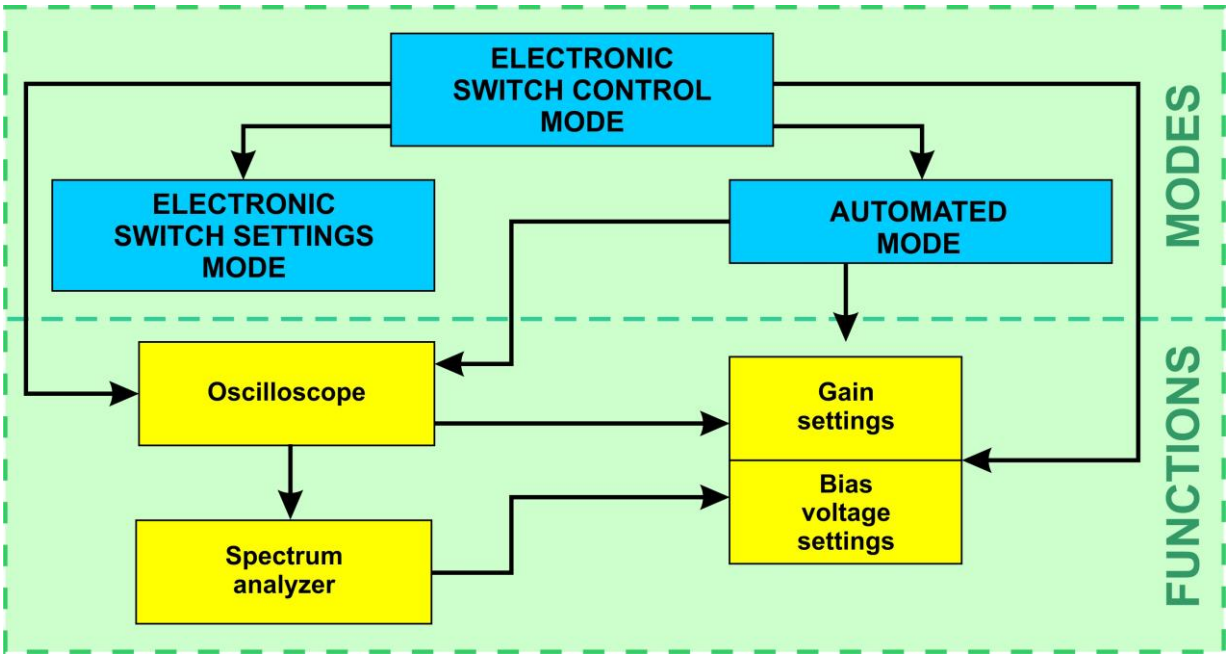
# 7. "LOW FREQUENCY AMPLIFIER" CHANNEL

The "LOW FREQUENCY AMPLIFIER" channel is intended for the detection of low-frequency signals from eavesdropping devices in low current circuits.

An oscillogram, spectrogram and acoustic information are used to analyze the detected signals.

The channel is turned on from the main menu of the device (fig.4)

**FUNCTIONAL SCHEME OF THE "LOW FREQUENCY AMPLIFIER" CHANNEL**




**FUNCTIONALITY:**

- electronic switch setup
- connecting pairs of wires in the manual mode
- automatic sequential selection of all paired wire combinations, with a possibility to analyze signals on each combination acoustically
- gain setting
- applying a bias voltage to the circuit
- acoustic analysis of the signal on the pair of wires connected to the Device
- measuring direct and alternating voltage on the pair of wires connected to the Device
- analyzing the signal on the pair connected to the Device by means of oscillogram and spectrogram

## 7.1. "ELECTRONIC SWITCH CONTROL" MODE

After the channel is turned on, the "ELECTRONIC SWITCH CONTROL" mode starts. The screen view is shown in fig.40.

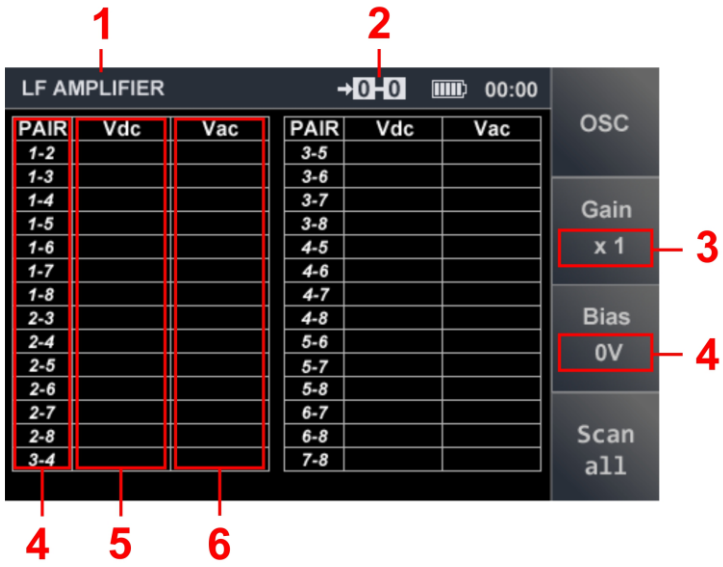



**Fig.40**

**In fig.40:**

1 - active channel
2 - pair of wires connected
3 - gain selected
4 - bias voltage selected
5 - wire pairs
6 - measured values of direct voltage
7 - measured values of alternating voltage

The measured values of direct and alternating voltage are shown for the pair of wires that is currently selected in the table (fig.41).

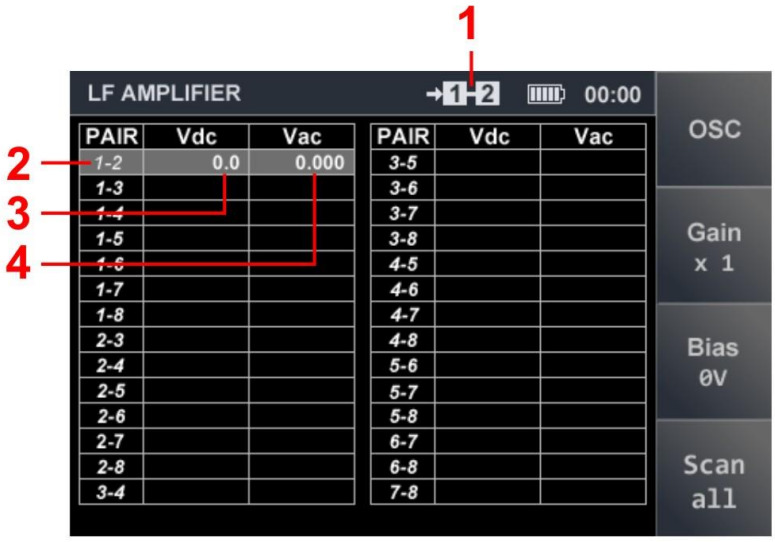



**Fig.41**

**In fig.41:**

1 - connected pair of wires
2 - current table row
3 - the value of the DC voltage
4 - the value of the AC voltage

**Controls:**

| Key | Action |
|---|---|
| ⇩ ⇧ ⇦ ⇨ | table row selection (connecting pairs of wires) |
| **F1, ENTER** | turning on OSCILLOSCOPE |
| **F2** | gain setting on/off |
| **F3** | bias voltage setting on/off |
| **F4** | activating the AUTOMATED mode |
| **ESC, MODE** | switching to the main menu of device |
| **FUNC** | activating "ELECTRONIC SWITCH SETTINGS" mode |

## 7.2. "ELECTRONIC SWITCH SETTINGS" MODE

Switching on the "ELECTRONIC SWITCH SETTINGS" mode is performed by pressing the "FUNC". The settings procedure is described in 6.7. This is what the screen looks like upon setting the electronic switch to the 6P4C scheme (fig.42). Pins #1, 2, 7, 8 are disabled (highlighted grey). The four central pins #3,4,5,6 are enabled (highlighted white).


**Fig.42**

To finish the electronic switch setup and return to "ELECTRONIC SWITCH CONTROL" mode, press "FUNC" or "ESC".

## 7.3. SETTING THE GAIN

In order to set the gain value, do the following

1. Press "F2". The "Gain" field will become brighter.
2. Using the keys ⇩ ⇧ ⇦ ⇨, set the desired gain multiplier (x1, x2, x5, x10, x20, x50, x100). The selected value will be shown on the screen (fig.43, 1).
3. If setting x1 gain is desired, press "ENTER".
4. When done, press "F2". The "Gain" field will become darker.

**Important!** While setting the gain, other features are inaccessible.

The screen view when setting the gain value is shown in fig.43.


**Fig.43**

The selected gain value remains unchanged until next adjustment or "LOW FREQUENCY AMPLIFIER" channel deactivation (return to main menu of device).

## 7.4. SETTING THE BIAS VOLTAGE

In order to apply a bias voltage to a connected pair of wires, do the following

1. Press "F3". The "Bias" field will become brighter.
2. Using the keys ⇩⇧ select the bias voltage (-30 V or +30 V) which will be displayed on the screen (fig.44, 1 and 2). The bias voltage value will be marked green, and voltage in the circuit will be marked white.
3. To reverse the sign of the bias voltage, use ⇦ or ⇨.
4. To set "0" value, press "ENTER".
5. To finish, press "F3". The "Bias" field will become darker.

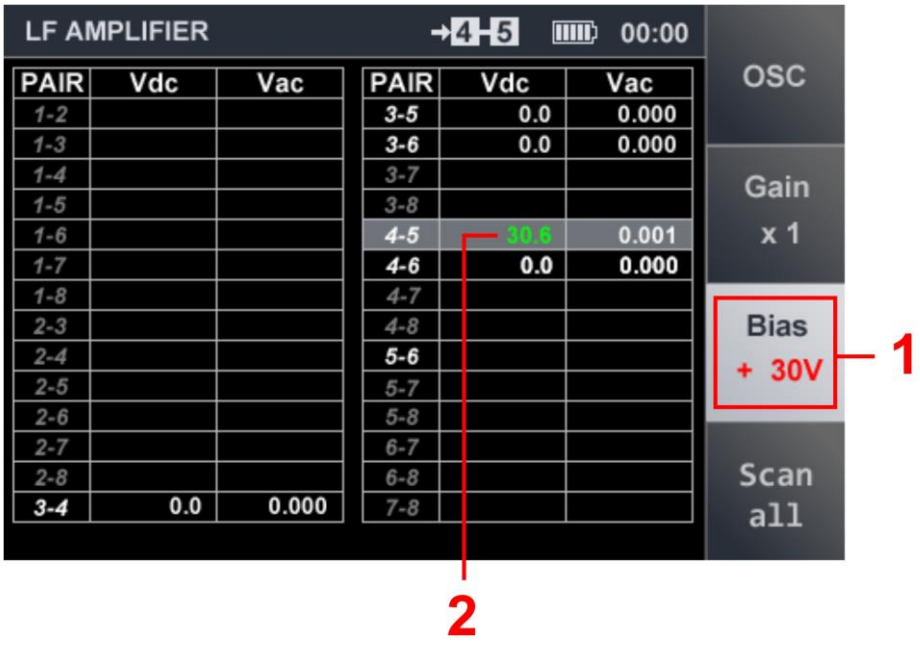



**Fig.44**

**Important!** While setting the bias voltage, other functions will be inaccessible.

The bias voltage, once set, will remain unchanged until deactivation of the "LOW FREQUENCY AMPLIFIER" channel (switching to the main menu of device).

If the voltage on the pair connected to the ST 500 is beyond ±3 V, the application of bias voltage to these wires is disabled.

The measured voltage value will in this case be marked red (fig.45, 3). When this pair is engaged (by selecting the corresponding table row) a red sign reading "OVER" will appear in the upper-center part of the screen (fig.45, 2) and the "F3" key field will look as shown in fig.45, 4.

If the voltage (Vdc) in the connected pair exceeds ± 50 V, the inscription ">50" appears in the corresponding cell.

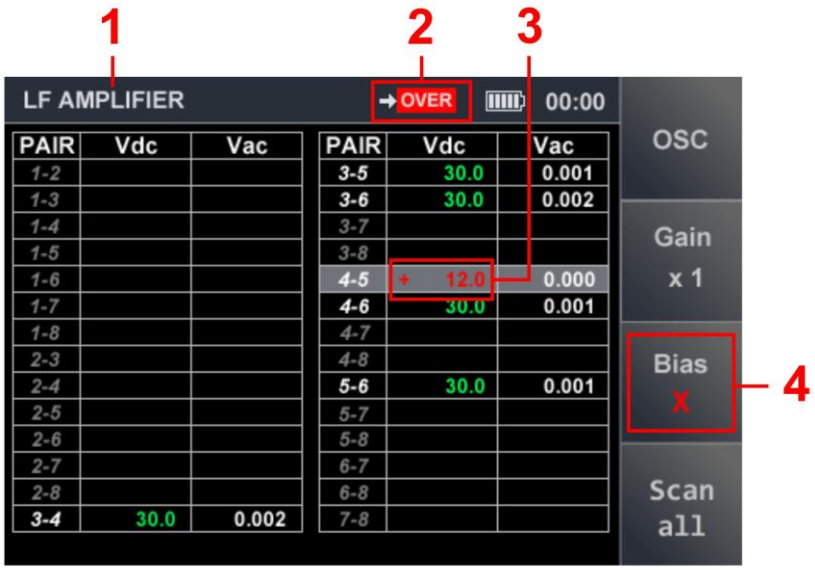



**Fig.45**

In this case, to apply a bias voltage, de-energize the cable.

### 7.5. AUTOMATED MODE

The AUTOMATED mode is intended for cycling through all possible paired combinations of wires in a multicore cable.

To activate this feature, press "F4" ("Scan all") (fig.40). The electronic switch will consecutively engage all the pairs of wires, staying for several seconds at each of them (each time the corresponding table row will become active).

The user can analyze the received signal by listening to the output sound.

If during scanning suspect signals have been detected, when the cycle is over they should be analyzed by means of "OSCILLOSCOPE" and "SPECTRUM ANALYZER".

### 7.6. OSCILLOSCOPE

The OSCILLOSCOPE is activated from "ELECTRONIC SWITCH CONTROL" mode or the AUTOMATED mode by pressing "F1".

Upon activation, the screen will look as shown in fig.46.

