

ST300 SPIDER

LINE AND MAINS ANALYZER

OPERATING MANUAL

OPERATING MANUAL

| CONTENTS | | Pg |
|----------|---|----|
| | Introduction | 3 |
| 1. | General Information on ST300 "SPIDER" | 3 |
| 1.1. | Purpose and Main Features | 3 |
| 1.2. | Packing and Kit | 4 |
| 1.2.1. | Packing | 4 |
| 1.2.2. | Supply Kit | 5 |
| 1.3. | Design | 6 |
| 1.3.1. | Main Unit | 6 |
| 1.3.2. | Electronic Switch | 7 |
| 1.3.3. | Connecting the Electronic Switch to the Main Unit | 8 |
| 1.3.4. | Receiver of the Cable Locator | 8 |
| 1.3.5. | Adaptor for Testing Power Mains | 10 |
| 1.3.6. | Test sound player | 11 |
| 2. | Operation Modes of ST300 | 12 |
| 2.1. | Startup | 12 |
| 2.2. | Start Menu (Mode Selection Menu) | 12 |
| 2.3. | Settings | 13 |
| 2.3.1. | Date Setup | 13 |
| 2.3.2. | Time Setup | 14 |
| 2.3.3. | Interface Language Setup | 14 |
| 2.4. | Electronic Switch Control Mode ("SWITCH") | 14 |
| 2.4.1. | Main Screen of the "SWITCH" Mode | 14 |
| 2.4.1.1. | Selecting a Wire Pair | 15 |
| 2.4.1.2. | Display of Wire Pair Selection | 15 |
| 2.4.1.3. | Display of Voltage in the Selected Wire Pair | 15 |
| 2.4.1.4. | Switching to Other Modes | 15 |
| 2.4.2. | Additional Modes | 15 |
| 2.4.2.1. | Automatic Measurement Mode | 15 |
| 2.4.2.2. | "CABLE LOCATOR" Mode | 16 |
| 2.5. | "LOW FREQUENCY AMPLIFIER" Mode | 17 |
| 2.5.1. | Main Screen of the "LFA" Mode | 17 |
| 2.5.1.1. | Cable Settings | 18 |
| 2.5.1.2. | Gain Control | 19 |
| 2.5.1.3. | Setting a Bias Voltage | 19 |
| 2.5.1.4. | Switching to Other Modes | 20 |
| 2.5.2. | Automatic Mode of the LF Amplifier | 20 |
| 2.6. | "WIRED RECEIVER" Mode | 21 |
| 2.6.1. | Main Screen of the "WIRED RECEIVER" Mode | 21 |
| 2.6.2. | Differential Wired Receiver Mode | 22 |
| 2.6.3. | Monitoring Signal at a Set Frequency | 23 |
| 2.6.4. | "OSCILLOSCOPE" Mode | 24 |
| 2.6.5. | Automatic Mode of the Wired Receiver | 24 |
| 2.7. | "NONLINEAR JUNCTION DETECTOR" Mode | 25 |
| 2.7.1. | Main Screen of the "NLJD" Mode | 26 |
| 2.7.1.1. | Cable Settings | 26 |
| 2.7.2. | Automatic Mode of the Nonlinear Junction Detector | 26 |
| 2.7.2.1. | Cable Settings | 27 |

ST300 SPIDER

| | CONTENTS | Pg |
|----------|---|----|
| 2.7.1.2. | Automatic Scanning | 27 |
| 2.8. | "REFLECTOMETER" Mode | 27 |
| 2.8.1. | Main Screen of the "REF" Mode | 28 |
| 2.8.1.1. | Setting the Velocity Factor | 29 |
| 2.8.1.2. | Cable Settings | 29 |
| 2.8.1.3. | Measurements in the Main Screen | 29 |
| 2.8.2. | Automatic Reflectometer Mode | 30 |
| 3. | Basic Search Routines with ST300 | 32 |
| 3.1. | Physical Connection to the Tested Line | 32 |
| 3.2. | Electronic Connection to the Tested Line | 37 |
| 3.3. | Search for Low-Frequency Transmissions in Low-Current Lines | 40 |
| 3.3.1. | Search for Low-Frequency Transmissions: Manual "LFA" Mode | 40 |
| 3.3.2. | Search for Low-Frequency Transmissions: Automatic "LFA" Mode | 42 |
| 3.4. | Search for High-Frequency Transmissions in Cabling | 44 |
| 3.4.1. | Search for High-Frequency Transmissions in Power Mains | 44 |
| 3.4.2. | Search for High-Frequency Transmissions in Low-Current Lines | 46 |
| 3.5. | Nonlinearity Detection in Cabling | 47 |
| 3.5.1. | Nonlinear Junction Detector of ST300 in Use: Manual Mode | 78 |
| 3.5.2. | Nonlinear Junction Detector of ST300 in Use: Automatic Mode | 79 |
| 3.6. | Anomaly Detection in a Cable | 50 |
| 3.6.1. | Reflection Meter of ST300 in Use: Cable Testing from both Ends | 51 |
| 3.6.2. | Reflection Meter of ST300 in Use: Automatic Mode | 52 |
| 3.7. | Cable Tracing | 55 |
| 3.7.1. | Cable Locator of ST300 in Use: Non-Contact Search | 55 |
| 3.7.2. | Cable Locator of ST300 in Use: Contact Search | 56 |
| 3.8. | Locating a Detected Bugging Device | 57 |
| 3.8.1. | Locating a Detected Bugging Device with Test Sound | 57 |
| 3.8.2. | Locating a Detected Bugging Device with ST300 and a Nonlinear Junction Detector | 58 |
| 4. | Power Supply and Battery Charging | 59 |
| 5. | Technical Specifications of ST300 | 60 |
| 6. | Reference Information | 62 |
| 6.1 | Twisted Pair Cabling | 62 |
| 6.2 | RJ Standards | 62 |
| 6.3 | Wiring Scheme of a 4 Twisted-Pair Cable | 62 |
| 6.4 | Wiring Scheme of a 3, 2, and 1 Twisted-Pair Cable | 64 |
| 6.5 | Reference Information on Telephone Lines | 64 |