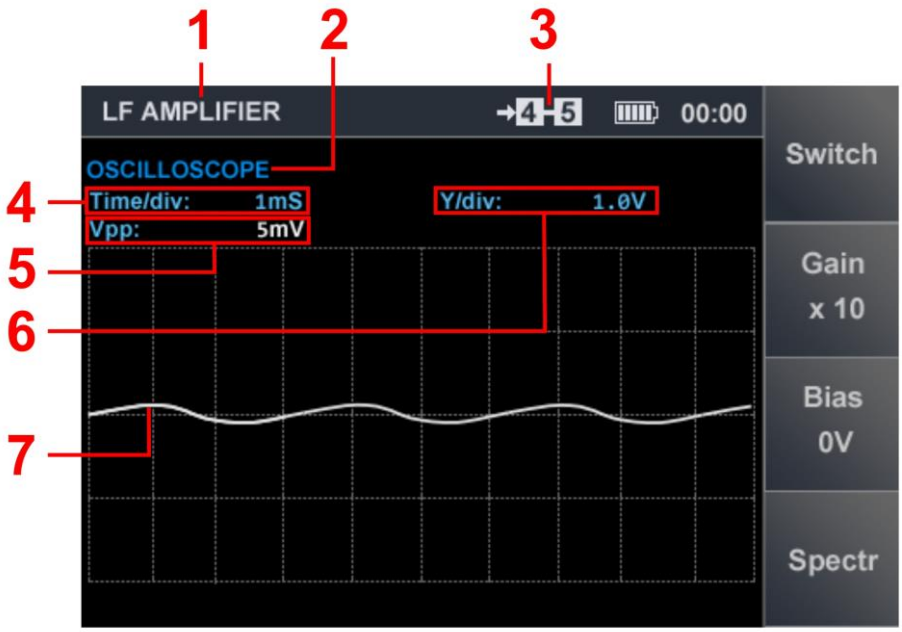



**Fig.46**

**In fig.46:**

1 - active channel
2 - data representation form
3 - connected pair of wires
4 - set division value of the time axis (mcs or ms)
5 - measured value of signal magnitude
6 - vertical zoom
7 - oscillogram

Upon activation of the OSCILLOSCOPE, the gain value and bias voltage, set in the "ELECTRONIC SWITCH CONTROL" mode, are retained. Both these parameters can be adjusted without exiting the OSCILLOSCOPE. The adjustment procedure is described in 7.3.1. and 7.3.2.

**Controls:**

| Key | Action |
|---|---|
| ▽ △ | vertical zoom of the OSCILLOSCOPE |
| ◁ ▷ | horizontal zoom of the OSCILLOSCOPE |
| **F1, ESC** | switching to "ELECTRONIC SWITCH CONTROL" mode |
| **F2** | activating/deactivating Gain Setting |
| **F3** | activating/deactivating Bias Voltage Setting |
| **F4** | activating "SPECTRUM ANALYZER" function |
| **MODE** | switching to the main menu of device |
| **FUNC, ENTER** | disabled |

### 7.7. SPECTRUM ANALYZER

The SPECTRUM ANALYZER is activated from the OSCILLOSCOPE by pressing "F4" ("Spectr"). The screen will look as shown in fig.47.

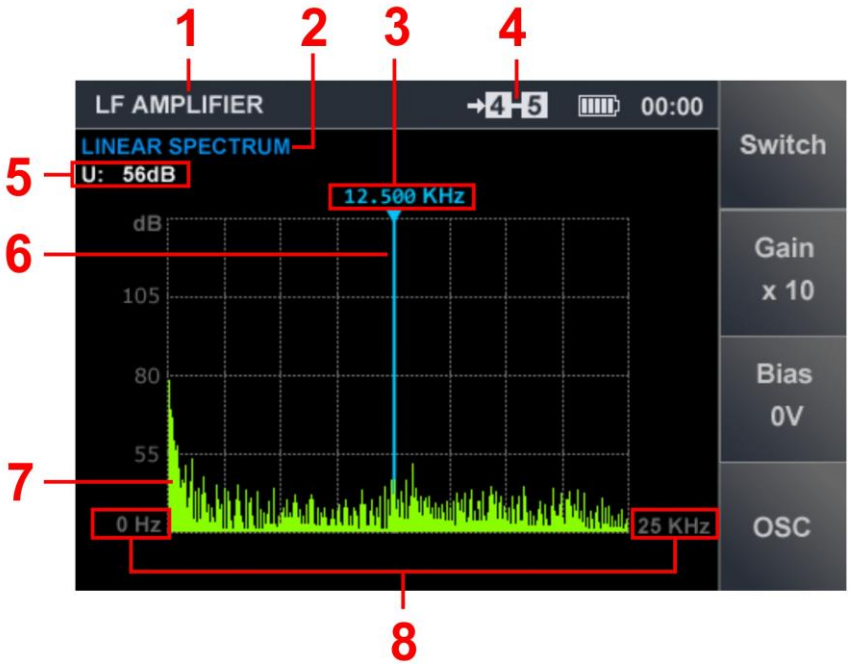



**Fig.47**

**In fig.47:**

1 - active channel
2 - data representation form
3 - frequency value at cursor position
4 - connected pair of wires

**SPECTRUM ANALYZER Controls**

| Key | Action |
|---|---|
| ◁▷ | cursor positioning |
| **F1, ESC** | switching to **"ELECTRONIC SWITCH CONTROL" mode** |
| **F2** | activating/deactivating **Gain Setting** |
| **F3** | activating/deactivating **Bias Voltage Setting** |
| **F4** | activating **OSCILLOSCOPE** |
| **MODE** | switching to the main menu of device |

# 8. SOFTWARE

## 8.1. PURPOSE

1. Preparation and loading into ST 500 of a priori information for analyzing the received signals using the "SELECTIVE HF DETECTOR" channel in AUTOMATED and "WIRELESS COMMUNICATION" modes:

- adjustment of "THREAT" and "NON-THREAT" frequency bands,
- customizing the parameters frequency bands used by digital communications devices,
- customizing the parameters of frequency bands used by base stations of mobile communications networks,
- making/editing user lists.

2. Updating the firmware of the main unit processor.

## 8.2. FUNCTIONALITY

**The user can do the following**

1. Adjust the factory settings, then download the data to the device and/or save them as a file on the HDD.
2. Download data from the ST 500 or from the HDD, make the necessary changes, then upload the corrected data to the device and/or save it as a file on the HDD.

Files on the HDD are saved in the "xxx.dat" format, ("xxxx" is the file name assigned by the user when saved).

Only one file can be downloaded to the device, an unlimited number of files can be saved to the HDD.

## 8.3. PC REQUIREMENTS

Operation System: Windows 7, 8, 10 (64 bit)
Free HDD space: at least 100 Mb

## 8.4. INSTALLATION

The distribution kit is located in the Prog_ST500 folder on the flash card supplied.
Installation Order:

1. Copy the Prog_ST500 folder to the PC.
2. Install the ST 500 driver on the PC (run the CDM21228_Setup.exe file).
3. Run the ST500.exe file.
4. Using the USB cable (fig.1, 5) connect the ST 500 main unit to the PC.
5. Turn on the main unit.

On the PC screen (on the status bar (fig.48, 7) should appear the inscription: "Подключено по USB" or "USB connected". The following message should appear on the screen of the ST 500: "USB connected". After that, the software is considered to be successfully installed on the PC.

## 8.5. GRAPHICAL INTERFACE

The PC screen with running ST 500 software is shown in fig.48.

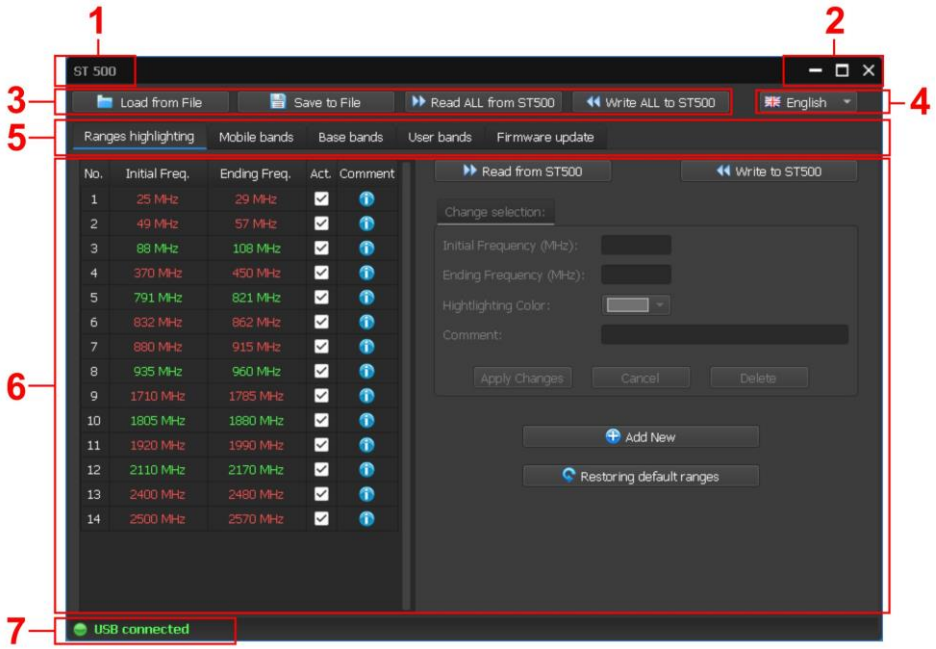



**Fig.48**

In fig.48:

1 - software name
2 - application window control (minimize, maximize, close)
3 - mode tabs
4 - language setting (русский/English)
5 - software mode tabs
6 - data field and controls in the active mode
7 - status bar (connecting ST 500 to PC)

**The status bar (fig.48, 7) can indicate one of the three states:**

1. **"USB Connected"**: the Main Unit is on and connected to the computer.
2. **"Request to connect to ST500..."**: the PC sends a request to connect the main unit (the driver is installed, the main unit is turned off and connected to the PC).
3. **"No response from ST500!"**: The response of the ST 500 to the PC request is not received (the main unit is not connected to the PC and/or turned off and/or the driver is not installed).

## 8.6. OPERATION MODES

1. "RANGES HIGHLIGHTING" mode
2. "MOBILE BANDS" mode
3. "BASE BANDS" mode
4. "USER BANDS" mode
5. "FIRMWARE UPDATE" mode

The inclusion of the mode is made by switching to the appropriate tab (fig.48, 5).

### 8.6.1. "RANGES HIGHLIGHTING" MODE

This mode is intended for defining the limits of bands in which the presence of "THREAT" or "NON-THREAT" signals is likely.

**"THREAT"** bands:

- operating frequency bands of digital mobile communications devices
- operating frequency bands of mobile cell phone base stations
- known frequency bands utilized by eavesdropping devices

**"NON-THREAT"** bands:

- operating frequency bands of base stations of mobile communications networks
- broadcasting bands of television and radio stations
- operating frequency bands of various radio devices in legitimate use on site

"THREAT" frequency bands are highlighted red, "NON-THREAT" bands are highlighted green.

Once information on "THREAT" and "NON-THREAT" bands is loaded into ST 500, signals listed in the AUTOMATED mode table of the SELECTIVE HF DETECTOR (3.6), will be highlighted accordingly. If a signal is detected in a "THREAT" band it is highlighted red, if in a "NON-THREAT BAND", green.

If a signal's frequency falls within neither of these bands, the signal is classified as "UNKNOWN" and highlighted white.

If search for eavesdropping devices is conducted on the site on a regular basis, it is advisable to save band assignments in data files.

The mode is activated by selecting the "RANGES HIGHLIGHTING" tab. The screen upon mode activation is shown in fig.49.

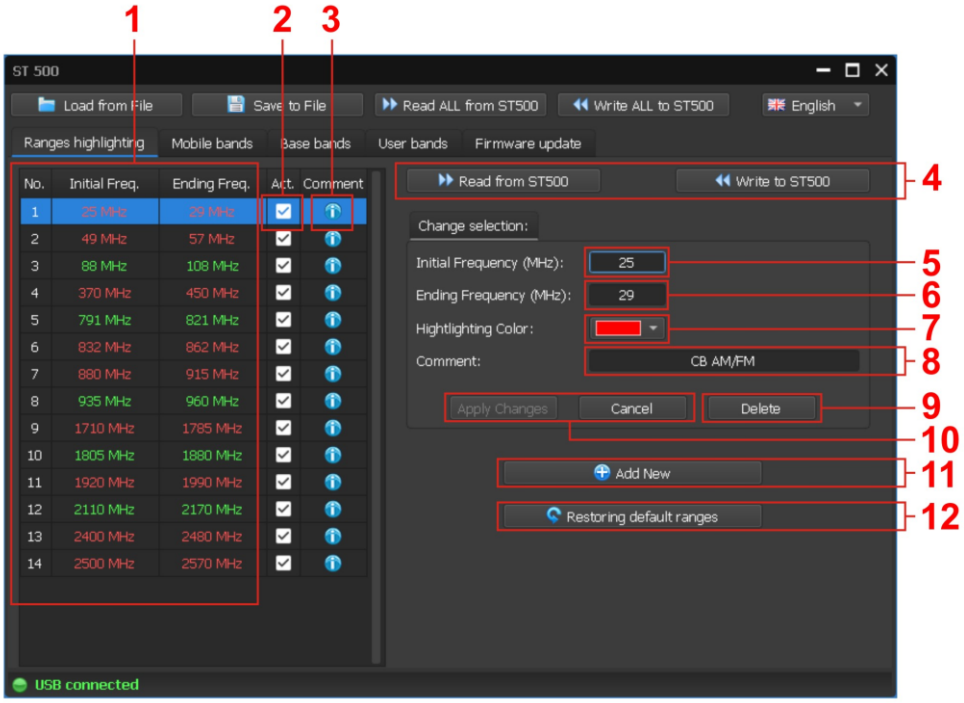



**Fig.49**

**In fig.49:**

1 - list of highlighted ranges: sequence number, initial (lower) and ending (upper). The line of the adjustable range is highlighted in blue
2 - activity checkbox. If not ticked: signals found in this range will be classified as "UNKNOWN"
3 - info button showing a user comment left while editing the range
4 - controls for data exchange with ST 500
5 - input field for initial (lower) frequency
6 - input field for ending (upper) frequency
7 - text color selection box (red or green)
8 - input field for comments (only numbers and Latin letters can be used)
9 - band deletion (the active line highlighted blue will be deleted)
10 - accepting/canceling changes made
11 - adding a new range
12 - return to factory settings of the "RANGES HIGHLIGHTING" mode

**USING THE "RANGES HIGHLIGHTING" MODE**

1. Go to "RANGES HIGHLIGHTING" tab.
2. Load data by one of the below methods:

- from the PC, by clicking "Load from File" and selecting the file; all the data including range customizations will be loaded
- from ST 500, by clicking "Read ALL from ST500"; all the data including range customizations will be loaded
- from ST 500, by clicking "Read from ST500"; only range customizations will be loaded
- from ST 500, by clicking "Restoring default ranges"; list of ranges set by the manufacturer will be loaded.

**Parameter adjustment**

1. To edit a band, select the corresponding table row, which will be highlighted blue
2. Edit the following parameters:
- initial (lower) and/or ending (upper) frequency band (fig.49, 5, 6)
- highlighting color (fig.49, 7)
- comment (fig.49, 8)
- on/off activity checkbox (fig.49, 2)

3. Click "Apply Changes" to save the adjustments, or "Cancel" to exit without saving changes.

**Adding a new band**

1. Click "Add New"
2. Input new band parameters:

- lower and upper frequency bounds (fig.49, 5,6)
- highlighting color (fig.49, 7)

- comment (fig.49, 8)
- on/off activity checkbox (fig.49, 2)

3. Click "Apply Changes" to save the changes made, or "Cancel" to exit without saving changes

**Restrictions for band editing or addition**

1. Frequency ranges cannot border on, or overlap with, one another. If this restriction is not met, the following warning prompt will appear,

***"Initial Frequency is in a different range # xx (xxx - xxx)"***
***"Ending Frequency is in a different range # xx (xxx - xxx)"***

2. The width of a range cannot exceed 200 MHz. If this restriction is not met, the following warning prompt will appear,

***"The range should be no more than 200 MHz!"***

**Deleting a band**

To delete a band, select the corresponding table row and click "Delete". Upon confirmation the line will be deleted from the list.

**Finishing**

Before completing the work, save the changes in any of the following methods:

- download to the PC HDD by clicking the "Save to File" and specifying the path for saving and the file name (information about the selected ranges and information from other modes will be saved);
- download to the ST 500 only information on the made adjustments of the selected ranges by clicking "Write to ST500";
- download to the ST 500 information about all the lists (in all modes) by clicking "Write ALL to ST500".

### 8.6.2. "MOBILE BANDS" MODE

This mode is intended for creating and editing a list of frequency bands utilized by mobile communication systems in the region.

This information, downloaded to ST 500, is used by the SELECTIVE HF DETECTOR channel, "WIRELESS COMMUNICATION" mode, "MOBILE DEVICES MONITORING" function (3.4.1).

The mode is activated by selecting the "Mobile bands" tab. The device screen will look as shown in fig.50.

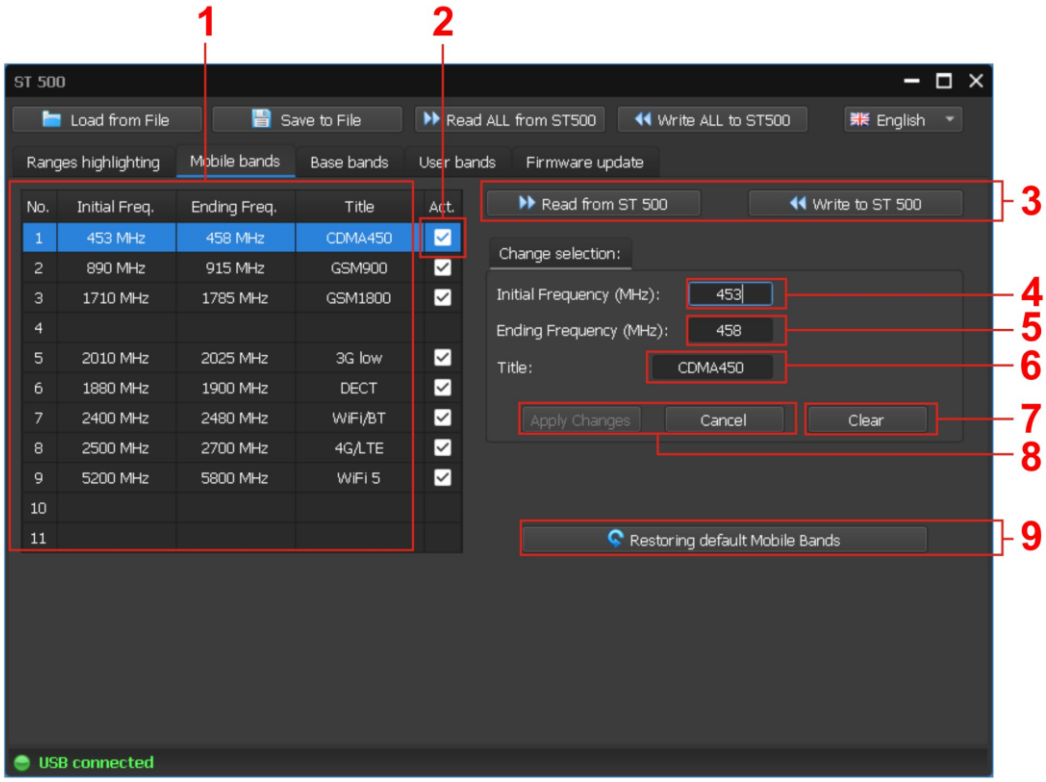



**Fig.50**

**In fig.50:**

1 - list of frequency bands of mobile devices: sequence number, initial (lower) and ending (upper) frequencies, range designation. The line of the adjustable range is highlighted in blue
2 - activity checkbox. If not ticked: no search for signals in this range
3 - control of data exchange with ST 500 (reads and writes data relating only to the "Mobile bands" mode)
4 - input field for initial (lower) frequency
5 - input field for ending (upper) frequency
6 - input field for range designation (only numbers and Latin letters can be used)
7 - band deletion
8 - accepting or canceling changes made
9 - download factory settings (list of mobile communication device ranges used in Russia)

**USING THE MODE "MOBILE BANDS"**

1. Go to tab "Mobile bands". The PC screen will look as shown in fig.50
2. Download data in any of the following ways:

- from the PC, by clicking "Load from File" and selecting the file; all the data including range customizations will be loaded
- from ST 500, by clicking "Read ALL from ST500"; all the data including range customizations will be loaded
- from ST 500, by clicking "Read from ST500"; only band customizations will be loaded
- from ST 500, by pressing "Restoring default Mobile Bands"; manufacturer-defined presets will be loaded, with mobile communication bands specific to Russia

**Changing parameters**

1. To edit a band in the list, select the corresponding table row, which will be highlighted blue.
2. Edit parameters:

- initial (lower) and/or ending (upper)band frequency (fig.50, 4,5)
- name or comment on the band (fig.50, 6)
- tick highlighting on/off (fig.50, 2)

3. Press "Apply Changes" to save the changes, or "Cancel" to exit without saving changes.

**Adding a new band**

1. Set the cursor to the "empty" line.
2. Input band parameters:

- initial (lower) and ending (upper) band frequency (fig.50, 4,5)
- name or comment on the band (fig.50, 6)
- tick highlighting on/off (fig.50, 2)

3. Click "Apply Changes" to save the changes, or "Cancel" to exit without saving changes.

**Restrictions for band editing or addition:**

1. The maximum number of bands (list rows) is 11.
2. The band should not exceed 600 MHz. If this condition is violated, a warning appear on the screen:

***"The band should be no more than 600 MHz!"***

3. The value of the initial frequency must be less than the ending frequency. If this condition is violated, a warning appear on the screen:

***"Initial Frequency > Ending Frequency!"***

**Deleting a band**

To delete a band, place the cursor on the corresponding line and click "Clear" and then confirm the action.

**Finishing**

Save changes by one of the below methods:

- download to PC's HDD by clicking the "Save to File" and specifying the path to save and the name of the file (the list of mobile devices and information from other modes will be saved)
- download only the information about the made adjustments of the ranges of mobile devices in the memory of the ST 500 by clicking the "Write to ST500"
- download information about all lists (in all modes) into the memory of the ST 500 by clicking the "Write ALL to ST500"

### 8.6.3. "BASE BANDS" MODE

This mode is intended for creating and editing a list of frequency bands utilized by mobile communication systems in the region.

These data loaded to ST 500 memory, are used by the SELECTIVE HF DETECTOR channel, "WIRELESS COMMUNICATION" mode, "BASE STATIONS MONITORING" function (3.4.2). To activate the mode, select the "Base bands" tab.

The order of loading, updating, saving data and limiting is similar to the procedures described in 8.6.2.

### 8.6.4. "USER BANDS" MODE

This mode is intended for creating and editing a list of frequency bands that are of a specific interest to the user. These data loaded to ST 500 memory, are used by the SELECTIVE HF DETECTOR channel, "WIRELESS COMMUNICATION" mode, "USER LIST" function (3.4.3). To activate the mode, select the "User bands" tab.

The order of loading, updating, saving data and limiting is similar to the procedures described in 8.6.2.

### 8.6.5. "FIRMWARE UPDATE" MODE

The current firmware version is shown on the screen when the device is turned on (fig.51).


**Fig.51**

Get information and download the latest version of the firmware can be on the ST Group Ltd official site: http://spymarket.com/tp

When "Firmware update" is on, the screen looks as shown in fig. 52 below.

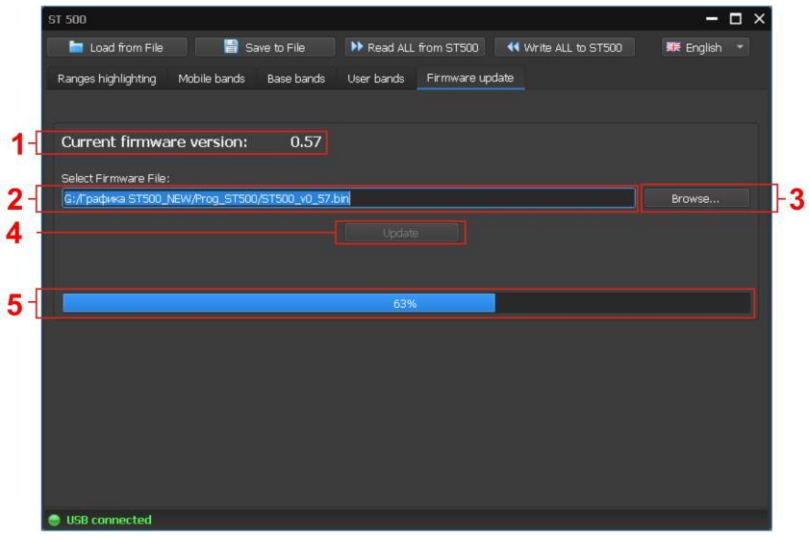



**Fig.52**

**In fig. 52:**

1 – current firmware version
2 – path to the latest firmware file
3 – browsing button
4 – update start button
5 – update progress bar

**To update the firmware**

1. Download to PC from ST Group Ltd official site http://spymarket.com/tp file **ST500_vx_xx.bin** ('x_xx' is version number)
2. Start ST 500 software.
3. Connect ST 500 to PC.
4. Select tab "Firmware update".
5. Click "Browse".
6. In the opened window select the path to the file with latest firmware version and click "Open". The file name and path will be shown on screen (fig.52, 2).
7. Click "Update". The progress will be shown on screen (fig.52, 5). Upon completion you will be prompted, "Update done!".
8. Click "OK".
9. The new firmware version will be shown in the corresponding field (fig.52, 1).

# 9. USE GUIDELINES

## 9.1. GUIDELINES FOR USE OF "SELECTIVE HF DETECTOR" CHANNEL

The "SELECTIVE HF DETECTOR" channel is intended for detection, identification and localization of radio transmitting, "active" eavesdropping devices in the range of 20 - 6000 MHz.

**Three option of searching for eavesdropping devices:**

- AUTOMATED mode
- manual modes ("PANORAMA" or DIFFERENTIAL mode)
- search in previously known frequency ranges (in the "WIRELESS COMMUNICATION" mode).

**Three stages in the search for eavesdropping devices:**

stage #1 - detection of the signal
stage #2 - identification of the detected signal ("threat"/"non-threat")
stage #3 - localization of the source of a dangerous signal

The presented search algorithms are typical and can be adjusted depending on the features of the object being checked and the tasks set.

### 9.1.1. SEARCH IN THE AUTOMATED MODE

The AUTOMATED mode is used at small loading of a frequency range in the area of search

**SEARCH ALGORITHM:**

1. In the checked room:
    - activate the test sound source and adjust the sound volume
    - connect the antenna and headphones to the main unit of ST 500
    - turn on ST 500
2. Turn on "SELECTIVE HF DETECTOR".
3. Depending on the activity in the frequency range, set the optimal gain, making sure that no off-scale occurs.
4. Turn on the AUTOMATED mode.
5. Sort the table by signal level in ascending order.
6. Select the first table row as current.
7. Analyze the demodulated signal as follows:
    - listen to the signal in headphones at different passband (1 and 20 MHz)
    - analyze the signal with the oscilloscope
    - fine tune the frequency if necessary

**Signs of "THREAT" signal:**

- at the frequency of the detected signal, the test sound is heard through the headphones,
- the test sound is not heard in the headphones, but the oscilloscope picture of the demodulated signal changes with the test sound,
- the detected signal is marked red in the table, which means that a mobile digital device is nearby, or the signal is within the band utilized by radio-transmitting eavesdropping devices,
- there is a radical decrease in the level of the detected signal when ST 500 is brought outside the checked room.

8. Analyze all the other signals in a similar way.

### 9.1.2. SEARCH IN THE "PANORAMA" MODE AND DIFFERENTIAL MODE

The "PANORAMA" and DIFFERENTIAL mode are used to search for eavesdropping devices under heavy radio traffic conditions on site.

1. Turn on the test sound source and adjust the sound volume in the checked room.
2. Outside the checked room:

   - connect the antenna and headphones to the main unit of ST 500 and turn it on
   - put on the headphones

3. Turn on SELECTIVE HF DETECTOR channel ("PANORAMA" Mode).
4. Depending on the activity in the frequency range, set the optimal gain, making sure that no off-scale occurs.
5. Activate the DIFFERENTIAL mode, obtaining a differential view.
6. Enter the room while monitoring the differential view; note any new signals that may appear, or increasing levels of the ones already detected.
7. If new signals have appeared, select the table row with the strongest one.
8. Activate "FIXED FREQUENCY ANALYSIS" function.
9. Analyze the detected signal as follows:

- listen to the signal in headphones at different passband (1 or 20 MHz)
- analyze the signal with the oscilloscope
- if needed, use frequency fine tuning

**Signs of "THREAT" signal:**

- at the frequency of the detected signal, the test sound is heard through the headphones
- the test sound is not heard in the headphones, but the oscilloscope picture of the demodulated signal changes with the test sound
- there is a radical decrease in the level of the detected signal when ST 500 is brought outside the room.