INTRODUCTION

This manual explains the operating principles, design, and functioning of the ST300 "SPIDER" Line Analyzer, please study it carefully before using the device.

Please connect any cabling, adaptors and/or auxiliary equipment to the device, observing the procedures and order as described in the applicable sections of this manual. For connection to power mains, please only use standard cables and adaptors supplied with ST300.

Please bear in mind that only properly trained and certified personnel may test power mains.

1. GENERAL INFORMATION ON ST300 "SPIDER"

1.1. PURPOSE AND MAIN FEATURES

Purpose

The ST300 "SPIDER" Line Analyzer is designed to detect and locate eavesdropping devices directly (galvanically) connected to power electric lines and low-current circuits. It employs both passive and active methods, which allows detecting eavesdropping devices that are active at the time of the sweep, as well as those that are "silent".

Main Features

ST300 "SPIDER" implements an essential set of features required for detecting and locating wire-connected eavesdropping electronics. Its capabilities include:

- the detection and estimation of signals from hard-wired microphones in low-voltage lines;
- forced activation of electret microphones by applying a bias voltage;
- detection of cable transmissions from eavesdropping devices in the frequency range from 100kHz to 150MHz;
- detection and estimation of unsolicited electric (galvanic) connections to cabling, in the modes of a nonlinear junction detector and a reflection meter;
- tracing the cabling in walls and other structures;
- testing multiple conductor cables with the aid of an electronic switch;
- measuring AC and DC voltages.

The device can be used on its own, or controlled from a computer utilizing special software.

WARNING! In all modes of operation, ST300 may only be powered from its internal power source (inbuilt battery)!

1.2. PACKING AND KIT

ST300 comes in a kit that serves all of the above-named research tasks and makes the device multi-purpose, its operation autonomous, and its transportation and storage safe and convenient.

1.2.1. Packing

ST300 is a portable device. It is carried and stored in a NANUK-915 shock- and moisture-proof plastic case. For the safety of transportation and storage, and the convenience of use, a three-layered packing scheme is employed, shown in Fig. 1.

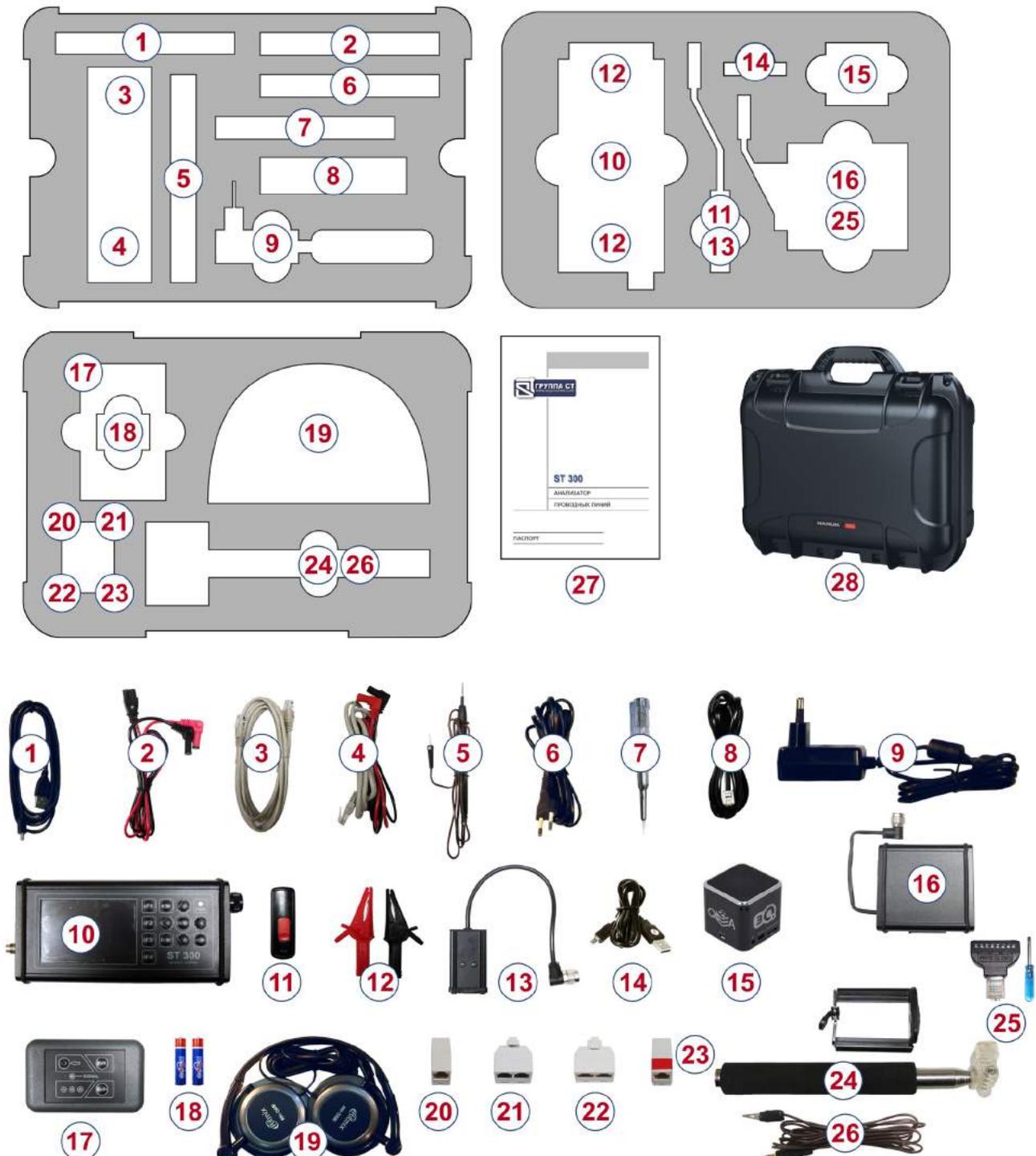


Fig.1

In Fig. 1, items supplied with ST300 are assigned the same numbers as in the following subsection (1.2.2) of this manual. Each item has its own position in the case; in order to avoid mechanical damage of the Main Unit and its accessories, please place them according to the manufacturer's layout.

1.2.2. Supply Kit

The Supply Kit that comes with ST300 includes:

- 1 – USB cable for connecting ST300 to a laptop1 pc.
- 2 – cable for telephone junction-box testing.....1 pc.
- 3 – cable for connecting the electronic switch to RJ45 sockets1 pc.
- 4 – cable for connecting the electronic switch to twin wire low voltage lines.....1 pc.
- 5 – probe for the cable locator receiver.....1 pc.
- 6 – cable for testing power mains equipped with electric sockets.....1 pc.
- 7 – tester screwdriver1 pc.
- 8 – cable for connecting the electronic switch to telephone sockets.....1 pc.
- 9 – charger.....1 pc.
- 10 – ST300 main unit1 pc.
- 11 – flashcard with software and documentation.....1 pc.
- 12 – crocodile clamp2 pcs.
- 13 – mains adaptor1 pc.
- 14 – cable for the test sound player.....1 pc.
- 15 – test sound player.....1 pc.
- 16 – electronic switch1 pc.
- 17 – receiver of the cable locator1 pc.
- 18 – accumulator batteries for the cable locator receiver (AAA).....2 pcs.
- 19 – headphones.....1 pc.
- 20 – pass-through socket (RJ45).....1 pc.
- 21 – splitter (RJ45).....1 pc.
- 22 – splitter (RJ12).....1 pc.
- 23 – short-circuiter socket (RJ45).....1 pc.
- 24 – telescopic arm of the cable locator receiver.....1 pc.
- 25 – multiwire cable connector (with a screwdriver)1 pc.
- 26 – ground connection cable.....1 pc.
- 27 – device passport.....1 pc.
- 28 – protective case with custom panels.....1 pc.

1.3 DESIGN

1.3.1 Main Unit

The appearance, connectors, control and display elements, as well as mechanical parts of the Main Unit, are shown in Fig. 2.