10. Analyze all the other signals in a similar way.

### 9.1.3. SEARCH IN THE "WIRELESS COMMUNICATION" MODE

In the "WIRELESS COMMUNICATION" mode, the frequency bands that meet a specific digital communication standard and are used by eavesdropping devices are monitored. When searching for eavesdropping devices, three functions are used:

1. "Mobile devices monitoring" (3.4.1)
2. "Base stations monitoring" (3.4.2)
3. "User list" (3.4.3)

**Factory settings of the "WIRELESS COMMUNICATION" mode:**

| **MOBILE DEVICES** | **Frequency range, MHz** | |
|---|---|---|
| CDMA450 | 453 | 458 |
| GSM900 | 899.5 | 915 |
| GSM1800 | 1710 | 1785 |
| 3G | 1920 | 1980 |
| 3G low | 2010 | 2025 |
| DECT | 1880 | 1900 |
| WiFi/BT | 2400 | 2480 |
| 4G/LTE | 2500 | 2700 |
| WiFi 5 | 5200 | 5800 |
| **BASE STATIONS** | **Frequency range, MHz** | |
| CDMA450 | 463 | 468 |
| GSM900 | 935 | 960 |
| GSM1800 | 1805 | 1880 |
| 3G | 2110 | 2170 |
| 3G low | 2010 | 2025 |
| DECT | 1880 | 1900 |
| **USER LIST** | **Frequency range, MHz** | |
| ---- | 88 | 108 |
| ---- | 430 | 450 |

Using the ST 500 software, bands can be added to, or removed from the user list, as well as the lists of mobile device and base station frequencies, and band parameters can adjusted.

The search procedure is the same for all functions of the "WIRELESS COMMUNICATION" mode:

1. In the checked room:

- connect the antenna and headphones to the main unit of ST 500
- turn on the test sound source and adjust the sound volume (only when using "USER LIST")
- turn on ST 500

2. Activate "SELECTIVE HF DETECTOR" channel.
3. Depending on the activity in the frequency range, set the optimal gain, making sure that no off-scale occurs.
4. Turn on "WIRELESS COMMUNICATION" mode
5. Activate one of the functions ("Base stations monitoring", "Mobile devices monitoring", "User lists").

6. Monitor signal presence, watching the level bars in the table.
7. If radio traffic is detected in any band, it is necessary to investigate the observed signals. To do this, set the cursor to the desired band and activate the "ANALYSIS OF DETECTED SIGNALS" function.

**Signs of "THREAT" signal while analyzing frequency bands used by digital mobile communications devices ("MOBILE DEVICES MONITORING" function):**

- high levels of a detected digital signal (in the absence of legitimate mobile communications devices nearby)
- time-frequency structure of the signal different from the standard pattern (while analyzing with the oscilloscope)
- an analog signal detected, that correlates with the test sound

**Signs of "THREAT" signal while analyzing the ranges of mobile telecoms base stations ("BASE STATIONS MONITORING" function):**

- time-frequency structure of the signal different from the standard pattern (while analyzing with the oscilloscope)
- an analog signal detected, that correlates with the test sound

**Signs of "THREAT" signal while analyzing the user list ("USER LIST" function):**

- at the frequency of the detected signal, the test sound is heard through the headphones
- the test sound is not heard in the headphones, but the oscilloscope picture of the demodulated signal changes with the test sound
- there is a radical decrease in the level of the detected signal when ST 500 is brought outside the room

### 9.1.4. LOCALIZATION OF THE SOURCE OF DETECTED SIGNAL

If the eavesdropping device uses an open transmission channel, an **acoustic** or **energetic** method is used for localization. Localization of the source of the encoded signal is produced only by the **energy method.**

When using the **acoustic method**, the operator turns on the test sound source, moves it around the room (listening to the demodulated signal in the headphones) and searches for the place in the room where the signal is heard best.

For more accurate localization, it is recommended to knock lightly on interior items located near this place. A knock will be heard quite well in the headphones.

**Energy method** is to determine the place in the room where the signal level will be maximum. The analysis is performed using indicators that are implemented in various modes of the SELECTIVE HF DETECTOR:

- "PANORAMA" or DIFFERENTIAL mode, "FIXED FREQUENCY ANALYSIS" function (fig.12, 2)
- "AUTOMATED" mode table (fig.14, 4)
- "WIRELESS COMMUNICATION" mode, "ANALYZING DETECTED SIGNALS" function (fig.19, 13)

Having determined the place in the room where the signal level is maximum, it is necessary to use the "SET "0" function (3.2.2). This will allow to more accurately determine the location of the eavesdropping device.

When localizing a GSM signal source in an energetic way, difficulties may arise. The signal level in different places of the room will be approximately the same, and it is difficult to determine where the signal level is at its maximum.

Setting the minimum gain value will also not solve this problem. Localization is recommended with the antenna turned off. In most cases, this will allow to determine the installation location of the GSM device.

### 9.2. GUIDELINES FOR USE OF "IR DETECTOR" CHANNEL

The IR DETECTOR channel is intended for the detection and location of eavesdropping devices that send transmissions within the infrared range to a special IR receiver.

The operation range of such a system may be hundreds of meters, provided there is an **unobstructed line of view** between the IR transmitter and IR receiver. As a rule, the receiver will be outside the inspected room, with the IR transmitter inside and directly opposite a window.

Search for the eavesdropping device should begin from the window, while directing the IR-sensor (fig.2, 5) at the suspected location of the IR receiver.

**Search algorithm:**

1. Turn on the test sound source in the checked room.
2. Turn on ST 500 and activate IR DETECTOR.
3. Direct the IR sensor at the suspected location of the IR receiver.

**Important! The detection range of the IR detector is 50-70 cm.**

4. Observe the changes in the signal level on the indicator (fig.20, 2), the waveform shape (fig.20, 4) and the sound volume in the headphones.

An increase in the signal level should indicate that an active IR source is within the field of view of the IR sensor ($\pm 20^0$).

**Signs of "THREAT" signal:**

- High signal levels, test sound heard in the headphones
- High signal levels, test sound not heard in the headphones, oscilloscope picture typical for a digital signal

The signal is localized using the received signal level indicator (fig.20, 2). The IR signal source is set at the point where the signal level is at its maximum.

For more precision, use the DIFFERENTIAL mode.

#### 9.2.1. SELECTION OF "FALSE" SIGNALS

When approaching a radio signal source (WiFi router, DECT base, etc.), the received signal level may increase due to pickups on the instrument's input circuits. To select "false" and IR signals, close the IR sensor with your hand (fig.2, 5). A significant decrease of the signal level on the indicator (fig.20, 2) indicates that a signal in the IR range. When receiving a "false" signal, the level on the indicator does not change.

### 9.3. GUIDELINES FOR USE OF THE "WIRED RECEIVER" CHANNEL

The WIRED RECEIVER channel is intended for the detection of wired high-frequency transmitters in electric mains and low current circuits.

The range of information transmission via electric mains, as a rule, does not exceed 500 meters within one or several buildings, which are powered from one low-voltage bus of a transformer substation. When using telephone lines and LAN cables, the transmission distance may exceed 500 meters.

**Method of connection to the circuit:** parallel.
**Power Supply:** from the circuit, or from an autonomous source.
**Search objects:**

- Power mains lines
- Telephone lines
- LAN cabling
- Other low current lines, including those out of operation (with no end user devices connected) and/or illegitimately laid cabling

**Auxiliary equipment:**

- Adapter for connecting the main unit to electric mains (fig.1, 2)
- Test sound source

To search for HF signals in electric mains and low current circuits, the "PANORAMA" (DIFFERENTIAL) and the AUTOMATED modes are used.

For the analysis of the detected signal, the "FIXED FREQUENCY ANALYSIS" function and OSCILLOSCOPE are used.

#### 9.3.1. ELECTRIC MAINS TESTING

**The initial state.**

The electric mains is powered and it is possible to de-energize it. This line only supplies the checked room. It is suspected that high-frequency transmitters may be planted on the mains cabling or user devices connected to it, transferring data through the cabling outside the room.

**Search algorithm:**

1. De-energize the circuit.
2. Make sure there is no voltage on the electric mains branch in the room.
3. Disconnect all consumer devices from the mains (plug them out of the sockets).
4. Connect the electric mains adapter to the main unit, and to one of the electric sockets on the circuit.
5. Turn on ST 500 activate the "WIRED RECEIVER" channel.
6. Set "MAINS" in the circuit type selection menu.
7. Select the frequency range to scan (100 kHz – 60 MHz or 100 kHz – 180 MHz); all activity within the range will be shown, with the mains branch de-energized.
8. Turn on the attenuator ("F4").

When an electric mains circuit is being tested, the electronic switch automatically engages the pair of wires "1-2", which corresponds to the wiring scheme of the adaptor's plug. In the status bar the symbol  (electric mains mode) is shown.

On the screen, reception within the selected frequency band on deenergized line will be shown. With power cut off, no eavesdropping devices powered from the circuit will be working, so all the signals received at this time can be considered "non-threat" (interference, broadcast signals, *etc.*)

To exclude all those from the search, the DIFFERENTIAL mode should be used.

9. Turn on "DIFFERENTIAL MODE" ("F3").

A differential spectrum showing activity in the frequency band will appear on the screen. The levels of all previously received signals will be set as "0", and from this point on only new signals will be displayed.

10. Turn on the power switch on the electric switchboard.

If a high-frequency transmitter is connected to the circuit, it will be activated now that the power supply is back on, and signals from eavesdropping devices will be registered.

When new signals appear in the differential spectrum, turn on the AUTOMATED mode ("F2" - "Search"). A table listing the detected signals will appear, with the first table row selected (lowest signal frequency). It is recommended to sort the table by level.

11. Turn on the test sound source and adjust the sound volume.
12. Connect headphones ("PHONE" socket) and adjust the sound volume.
13. Analyze the demodulated signal alternating "AM"/"FM" ("F2").
14. If necessary, fine-tune the signal frequency.
15. If necessary, analyze the demodulated signal on the oscilloscope ("F3"); to return to the AUTOMATED mode table, press again "F3".
16. Select the next table row.
17. Repeat the research procedure, changing between AM/FM ("F2").
18. Test all the detected signals in a similar way.

The absence of new signals in differential spectrum upon turning power back on means that there are no active eavesdropping devices connected to the circuit. However, it should be noted that there may be malfunctioning or remotely controlled devices that are currently turned off or on standby. Such devices can be detected with instruments employing "active" search methods (nonlinear junction detectors and reflectometers).

**Variants of possible changes in the differential spectrum when the power supply is turned on and the reasons for its occurrence:**

- New signals were detected, in the analysis of which it was possible to hear the reference sound. This means that an analog HF transmitter installed in the room is operating in the tested line.
- New signals were detected, the analysis of which failed to hear the reference sound. The line may have a digital (or coded) HF transmitter.
- A significant increase in background levels is observed in the frequency range 10–100 MHz. This may be caused by the operation of a PLC modem.

If "THREAT" signals were not detected, check the changes in the differential spectrum when the consumers are connected.

It is required to receive a differential panorama of the powered line, and then in turn connect consumers. Thus, it is possible to establish which consumer is the source of the "THREAT" signal.

19. Exit the AUTOMATED mode ("ESC"); the current differential spectrum on the powered circuit with no consumer connections will be shown.
20. Exit the DIFFERENTIAL mode ("F3"); the current differential spectrum on the powered circuit with no consumer connections will be shown.
21. Turn on the DIFFERENTIAL mode ("F3"); the differential spectrum on the powered circuit will be shown, with all the previously detected signals set as "0".
22. Connect one of the consumer devices to the circuit. If new signals are detected in the "PANORAMA" mode, turn on the AUTOMATED mode ("F2") and analyze each of them as described earlier in this manual.

Upon analyzing all the signals, exit the AUTOMATED mode ("ESC"), turn off DIFFERENTIAL mode ("F3") and then turn it back on to obtain a new differential spectrum.

Connect the next consumer device to the circuit and analyze the new signals, following the above procedure.

The analysis is complete when the circuit has been tested with all the consumer devices connected consecutively. The consumer devices whose connection lead to the appearance of "THREAT" signals in the differential spectrum, must be dissembled and checked for non-standard components.

### 9.3.2. LOW CURRENT CIRCUIT TESTING

In contrast to power two-core cabling, low current cabling is, as a rule, multi-core, and the operator must test all the possible paired combinations of wires.

A testing procedure for an office PBX line is described below.

**The initial state:**

Office PBX is connected to the telephone line. The telephone is connected to the line through a telephone socket (the telephone receiver is "hung up"). The telephone line is powered from the PBX and is operating normally.

The HF transmitter can be connected to a telephone line laid in the room, or installed in the telephone.

**Analog telephone line search algorithm:**

1. Connect ST 500 to the telephone line (fig.25 and fig.26).
2. Turn on the test sound source and adjust the sound volume.
3. Connect headphones to the main unit.
4. Turn on ST 500 and activate "WIRED RECEIVER" channel.
5. Select circuit type ("Low Voltage").
6. Select one of the frequency bands.
7. The table of combinations of pairs will be display on the screen.
8. Press "FUNC" (turn on "ELECTRONIC SWITCH SETTINGS" mode).
9. Press "F3" (turn on 6P4C connecting); the connection scheme is shown in Supplement #2

When a four-wire telephone line cable is connected, the switch contacts with numbers 3, 4, 5, 6 will be used. Wire combinations 3-4, 3-5, 3-6, 4-5, 4-6, 5-6 should be checked.

It is necessary to take into account that the transmitter can be powered normally (from the involved "4-5" pair), and transmit information through another pair.

10. In the table set the cursor on the line corresponding to the pair "3-4". The cell displays the voltage value in the connected pair. During normal operation of the telephone line, there is no voltage on this pair.
11. Press "ENTER". Activity in the frequency band on the pair "3-4" will be shown.
12. If necessary, turn on the attenuator ("F4").
13. Activate the AUTOMATED mode ("F2").
14. Listen to all detected signals by switching AM/FM demodulation ("F2").
15. Exit the AUTOMATED mode ("ESC") to the "PANORAMA" mode.
16. Activate the "ELECTRONIC SWITCH CONTROL" mode ("F1").
17. Set the table cursor to the next pair of wires, press "ENTER".
18. Test all the remaining paired combinations, as described above in 10-16.

Listening to test sound source means that there is a working analog wired HF transmitter connected to the telephone line in the room.

In this case, staying on the combination in which the "threat" signal was detected should disconnect the telephone set from the line. If this signal disappears, then its source is in the telephone.