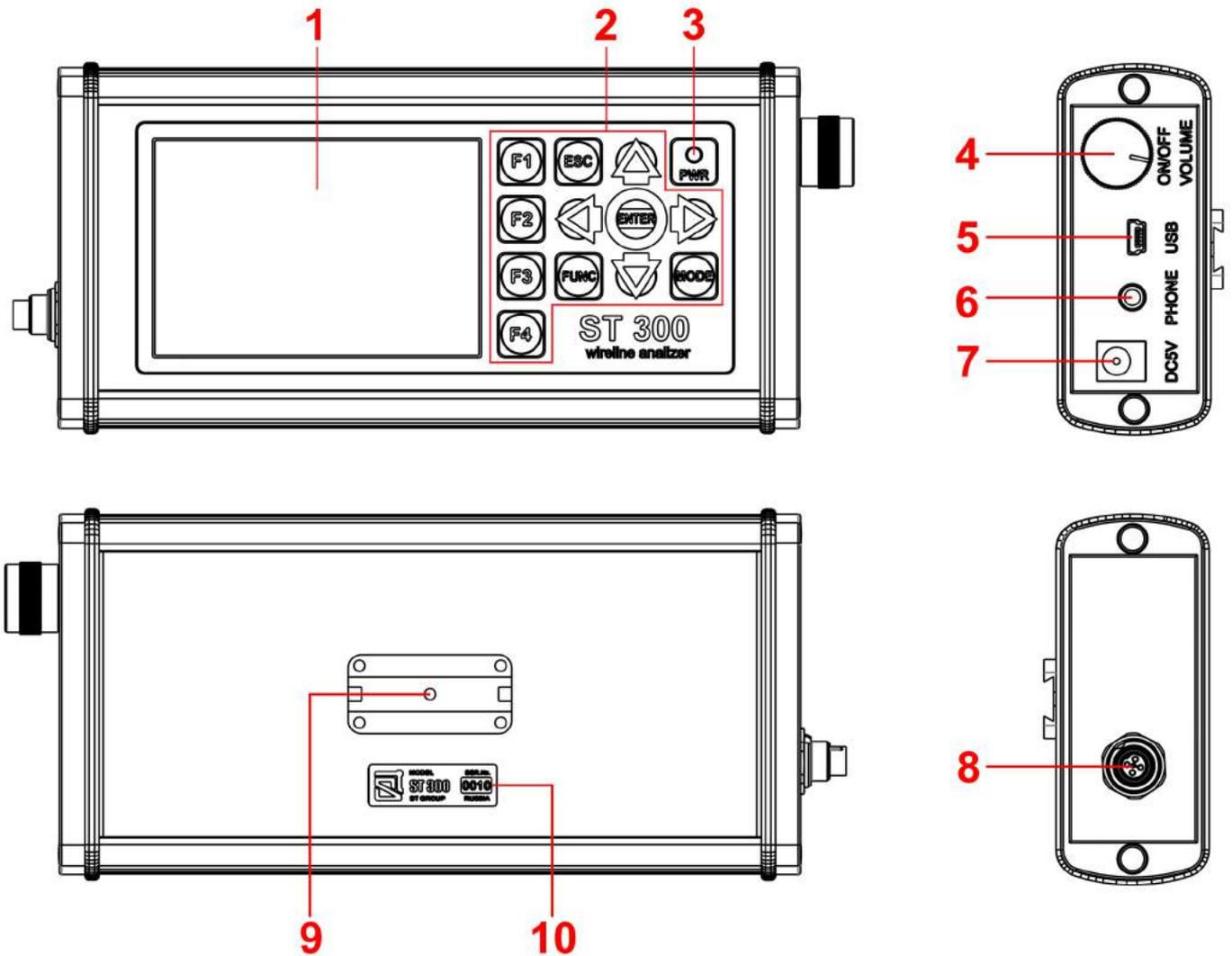


Fig.2

| # in fig. 2 | subscript on the unit | purpose |
|-------------|-----------------------|--|
| 1 | | color display for graphic data output |
| 2 | | keyboard |
| | F1-F4 | hotkeys whose assignment changes depending on the mode (and is shown on display) |
| | ESC | cancel / return to previous mode |
| | FUNC | additional functions |
| | ENTER | confirm mode selection / confirm action |
| | MODE | automatic mode on/off |

| # in fig. 2 | subscript on the unit | purpose |
|-------------|-----------------------|--------------------------------|
| 3 | PWR | external power indicator |
| 4 | ON/OFF VOLUME | power switch / volume control |
| 5 | USB | USB port for laptop connection |
| 6 | PHONE | headphone socket |
| 7 | DC5V | charger socket |
| 8 | | universal input connector |
| 9 | | slot for the Electronic Switch |
| 10 | | info shield |

1.3.2 Electronic Switch

The Electronic Switch is used for testing multiple-wire low-voltage cables. It is controlled from the Main Unit of ST300.

The appearance, connectors, control and display elements, as well as mechanical parts of the Electronic Switch, are shown in Fig. 3.

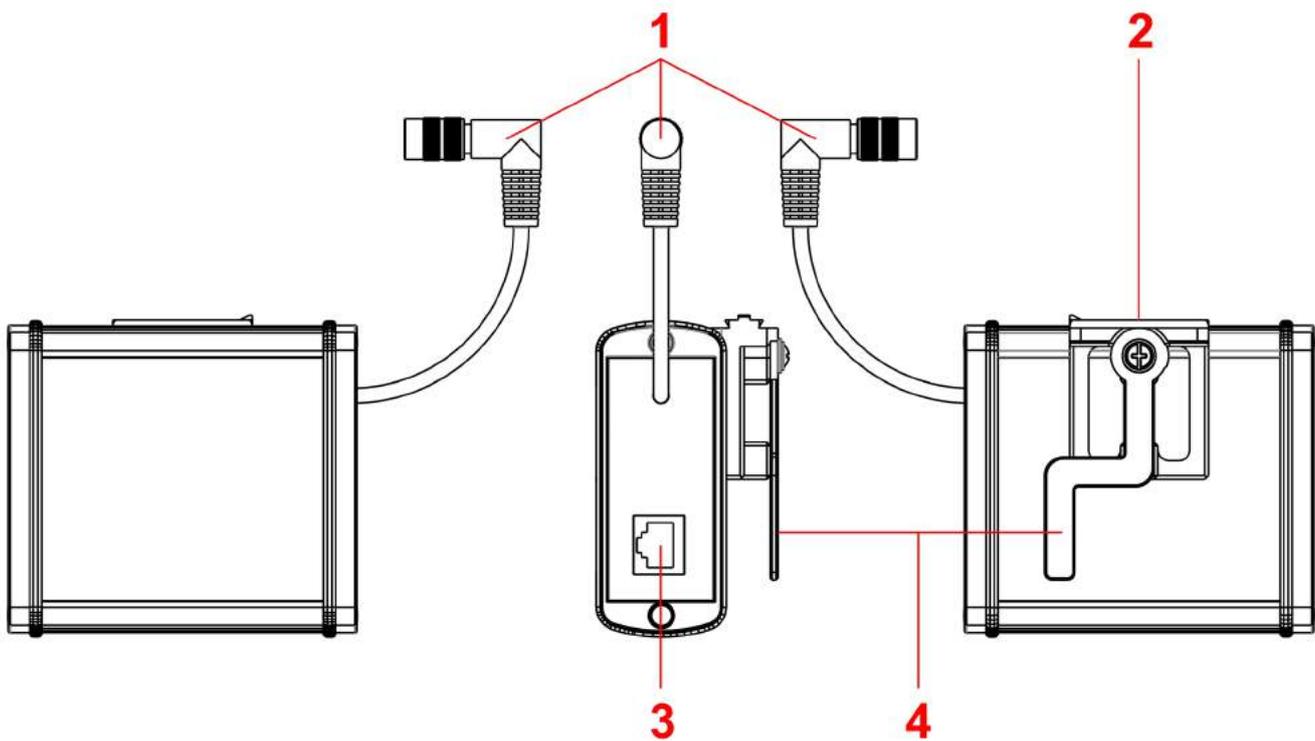


Fig.3

| # in fig. 3 | purpose |
|-------------|---|
| 1 | cable for connection to the main unit |
| 2 | bracket for attachment to the main unit |
| 3 | socket for cable with RJ45 connector |
| 4 | lever for attachment to the main unit |

1.3.3 Connecting the Electronic Switch to the ST300 Main Unit

The Electronic Switch is attached to the Main Unit with the aid of a T-slot & lock mechanism, parts of which are located on the body of the Main Unit, and on the Electronic Switch. The two units are locked together by rotating the lever.

The sequence of actions for joining the Electronic Switch with the Main Unit is shown in Fig. 4.

1. Insert the guide of the Electronic Switch into the T-slot on the Main Unit, with the lock arm in the vertical ("open") position. In the direction shown in the picture, slide the guide all the way through the slot (Fig. 4, step 1).

2. Rotate the lock lever all the way (Fig. 4, step 2).

3. Insert the Electronic Switch connector into the universal socket of the Main Unit (Fig. 4, step 3). Tighten the connector nut without applying extra force.

Step 4 in Fig. 4 portrays the Main Unit correctly joined with the Electronic Switch.

To disconnect and detach the Electronic Switch, proceed in the reverse sequence.

Caution! Connect (disconnect) the Electronic Switch only while the Main Unit is turned off!