If the signal is not lost when the telephone is disconnected, then its source is connected to the telephone line.

### 9.4. GUIDELINES FOR USE OF THE "LOW FREQUENCY AMPLIFIER" CHANNEL

The **LOW FREQUENCY AMPLIFIER** channel is intended for the detection of transmission channels utilized by dynamic and electret wired microphones, transmitting within the speech frequency band over low current lines.

**Dynamic microphones** are the most common type of microphones that do not require power supply and do not utilize a pre-amplifier. The transmissions are made over two wires (which can be cores in a multi-core cable). The transmission range can be hundreds of meters.

**Electret microphones** are a variety of capacitor microphones that are also quite common in eavesdropping equipment due to their low cost and ability to operate in rugged conditions.

Their design requires a pre-amplifier, for whose operation DC voltage of certain polarity is needed. This can be achieved by creating "phantom" power supply on the microphone, by simultaneous transmission of information signals over the feeding wires. Also, some electret microphones are equipped with independent power supply source.

**Method of connecting to the circuit:** parallel
**Power Supply:** 3 ÷ 20 V
**Tested circuits:**

- Telephone lines
- LAN cabling
- Other low current lines, including those out of operation (with no end user devices connected) and/or illegitimately laid cabling

**Auxiliary equipment:** test sound source

### 9.4.1. SEARCH FOR ACTIVE MICROPHONES IN AN ANALOG TELEPHONE LINE

**The initial state:**

1. The tested telephone line consists of 4 wires.
2. The cable is equipped with a 6P4C plug.
3. The consumer device is an analog telephone.
4. The two central connector pins are used by the telephone.
5. PBX' operation voltage is 26 V.
6. The line operates normally, with the telephone connected to it.

**Search algorithm:**

1. Connect ST 500 to the telephone line according to the scheme 3B (fig.25) or 3D,3E (fig.26).
2. Turn on the test sound source.
3. Turn on the ST 500, activate "LOW FREQUENCY AMPLIFIER" channel.
4. Press "FUNC" (turn on "ELECTRONIC SWITCH SETTINGS" mode).
5. Press "F3" to select 6P4C connection, The scheme is shown in Supplement #2.
6. Press "FUNC" (turn off "ELECTRONIC SWITCH SETTINGS" mode).
7. Press "F2" and set maximum gain (x100).
8. Connect the headphones to the main unit and adjust the sound volume.
9. Press "F4" (turn on the AUTOMATED mode).

The device will start iterating through all possible combinations of wire pairs. The tabular cursor moves through the table, stopping for a few seconds on the tested combination of wire pairs. At this time, the operator can listen to the received signal. After going through all the possible combinations, the scan will stop.

**Possible testing results and their interpretation:**

**Case 1**

| | | |
|---|---|---|
| Pair 3-6 | There is no voltage. The test sound cannot be heard in the audio output. | No dynamic microphone is detected. An electret microphone may still be connected, that had no power supply at the time of testing. A bias voltage check (9.4.2) is required. |
| Pair 4-5 | The voltage is DC 26 V.<br>The test sound cannot be heard in the audio output. | |

**Case 2**

| | | |
|---|---|---|
| Pair 3-6 | There is no voltage. The test sound can be heard in the audio output. | Either a dynamic microphone, or an electret microphone with independent power supply (possibly, from the telephone line) is connected. The microphone must be located. |
| Pair 4-5 | The voltage DC 26 V. The test sound cannot be heard in the audio output. | |

**Case 3**

| | | |
|---|---|---|
| Pair 3-6 | The voltage is DC 3-20 V. The test sound can be heard in the audio output. | An electret microphone is connected, with "phantom" power supply through wires #3 and #6. The microphone must be located. |
| Pair 4-5 | The voltage DC 26 V. The test sound cannot be heard in the audio output. | |

**Case 4**

| | | |
|---|---|---|
| Pair 3-6 | There is no voltage. The test sound cannot be heard in the audio output. | An electret microphone is connected, with "phantom" power supply from the telephone line and signal transmission over wires #4 and #5. The microphone must be located. |
| Pair 4-5 | The voltage DC 26 V. The test sound can be heard in the audio output. | |

Microphone localization algorithm is described in 9.5.

### 9.4.2. ACTIVATION OF ELECTRET MICROPHONES IN AN ANALOG TELEPHONE LINE

In order to detect an electret microphone having no power supply, bias voltage must be applied to the circuit.

**The initial state -** the connection scheme, circuit type, and pin numbers are the same as described in 9.4.1.

**Search algorithm:**

1. Disconnect the circuit(branch) from the PBX.
2. Turn on the test sound source in the room.
3. Set the gain at 0 dB.
4. Set the bias voltage +30 V.
5. Activate the AUTOMATED mode ("F4").

The device will start going through all the possible paired combinations, pausing at each table line while the corresponding pair of cores is being tested; in the meantime, the operator can listen to the received signal.

If the sound from the test sound source can be heard in the headphones, it means an electret microphone is detected, and it will be necessary to locate it.

After all the combinations have been tested, scanning will stop.

If the test sound has not been heard in the headphones, search should be repeated in the AUTOMATED mode, with reversed bias voltage (-30 V).

**Recommendations:**

- If the test sound can be heard during testing, it is probable that the microphone is planted in the telephone set. To make sure, disconnect the telephone; if the test sound can no longer be heard, the eavesdropping device is in the telephone.
- Any detected signals that have no relation to the test sound should be analyzed with oscilloscope or spectrum analyzer.

## 9.5. LOCALIZATION OF THE SIGNAL SOURCE DETECTED BY THE "WIRED RECEIVER" OR "LOW FREQUENCY AMPLIFIER" CHANNEL

### 9.5.1. ACOUSTIC METHOD

The acoustic localization method is applied only when an **"open transmission channel"** of the eavesdropping device is detected. To implement the method, two operators are required. One of them moves the test sound source around the room, the other operator controls the level of the received signal using the ST 500.

**Actions with the test sound source:**

1. Turn on the test sound source.
2. Decrease the sound volume.
3. Carry the test sound source slowly around the room.

**ST 500 operator procedure:**

1. Activate "LFA" or "WR" (in whichever the transmission channel has been detected).
2. Connect the headphones, and listen to the sound background in the room.
2. Select the wire pair at which the test sound is audible
3. Find the spot where the test sound is the loudest

### 9.5.2. LOCALIZATION WITH ST 500 AND NONLINEAR JUNCTION DETECTOR (NLJD)

This method can only be used to locate **devices that incorporate electronic parts.** The procedure requires two people, one going the length of the cabling while pointing the active non-linear junction detector's antenna at it, and the other monitoring with ST 500 any response to the NLJD's irradiation from the cable.

Any electronics that are close to the cabling but not connected to it, in the proximity of the antenna will yield responses on the $2^{nd}$ and $3^{rd}$ harmonics; this will be registered by the non-linear locator operator, but not the operator of ST 500.

However, if the operator of ST 500 hears a typical signal from the NLJD through the headphones, this will mean that the NLJD's antenna is being pointed at an eavesdropping device directly connected to the circuit.

This method is most effective when using NLJD ST 400 "CAYMAN" or ST 401 "CAYMAN" in the "SEARCH" mode.

**NonLJD operator procedure:**

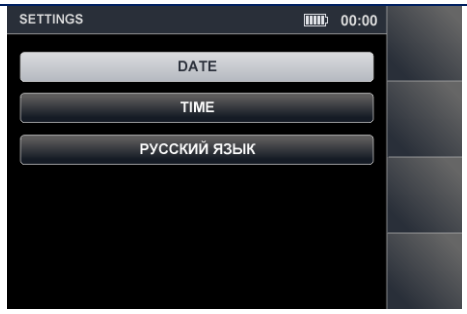
1. Disconnect all consumer devices from the cabling.
2. Turn on "CAYMAN" NLJD and set it to "SEARCH".
3. Connect the headphones or minimize the volume of the built-in speaker.
4. Move along the cable while pointing the NLJD's antenna at it.

**ST 500 operator procedure:**

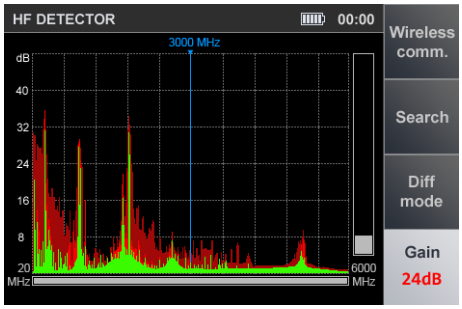
1. Connect ST 500 to the circuit.
2. Turn on ST 500.
3. Activate the channel ("LFA" or "WR") in which the suspect signal was detected.
4. In the table, select the wire pair at which the suspect signal was detected.
5. Connect the headphones.
6. Listen for a typical signal from the NLJD.

# 10. SUPPLEMENT #1. FUNCTIONS OF THE CONTROLS.

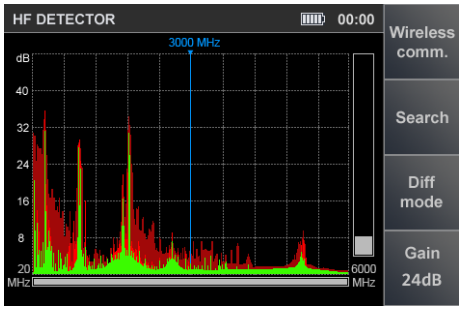
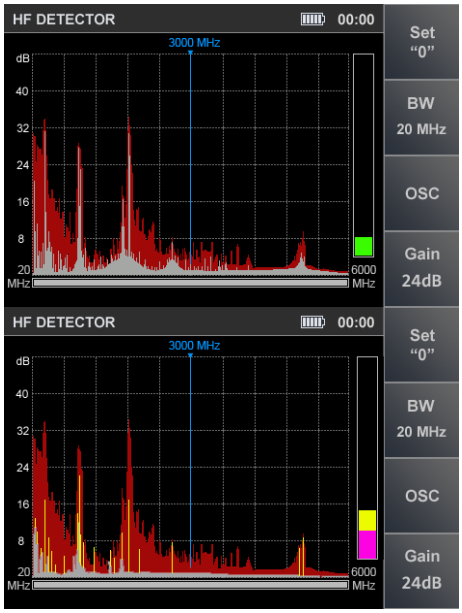
## 10.1. BASIC SETTINGS

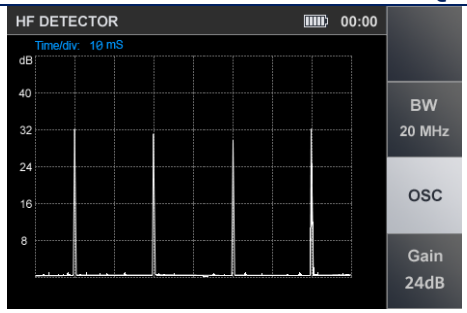
| MAIN MENU (CHANNEL SELECTION) | | |
|---|---|---|
|  | **F1** | enable **SELECTIVE HF DETECTOR** channel |
| | **F2** | enable **IR DETECTOR** channel |
| | **F3** | enable **WIRED RECEIVER** channel |
| | **F4** | enable **LOW FREQUENCY AMPLIFIER** channel |
| | ⇧ ⇩ | navigate |
| | **ENTER** | confirmation of action |
| | | entering the **SETTINGS** mode - place the cursor on the corresponding menu item and press ENTER |
| **SETTINGS** | | |
|  | ⇧ ⇩ | navigate |
| | **ENTER** | confirmation of action |
| | **ESC** | exit to the main menu of device |
| | | to change the interface language, select "ENGLISH" or "РУССКИЙ" and press ENTER |
| **SETTING THE DATE** | | |
|  | ⇦ ⇨ | navigate |
| | ⇧ ⇩ | change value |
| | **ENTER** | save and exit |
| | **ESC** | exit without saving |
| **SETTING THE TIME** | | |
|  | ⇦ ⇨ | navigate |
| | ⇧ ⇩ | change value |
| | **ENTER** | save and exit |
| | **ESC** | exit without saving |

## 10.2. SELECTIVE HF DETECTOR

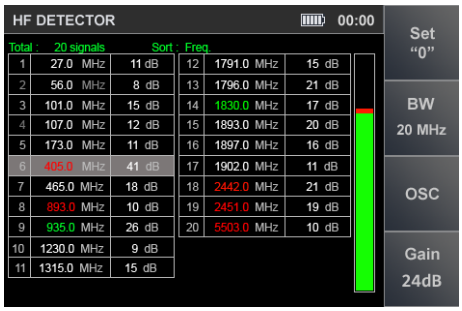
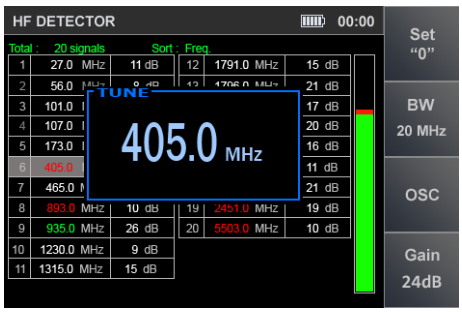
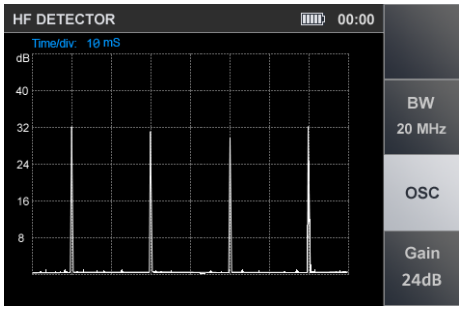
| GAIN ADJUSTMENT | |
|---|---|
|  |  increase gain |
| |  decrease gain |
| | **F4**<br>**ENTER** — deactivate **Gain adjustment** |
| | **MODE** — go to main menu of device |
| | **ESC**<br>**FUNC**<br>**F1-F3** — disabled |