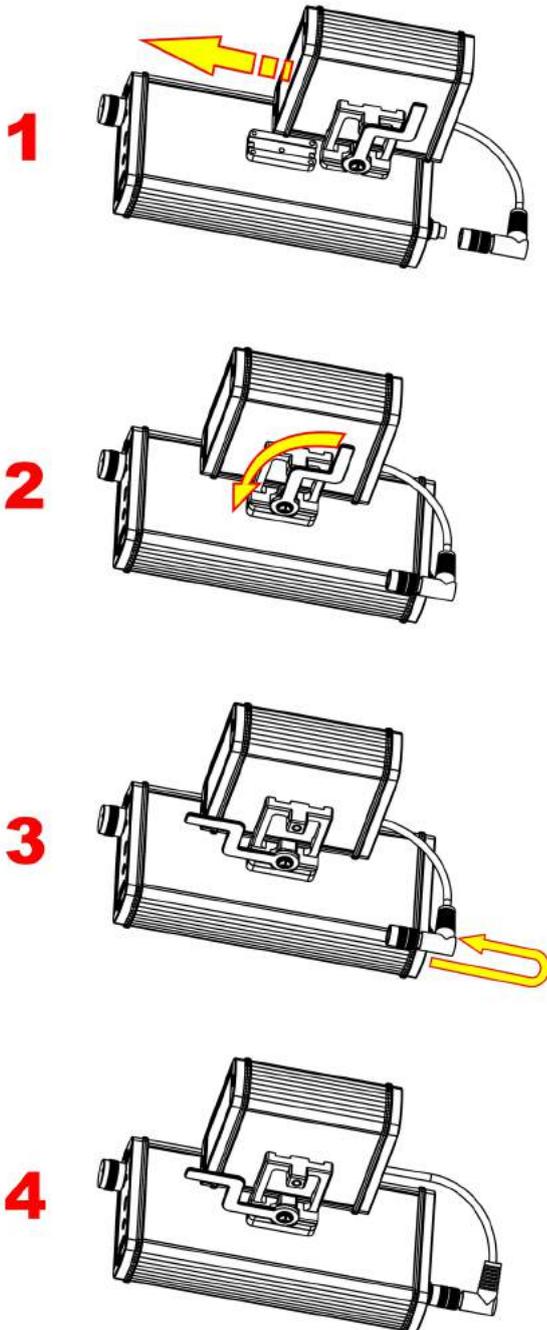


Fig.4

1.3.4 Receiver of the Cable Locator

The Receiver unit is a functionally complete device and has power supply of its own (two 1.5V "AAA" batteries). On the front panel of the unit are control and display elements, and a socket for the contact probe. On the back is the battery compartment lid. The unit has a speaker for sound notifications. The appearance of the Receiver and the locations of its control and display elements are shown in Fig. 5.

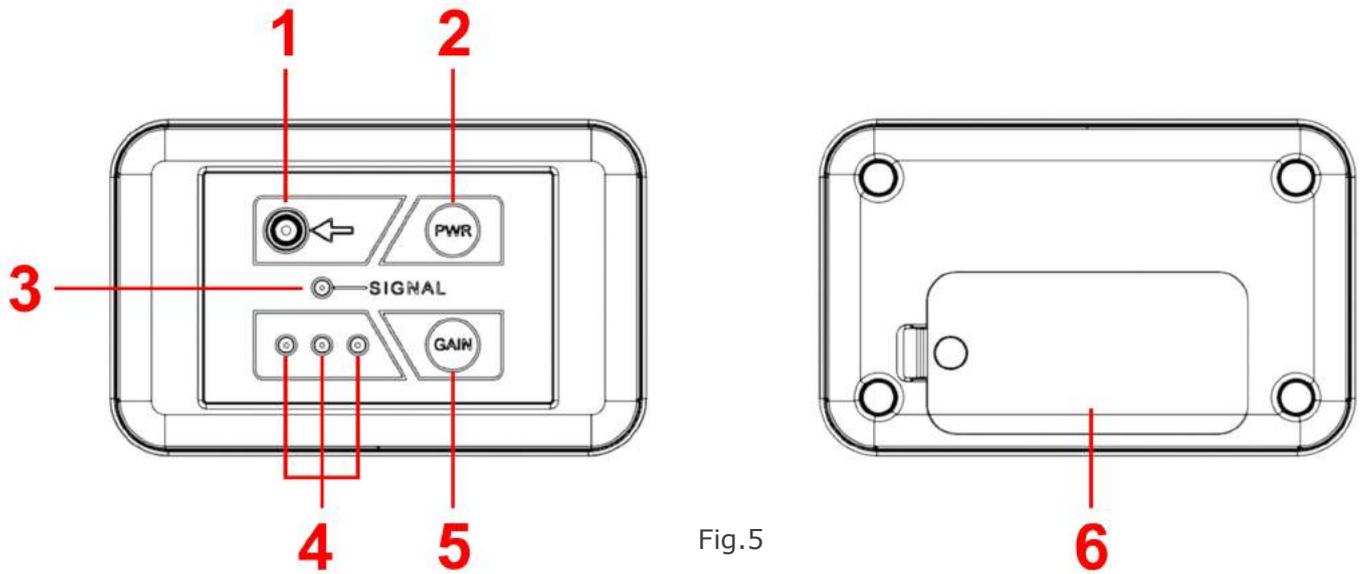


Fig.5

| # in fig. 5 | Sign on Unit | purpose |
|-------------|--------------|--|
| 1 | ⬅ | socket for the probe or telescopic arm plug (for contact testing) |
| 2 | PWR | power on/off; sound on/off |
| 3 | SIGNAL | test signal reception indicator (red LED) |
| 4 | | LED indicator bar showing the receiver sensitivity (minimum/medium/maximum) or indicating critically low battery, with all the three LEDs blinking |
| 5 | GAIN | sensitivity control |
| 6 | | battery compartment lid |

When the Receiver is used in a non-contact search, it is recommendable to use the telescopic arm supplied with ST300. This will, firstly, prevent the user's body capacitance affecting the receiver, and secondly, make it easier to explore the upper walls and ceiling.