### "PANORAMA" (DIFFERENTIAL) mode

| "PANORAMA" (DIFFERENTIAL) mode | |
|---|---|
|  | **ESC or MODE** — go to main menu of device |
| |  scaling **(Zoom +)** |
| |  scaling **(Zoom -)** |
| | scaling occurs relative to the set frequency (at cursor position). |
| |  frequency tuning |
| | **F1** — activate **"WIRELESS COMMUNICATION"** mode |
| | **F2** — activate **AUTOMATED** mode |
| | **F3** — activate/deactivate **DIFFERENTIAL** mode |
| | **F4** — activate **Gain Setting** |
| | **ENTER** — turn on "**FIXED FREQUENCY ANALYSIS**" function |
| | **FUNC** — disabled |
| **"PANORAMA" (DIFFERENTIAL) mode. "FIXED FREQUENCY ANALYSIS" function** | |
|  | **MODE** — go to main menu of device |
| | **ESC or ENTER** — turn off (step back) |
| |  cursor positioning (frequency tuning) |
| | **F1** — turn on/off **"SET "0""** |
| | **F2** — select passband (1 or 20 MHz) |
| | **F3** — activate **OSCILLOSCOPE** |
| | **F4** — activate **Gain Setting** |
| | **FUNC**  — disabled |

| "PANORAMA" MODE. FIXED FREQUENCY ANALYSIS, OSCILLOSCOPE | |
|---|---|
|  | **MODE** — go to main menu of device<br>**ESC F3** — turn off **OSCILLOSCOPE**<br>⇦⇨ — time-axis zoom<br>**F2** — select passband (1 or 20 MHz)<br>**F4** — activate **Gain Setting**<br>**ENTER** ⇧⇩ **FUNC** — disabled |

## AUTOMATED mode

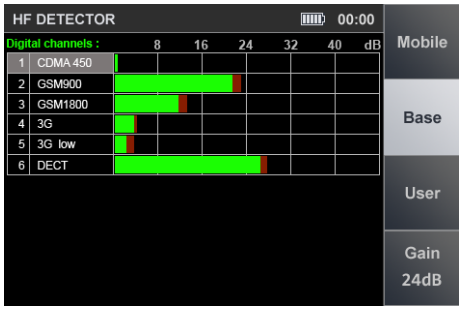
| AUTOMATED mode, main table | |
|---|---|
|  | **MODE** — go to main menu of device<br>**ESC** — return to the previous mode<br>**FUNC** — sort table (by ascending frequency or signal level)<br>**ENTER** — activate **"FREQUENCY TUNING"** function<br>⇦⇨ ⇧⇩ — navigate<br>**F1** — turn on/off **"SET "0"**<br>**F2** — select passband (1 or 20 MHz)<br>**F3** — activate **OSCILLOSCOPE**<br>**F4** — activate **Gain Setting** |
| **AUTOMATED mode, "FREQUENCY TUNING" function** | |
|  | **MODE** — go to main menu of device<br>**ESC and ENTER** — turn off **"FREQUENCY TUNING"** function<br>⇦⇨ — frequency tuning (with 0.2 MHz increment)<br>**F1** — turn on/off **"SET "0"**<br>**F2** — select passband (1 or 20 MHz)<br>**F3** — **OSCILLOSCOPE** activation<br>**F4** — activate **Gain Setting**<br>**FUNC** ⇩⇧ — disabled |
| **AUTOMATED mode, OSCILLOSCOPE** | |
|  | **MODE** — go to main menu of device<br>**ESC and F3** — turn off **OSCILLOSCOPE**<br>⇦⇨ — time-axis zoom<br>**F2** — select passband (1 or 20 MHz)<br>**F4** — activate **Gain Setting**<br>**ENTER** ⇧⇩ **FUNC** — disabled |

## "WIRELESS COMMUNICATION" MODE

### "MOBILE DEVICES MONITORING" function

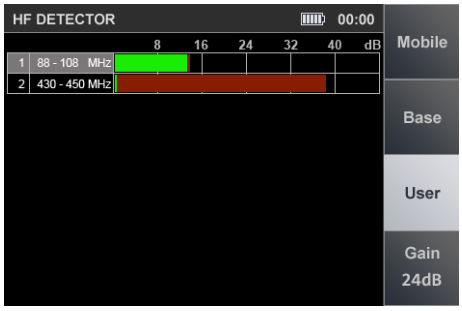

| | |
|---|---|
| **MODE** | go to main menu of device |
| **ESC** | go to **"PANORAMA"** |
| ⇩ ⇧ | navigate |
| **ENTER** | turn on **"ANALYZING DETECTED SIGNALS"** |
| **F2** | turn on **"BASE STATION MONITORING"** |
| **F3** | turn on **"USER LIST"** |
| **F4** | activate **Gain Setting** |
| **F1, FUNC** ⇦ ⇨ | disabled |

### "BASE STATIONS MONITORING" function



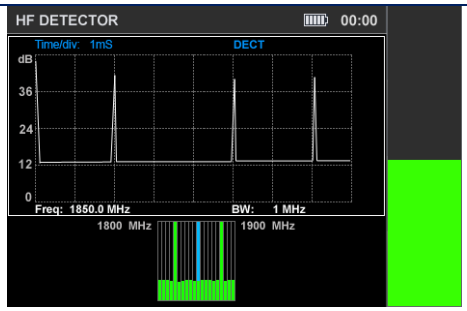

| | |
|---|---|
| **MODE** | go to main menu of device |
| **ESC** | go to the previous mode (step back) |
| ⇩ ⇧ | navigate |
| **ENTER** | turn on **"ANALYZING DETECTED SIGNALS"** |
| **F1** | turn on **"MOBILE DEVICES MONITORING "** |
| **F3** | turn on **"USER LIST"** |
| **F4** | activate **Gain Setting** |
| **F2, FUNC** ⇦ ⇨ | disabled |

### "USER LIST" function



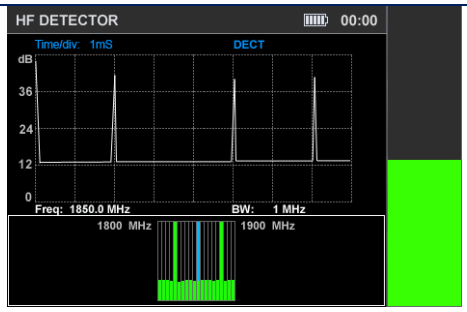

| | |
|---|---|
| **MODE** | go to main menu of device |
| **ESC** | go to the previous mode (step back) |
| ⇩ ⇧ | navigate |
| **ENTER** | turn on **"ANALYZING DETECTED SIGNALS"** |
| **F1** | turn on **" MOBILE DEVICES MONITORING"** |
| **F2** | turn on **"BASE STATIONS MONITORING"** |
| **F4** | activate **Gain Setting** |
| **F1, FUNC** ⇦ ⇨ | disabled |

### "ANALYZING DETECTED SIGNALS", OSCILLOSCOPE



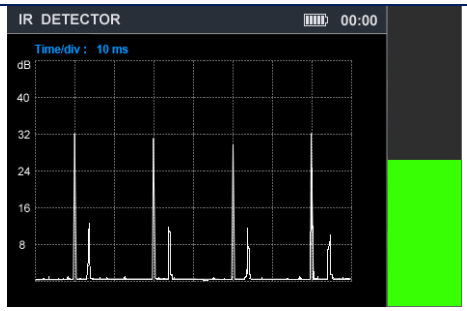

| | |
|---|---|
| **MODE** | go to main menu of device |
| **ESC** | go to the previous mode (step back) |
| ⇩ ⇧ | switch to **SPECTRUM ANALYZER** |
| **ENTER** | turn on/off **"SET "0"** |
| ⇦ ⇨ | time-axis zoom |
| **F1-F4 FUNC** | disabled |

### "ANALYZING DETECTED SIGNALS", SPECTRUM ANALYZER




| | |
|---|---|
| **MODE** | go to main menu of device |
| **ESC** | exit to the previous mode (step back) |
| ⇩ ⇧ | switch to **OSCILLOSCOPE** |
| **ENTER** | turn on/off **"SET "0"** |
| ⇦ ⇨ | setting frequency |
| **F1-F4 FUNC** | disabled |

## 10.3. IR DETECTOR

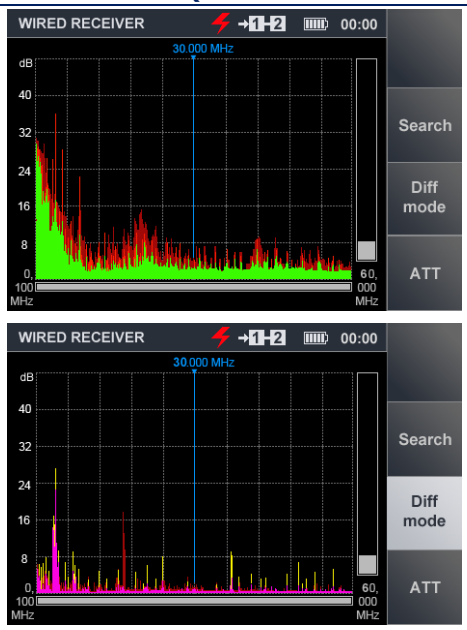



| | |
|---|---|
| **MODE ESC** | go to main menu of device |
| **ENTER** | activate /deactivate **DIFFERENTIAL mode** |
| ◄► | time-axis zoom |
| **F1-F4 FUNC** ▼▲ | disabled |

## 10.4. WIRED RECEIVER

## ELECTRIC MAINS TESTING

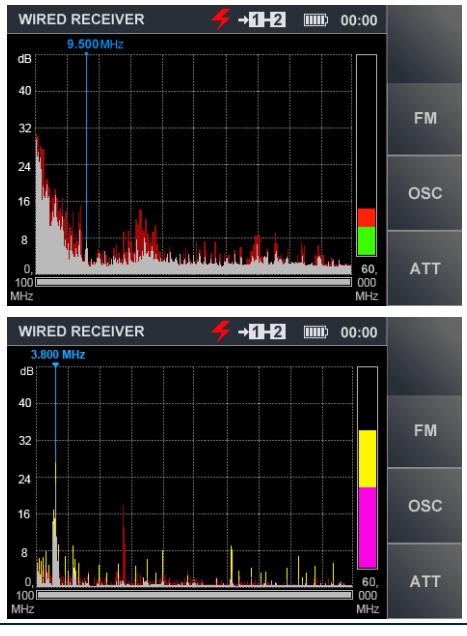
**"PANORAMA" (DIFFERENTIAL mode)**




| | |
|---|---|
| **ESC or MODE** | go to main menu of device |
| ▲ | scaling **(Zoom +)** [1] |
| ▼ | scaling **(Zoom -)**[1] |
| ◄► | cursor positioning |
| **ENTER** | turn on **"FIXED FREQUENCY ANALYSIS"** |
| **F2** | activate the AUTOMATED mode |
| **F3** | activate/deactivate **DIFFERENTIAL mode** |
| **F4** | activate/deactivate **Attenuator** |
| **F1 FUNC** | disabled |

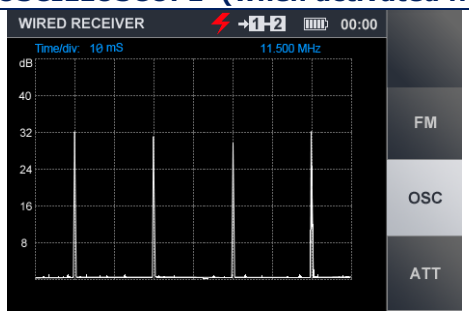
[1] - the scaling is centered on the selected frequency (at cursor position)

**"PANORAMA" (DIFFERENTIAL mode) FIXED FREQUENCY ANALYSIS function**



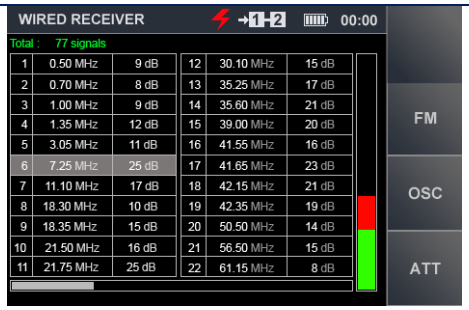

| | |
|---|---|
| **MODE** | go to main menu of device |
| **ESC or ENTER** | turn off (step back) |
| **F2** | toggle modulation **(FM/AM)** |
| **F3** | turn on **OSCILLOSCOPE** |
| **F4** | activate/deactivate **Attenuator** |
| ◄► | cursor positioning (frequency tuning) |
| **F1 FUNC** ▲▼ | disabled |

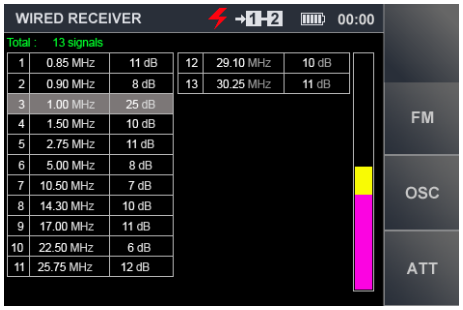
## OSCILLOSCOPE (when activated from the "PANORAMA" mode)




| | |
|---|---|
| **MODE** | go to main menu of device |
| **F3 ESC** | turn off **OSCILLOSCOPE** |
| **F2** | toggle modulation **(FM/AM)** |
| **F4** | activate/deactivate **Attenuator** |
| ◄► | time-axis zoom |
| **F1**<br>**FUNC**<br>▲▼ | disabled |

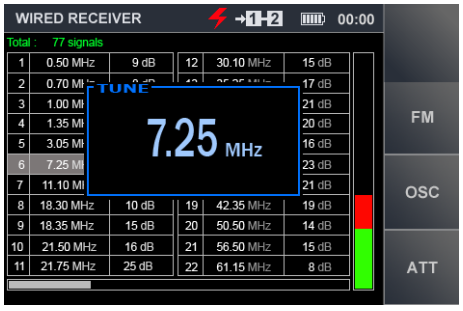
## AUTOMATED mode



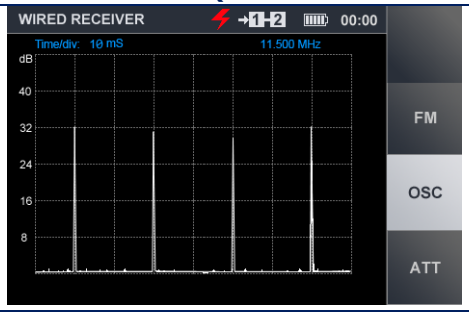

| | |
|---|---|
| **MODE** | go to main menu of device |
| **ESC** | return to the previous mode |
| **FUNC** | sort the table (by ascending frequency or signal level) |
| **ENTER** | turn on **"FREQUENCY TUNING"** function |
| ◄►<br>▲▼ | navigate |
| **F2** | toggle modulation **(FM/AM)** |
| **F3** | **OSCILLOSCOPE** activation |
| **F4** | activate/deactivate **Attenuator** |
| **F1** | disabled |

## "FREQUENCY TUNING" function




| | |
|---|---|
| **MODE** | go to main menu of device |
| **ENTER**<br>**ESC** | exit **"FREQUENCY TUNING"** function |
| ◄► | frequency tuning (with 10 kHz increment) |
| **F2** | toggle modulation **(FM/AM)** |
| **F3** | turn on **OSCILLOSCOPE** |
| **F4** | turn on/off **Attenuator** |
| **FUNC**<br>**F1**<br>▲▼ | disabled |

## OSCILLOSCOPE (when activated from the AUTOMATED mode)




| | |
|---|---|
| **MODE** | go to main menu of device |
| **F3 ESC** | turn off **OSCILLOSCOPE** |
| **F2** | toggle modulation **(FM/AM)** |
| **F4** | turn on/off **Attenuator** |
| ◄► | time-axis zoom |
| **F1**<br>**FUNC**<br>▲▼ | disabled |

## LOW CURRENT CIRCUIT TESTING

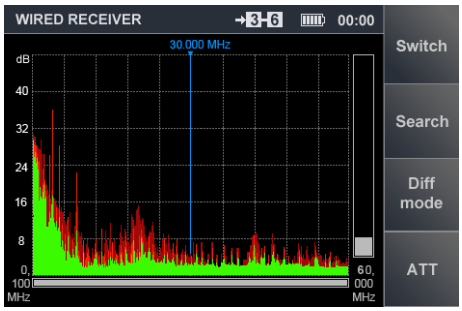
### "ELECTRONIC SWITCH CONTROL" mode

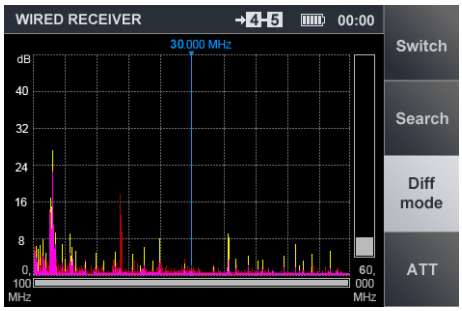

| | |
|---|---|
| **MODE**<br>**ESC** | go to main menu of device |
| ◄► ▲▼ | navigate |
| **ENTER** | activate **"PANORAMA"** mode |
| **FUNC** | activate **"ELECTRONIC SWITCH SETTINGS"** mode |
| **F1-F4** | disabled |

### "ELECTRONIC SWITCH SETTINGS" mode


| | |
|---|---|
| **ESC**<br>**FUNC** | deactivate **"ELECTRONIC SWITCH SETTINGS"** mode |
| **F1** | select/deselect the **8P8C** standard scheme |
| **F2** | select/deselect the **6P6C** standard scheme |
| **F3** | select/deselect the **6P4C** standard scheme |
| **F4** | select/deselect the **6P2C** standard scheme |
| ▲▼ | choose pin number (when setting manually) |
| **ENTER** | select/deselect pin (when setting manually) |
| ◄►<br>**MODE** | disabled |

### "PANORAMA" (DIFFERENTIAL mode)

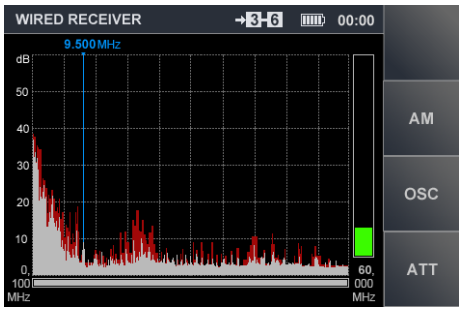


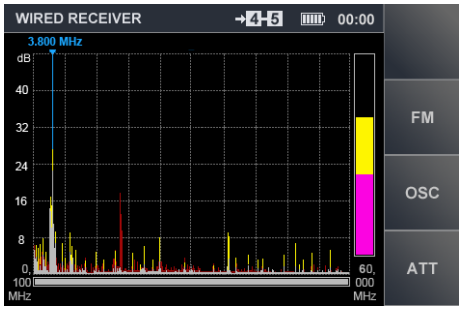




| | |
|---|---|
| **MODE** | go to main menu of device |
| ▲ | scaling **(Zoom +)** |
| ▼ | scaling **(Zoom -)** |
| ◄► | cursor positioning |
| **ENTER** | turn on **"FIXED FREQUENCY ANALYSIS"** function |
| **F1**<br>**ESC** | go to **"ELECTRONIC SWITCH CONTROL"** mode |
| **F2** | activate the **AUTOMATED** mode |
| **F3** | activate/deactivate **DIFFERENTIAL** mode |
| **F4** | turn on/off **Attenuator** |
| **FUNC** | disabled |

[1] - the scaling is centered on the selected frequency (at cursor position)

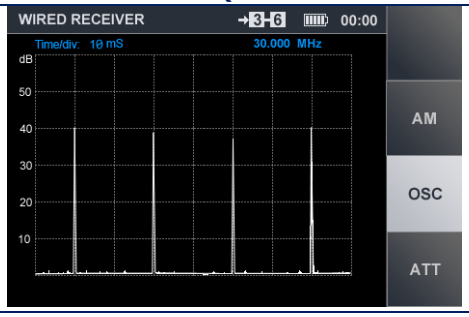
## "PANORAMA" (DIFFERENTIAL mode). "FIXED FREQUENCY ANALYSIS" function



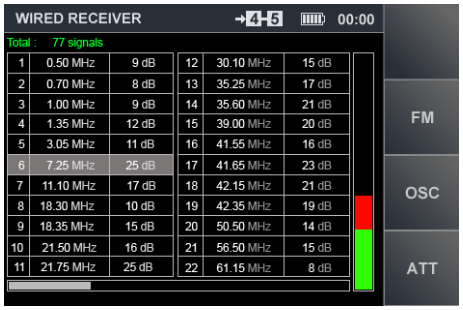

| | |
|---|---|
| **MODE** | go to main menu of device |
| **ESC**<br>**ENTER** | turn off **"FIXED FREQUENCY ANALYSIS"** function |
| **F2** | toggle modulation **(FM/AM)** |
| **F3** | turn on **OSCILLOSCOPE** |
| **F4** | turn on/off **Attenuator** |
| ◄► | cursor positioning (frequency tuning) |
| **F1**<br>**FUNC**<br>▲▼ | disabled |

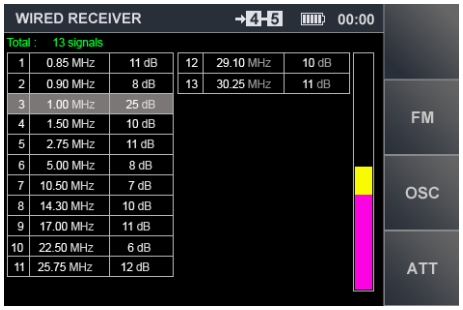
## OSCILLOSCOPE (when activated from the "PANORAMA" mode)




| | |
|---|---|
| **MODE** | go to main menu of device |
| **F3, ESC** | turn off **OSCILLOSCOPE** |
| **F2** | toggle modulation **(FM/AM)** |
| **F4** | turn on/off **Attenuator** |
| ◄► | time-axis zoom |
| **F1**<br>**FUNC**<br>▲▼ | disabled |

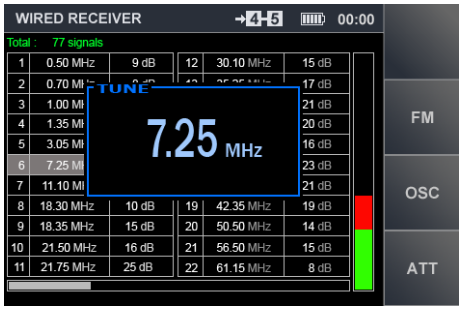
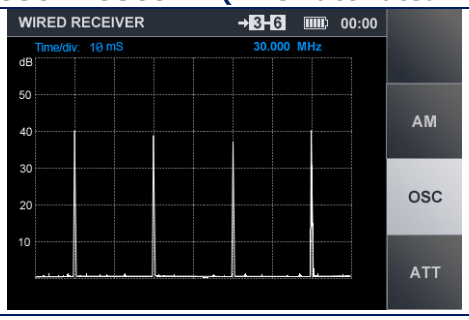
## AUTOMATED mode




| | |
|---|---|
| **MODE** | go to main menu of device |
| **ESC** | return to the previous mode[1] |
| **FUNC** | sort the table (by ascending frequency or signal level) |
| **ENTER** | turn on **"FREQUENCY TUNING"** function |
| ◄►<br>▲▼ | table row selection |
| **F1** | go to **"ELECTRONIC SWITCH CONTROL"** |
| **F2** | toggle modulation **(FM/AM)** |
| **F3** | turn on **OSCILLOSCOPE** |
| **F4** | turn on/off **Attenuator** |

[1] – returns to the DIFFERENTIAL mode, if the AUTOMATED mode was activated from the DIFFERENTIAL mode

| "FREQUENCY TUNING" function | |
|---|---|
|  | **MODE** — go to main menu of device<br>**ENTER ESC** — turn off **"FREQUENCY TUNING"** function<br>◄► — adjust frequency<br>**F2** — toggle modulation **(FM/AM)**<br>**F3** — turn on **OSCILLOSCOPE**<br>**F4** — turn on/off **Attenuator**<br>**FUNC F1** ▲▼ — disabled |
| **OSCILLOSCOPE (when activated from the AUTOMATED mode)** | |
|  | **MODE** — go to main menu of device<br>**F3, ESC** — turn off **OSCILLOSCOPE**<br>**F2** — toggle modulation **(FM/AM)**<br>**F4** — turn on/off **Attenuator**<br>◄► — time-axis zoom<br>**F1 FUNC** ▲▼ — disabled |

## 10.5. LOW FREQUENCY AMPLIFIER

| "ELECTRONIC SWITCH CONTROL" mode | |
|---|---|
|  | **MODE ESC** — go to main menu of device<br>◄► ▲▼ — navigate<br>**ENTER F1** — turn on **OSCILLOSCOPE**<br>**FUNC** — activate **"ELECTRONIC SWITCH SETTINGS"**mode<br>**F2** — activate **Gain Setting**<br>**F3** — activate **Bias Voltage Control**<br>**F4** — activate AUTOMATED mode |
| **"ELECTRONIC SWITCH SETTINGS" mode** | |
|  | **ESC FUNC** — deactivate **"ELECTRONIC SWITCH SETTINGS"** mode<br>**F1** — select/deselect the standard scheme **8P8C**<br>**F2** — select/deselect the standard scheme **6P6C**<br>**F3** — select/deselect the standard scheme **6P4C**<br>**F4** — select/deselect the standard scheme **6P2C**<br>▼▲ — choose pin number (when setting manually)<br>**ENTER** — select/deselect pin (when setting manually)<br>◄► **MODE** — disabled |

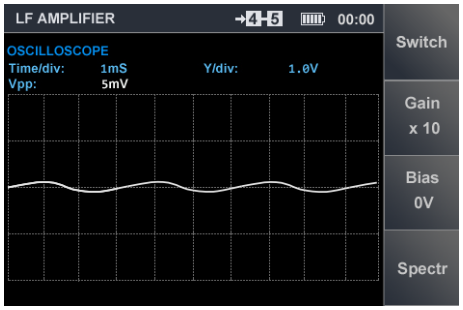
## GAIN SETTING


| | |
|---|---|
| **MODE** | go to the main menu of device |
| **F2** | deactivate **GAIN SETTING** |
| **F3** | activate **Setting the Bias Voltage** |
| ⇧ ⇨ | **Gain** + |
| ⇩ ⇦ | **Gain** - |
| **ENTER** | set minimum **gain** (x1) |
| **ESC FUNC F1 F4** | disabled |

## BIAS VOLTAGE CONTROL

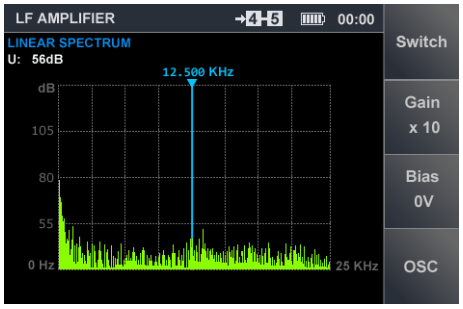

| | |
|---|---|
| **MODE** | go to main menu of device |
| **F3** | deactivate **Bias Voltage Control** |
| **F2** | activate **Gain Setting** |
| ⇧ ⇨ | setting the **Bias Voltage** +30 V |
| ⇩ ⇦ | setting the **Bias Voltage** -30 V |
| **ENTER** | setting the **Bias Voltage** 0 V |
| **FUNC ESC F1 F4** | disabled |

## OSCILLOSCOPE




| | |
|---|---|
| **MODE** | go to main menu of device |
| **F1 ESC** | go to **"ELECTRONIC SWITCH CONTROL"** mode |
| **F2** | activate **Gain Setting** |
| **F3** | activate **Bias Voltage Control** |
| **F4** | turn on **SPECTRUM ANALYZER** |
| ⇩ ⇧ | vertical zoom of the **OSCILLOSCOPE** |
| ⇦ ⇨ | horizontal zoom of the **OSCILLOSCOPE** |
| **ENTER FUNC** | disabled |

## SPECTRUM ANALYZER

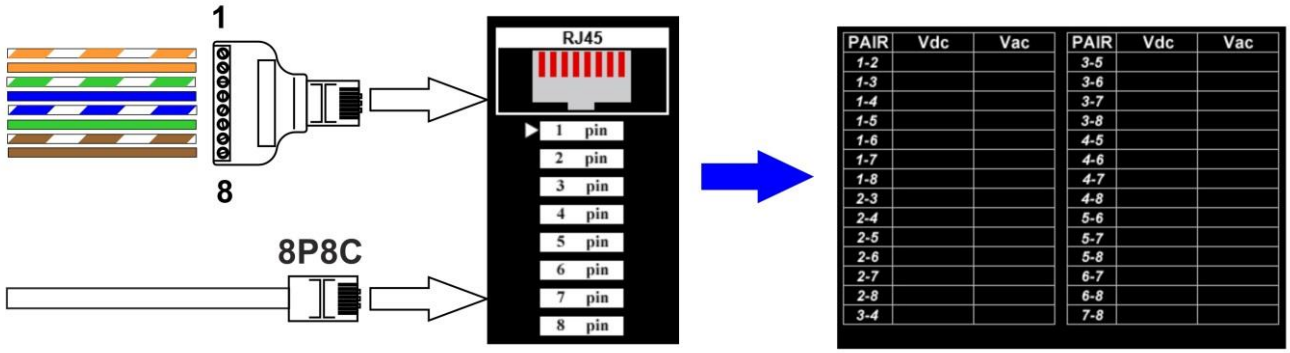



| | |
|---|---|
| **MODE** | go to main menu of device |
| **F1 ESC** | go to **"ELECTRONIC SWITCH CONTROL"** mode |
| **F2** | activate **Gain Setting** |
| **F3** | activate **Bias Voltage Control** |
| **F4** | turn on **OSCILLOSCOPE** |
| ⇦ ⇨ | cursor positioning |
| **ENTER FUNC** ⇩ ⇧ | disabled |