The arm consists of a telescopic handle and bracket-and-clamp assembly. The telescopic arm is shown in Fig. 6.

The numbers in Fig. 6 represent:

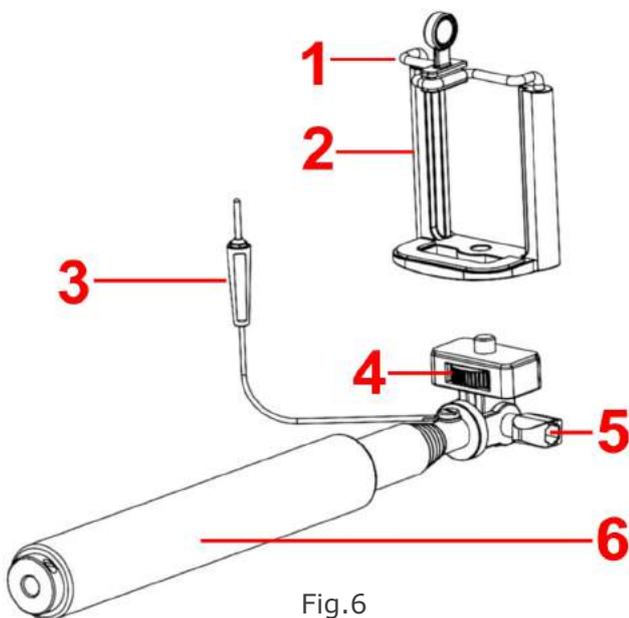


Fig.6

- 1 - hold-down bar
- 2 - bracket
- 3 - cable with a pin connector
- 4 - screw connecting the bracket to the telescopic arm
- 5 - screw that fixes the position (incline) of the bracket
- 6 - telescopic handle

To mount the Receiver onto the telescopic arm and prepare it for operation, pull up the hold-down bar 1, place the Receiver as shown in Fig. 7 and release the hold-down bar.

Plug the pin connector 3 into the corresponding socket of the Main Unit (1, Fig.5).

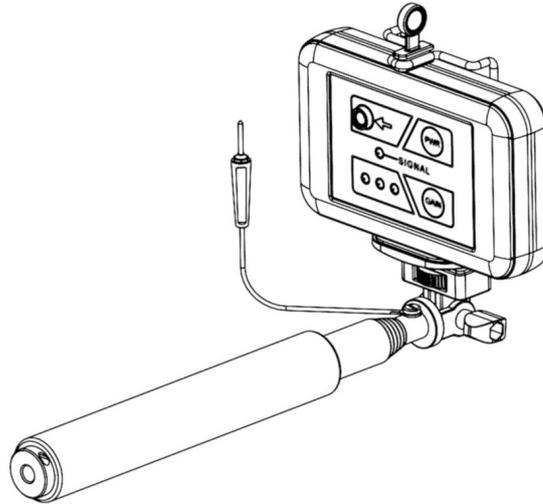


Fig.7

1.3.5 Adaptor for Testing Power Mains

The Mains Adaptor, shown in Fig. 8, is used to connect ST300 to lines with voltages over 100V.

The numbers in Fig. 8 represent:

- 1 - mains cable socket
- 2 - LED indicators of in the line being tested (two lit LEDs for AC, one lit LED for DC)
- 3 - connector for plugging into the Main Unit

For the connection of the Adaptor to a tested line, two mains cables are supplied with ST300. To connect through a standard electric outlet, please use the cable with a plug (1, Fig.9). For testing through a distribution box (contactor panel), please use the one with clamps (2, 3, Fig.9).