# 11. SUPPLEMENT #2. TYPICAL SETTINGS OF THE ELECTRONIC SWITCH.

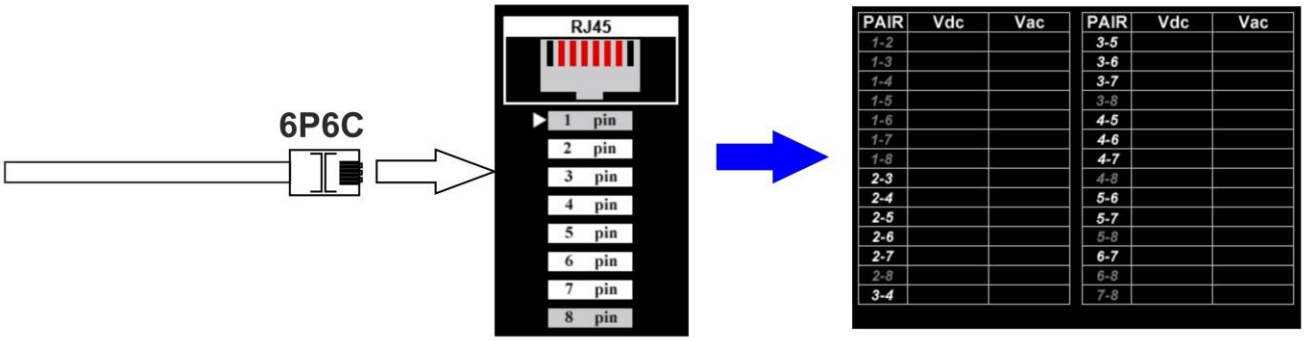
## 8C8P connecting ("F1")

Computer 8-wire line equipped RJ45 connector



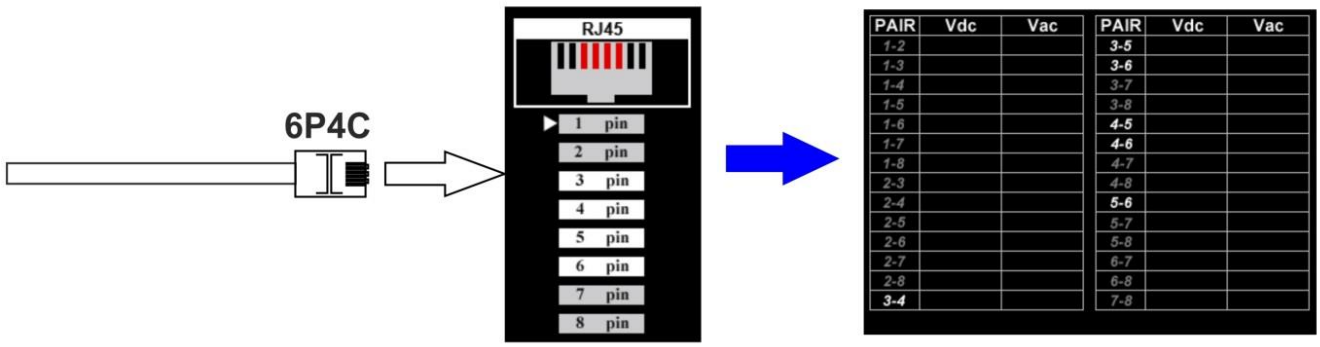

## 6P6C connecting ("F2")

6-wire  telephone line, equipped with connector RJ25 or RJ12



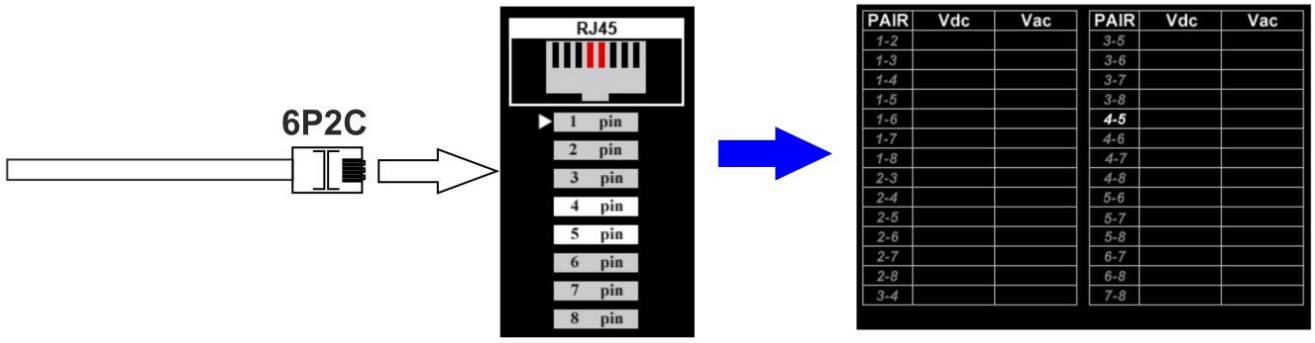

## 6P4C connecting ("F3")

4-wire telephone line (equipped with connectors RJ11)



### 6P2C connecting ("F4")

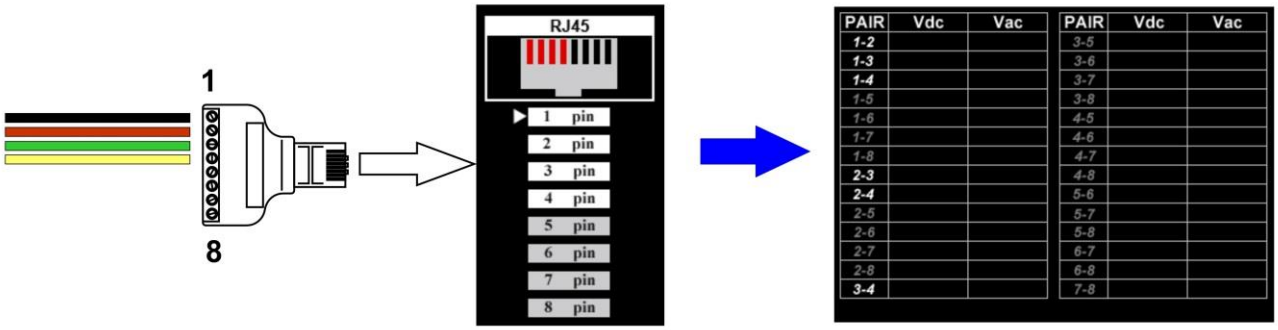
2-wire telephone line (equipped with RJ25 or RJ11)




---

### Manual setup of the electronic switch (△, ▽ and "ENTER")

Settings for an arbitrary 4-wire line, not equipped with a connector (connection through RJ45 adapter)




---

# 12. SUPPLEMENT #3. REFERENCE INFORMATION.

## 12.1. "TWISTED PAIR" CABLE

A twisted pair cable is a type of cable that consists of one or several twisted pairs, *i.e.*, insulated conductor strands twisted together with relatively few windings per length unit and enclosed in an outer plastic casing.

Twisting helps increase consistency between two cores of a pair (as electromagnetic interference from external sources will affect them equally) and to reduce electromagnetic interference, both external and mutual, when differential signals are being transmitted.

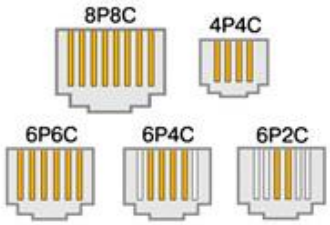
In order to reduce interaction of different pairs in a bundled twisted pair cable, cables of the 5$^{th}$ category or higher utilize twisted pairs with different numbers of windings per length unit.

Twisted pair cables are widely used in telecommunications and computer networking, and most typically consist of one, two, or four twisted pairs.

## 12.2. RJ CONNECTORS

RJ (Registered Jack) is a standardized physical network interface comprising both connectors ('plug' and 'socket') and their connection scheme. It is widely used in telecommunications. The most common standards of this kind are RJ11, RJ14, RJ25, and RJ45.

| Standard | Scheme | Number of pins | Purpose |
|---|---|---|---|
| RJ9 | 4P4C | 4 | connecting telephone handsets to their bases |
| RJ11 | 6P2C | 2 | connecting two-wire telephone sets to the network |
| RJ12 | 6P6C | 6 | connecting 6-wire telephone sets |
| RJ11 | 6P4C | 4 | connecting 4-wire telephone sets |
| RJ21 | 50-pin | 50 | connecting PBX's or other telecom equipment (sometimes also called "Telco" or "Amphenol") |
| RJ25 | 6P6C | 6 | connecting 6-wire telephone sets |
| RJ45S | 8P4C with key | 4 | connecting modems |
| RJ45 | 8P8C | 8 | creating local area networks |
| RJ50 | 10P10C | 10 | used by UPS units made by American Power Conversion and Eaton Corporation |



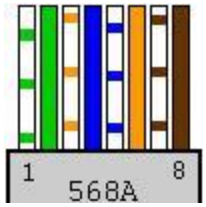

In the notation "xPyC", the letter "P" stands for 'Positions' in a plug, and "C", for "Contacts" in a socket.

## 12.3. WIRING SCHEME OF A FOUR TWISTED PAIR CABLE

For 10Base-T and 100Base-T Ethernet standards, four cores (orange and green pairs) are used, while the remaining four are reserved for the Gigabit Ethernet (1000Base-T) standard. There are two wiring schemes, 568A and 568B. The latter is more frequent.

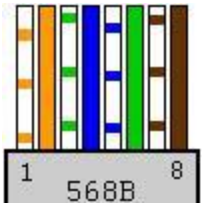
### 12.3.1. EIA/TIA-568A WIRING SCHEME

| 1st connector # | Color of wire | 2nd connector # |
|---|---|---|
| 1 | white and green (TX+) | 1 |
| 2 | green (TX-) | 2 |
| 3 | white and orange (RX+) | 3 |
| 4 | blue | 4 |
| 5 | white and blue | 5 |
| 6 | orange (RX-) | 6 |
| 7 | white and brown | 7 |
| 8 | brown | 8 |




### 12.3.2. WIRING SCHEME EIA/TIA-568B

| 1st connector # | Color of wire | 2nd connector # |
|---|---|---|
| 1 | white and orange (TX+) | 1 |
| 2 | orange (TX-) | 2 |
| 3 | white and green (RX+) | 3 |
| 4 | blue | 4 |
| 5 | white and blue | 5 |
| 6 | green (RX-) | 6 |
| 7 | white and brown | 7 |
| 8 | brown | 8 |




## 12.4. CROSSOVER WIRING SCHEME

The wiring scheme of a cable linking two network interface cards is different in that the green and orange pairs have their places swapped at one end of the cable, one of the connectors being 586A, and the other 586B. This is called a "crossover", or "null-hub" cable. The same scheme is used for cascading (connecting) hubs.

| 1st connector # | Color of wire | 2nd connector # |
|---|---|---|
| 1 | white and green (TX+) | 3 |
| 2 | green (TX-) | 6 |
| 3 | white and orange (RX+) | 1 |
| 4 | blue | 4 |
| 5 | white and blue | 5 |
| 6 | orange (RX-) | 2 |
| 7 | white and brown | 7 |
| 8 | brown | 8 |

A crossover connection between two computers is also possible as illustrated in the tables below, but such connections are rare.

| 1st connector # | Color of wire | 2nd connector # |
|---|---|---|
| **scheme 1** | | |
| 1 | white and green (TX+) | 3 |
| 2 | green (TX-) | 6 |
| 3 | white and orange (RX+) | 1 |
| 4 | blue | 7 |
| 5 | white and blue | 8 |
| 6 | orange (RX-) | 2 |
| 7 | white and brown | 4 |
| 8 | brown | 5 |
| **scheme 2** | | |
| 1 | white and orange (TX+) | 3 |
| 2 | orange (TX-) | 6 |
| 3 | white and green (RX+) | 1 |
| 4 | blue | 7 |
| 5 | white and blue | 8 |
| 6 | green (RX-) | 2 |
| 7 | white and brown | 4 |
| 8 | brown | 5 |

## 12.5. WIRING SCHEME OF A THREE, TWO, AND ONE TWISTED PAIR CABLE

| RJ connector pin # | RJ25 | RJ14 | RJ11 | Contemporary coloring | Obsolete coloring |
|---|---|---|---|---|---|
| 1 | X | | | white and green | orange |
| 2 | X | X | | white and orange | black |
| 3 | X | X | X | blue | red |
| 4 | X | X | X | white and blue | green |
| 5 | X | X | | orange | yellow |
| 6 | X | | | green | blue |

## 12.6. REFERENCE INFORMATION ON TELEPHONE LINES

There are analog, hybrid, and digital PBXs

- in circuits of analog PBXs signals are transmitted in the analog form
- in a digital PBX, the voice signal is converted into digital signal
- in a hybrid PBXs, analog signal in the speech frequency band is transmitted without conversion.

The term "hybrid" means that system and analogue phone sets can be plugged in.

| Line type | Purpose | User device |
|---|---|---|
| two-wire analogue | municipal telephone line, office PBX analogue line | analogue telephone |
| two-wire digital | office PBX digital line | digital telephone |
| four-wire digital | office PBX digital lines | digital system telephone |
| four-wire hybrid | office PBX hybrid lines | analogue system telephone |

**PAIRS OF WIRES USED IN TELEPHONE CIRCUITS**

| line type | RJ connector | RJ connector pin # | Wire coloring | |
|---|---|---|---|---|
| | | | Modern | Obsolete |
| 2-wire analog | RJ-9 | 2-3 – analog signal | green<br>orange | red<br>green |
| | RJ-11/14/25 | 3-4 – analog signal | white and blue<br>blue | red<br>green |
| 2-wire digital | RJ-11/14/25 | 3-4 – digital signal | white and blue<br>blue | red<br>green |
| 4-wire digital | RJ-14/25 | 3-4 – digital signal | white and blue<br>blue | red<br>green |
| | | 2-5 – PBX commands | white and orange<br>orange | black<br>yellow |
| 4-wire hybrid | RJ-14/25 | 3-4 – analog signal | white and blue<br>blue | red<br>green |
| | | 2-5 – PBX commands | white and orange<br>orange | black<br>yellow |