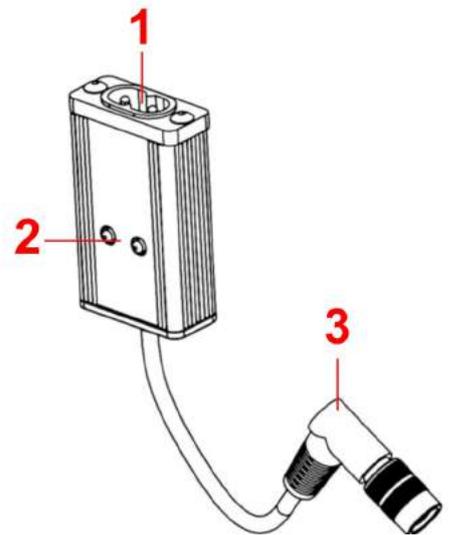


Fig.8

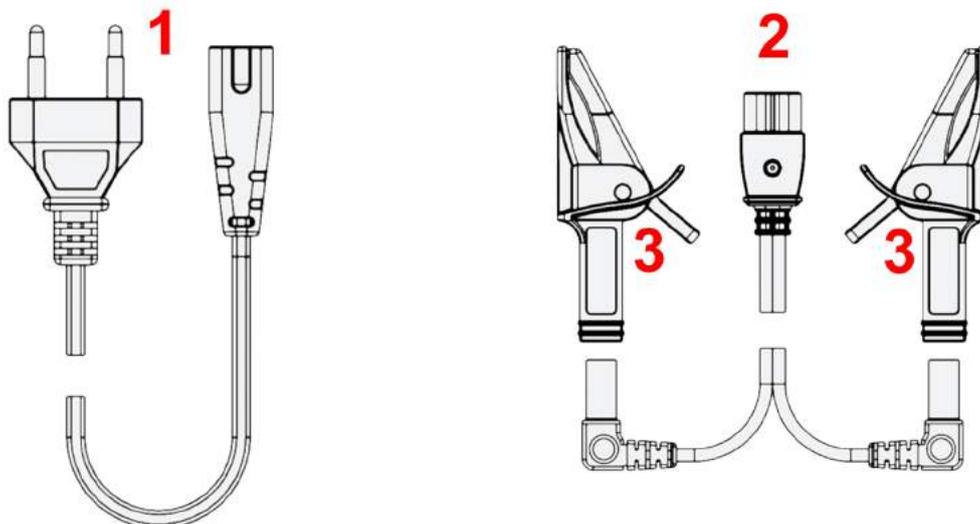


Fig.9

1.3.6 Test sound player

The Test sound player is used for:

- the emission of a known acoustic signal on site (if the sound response from ST300 correlates with the test sound, that means there is an active eavesdropping device around that sends uncoded transmissions);
- forced triggering of voice-activated eavesdropping electronics equipped with VOX;
- locating the detected eavesdropping electronics;
- emission of a masking noise during searches;
- playback from external devices connected via line input.

For these purposes, an MP3 player is supplied with ST300. Using a flash card, the operator may record and play custom signals that are best tailored to his search procedures.

Fig.10 shows the ports and controls of the Test Sound Player:

- 1 – speaker
- 2 – power indicator
- 3 – previous file playback
- 4 – next file playback
- 5 and 6 – volume control
- 7 – “Play/Pause/Stop”
- 8 – power switch
- 9 – headphone socket
- 10 – line input / charger
- 11 – microSD slot

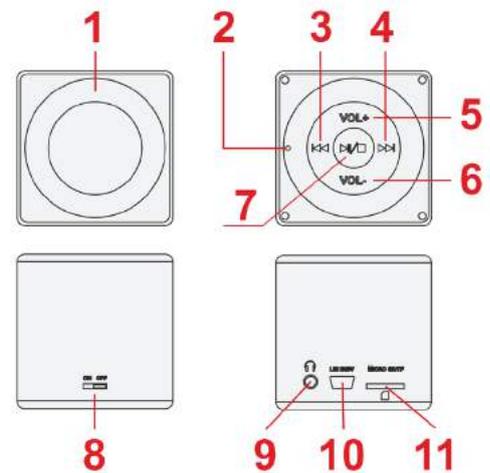


Fig.10

audio file playback:

Copy all the necessary files with test and masking signals to a microSD card. Insert the microSD card into the microSD slot (11, Fig.10). Turn on the MP3 player (8, Fig.10); the power indicator (2, Fig.10) will go on.

using the line input

This can be used for audio playback from ST300. It can also serve for establishing a sound loop with hidden microphones (Larssen effect).

Extract the microSD card from the port (11, Fig.10).

Turn off power (8, Fig.10).

Connect the Test Sound Player to the “PHONE” socket with Cable (6, Fig.2).

Adjust the volume level with buttons (5-6, Fig.10).

charging

The accumulator incorporated in the Test Sound Source is chargeable from a USB-port of a computer through a USB/mini-USB cable.

Connect the miniUSB end of the cable to the Player (10, Fig.10), and the USB end to a computer. If the power switch is in the “OFF” position, the indicator (2, Fig.10) will be shining red while the battery is being charged. The player can also be charged while turned on, with the indicator (2, Fig.10) shining blue; however, the charging time will increase.

2. OPERATION MODES OF ST300

For tackling the various tasks of detecting and locating eavesdropping electronics, ST300 "SPIDER" packs versatile features, both active and passive, and is supplied with a variety of accessories answering these needs.

It is designed and programmed to function in the following modes:

- electronic switch;
- low-frequency amplifier;
- wired receiver;
- wired nonlinear junction detector;
- reflection meter;
- cable locator.

All of these modes are user-activated. ST300 can only operate in one of the main modes at a time.

2.1 STARTUP

The Main Unit of ST300 is turned on and off with the "ON/OFF VOLUME" switch on its right side (4, Fig.2).

Within 1-2 seconds of activation the screen will show:

- manufacturer name and logo;
- name of the device;
- firmware version (Fig.11).

Press any button to go to the Start Menu.



Fig.11

2.2 Start Menu (Mode Selection Menu)

The Start Menu is the point of entry to all the operation modes of ST300.

Attention! If the Electronic Switch is not connected with the Main Unit of ST300, only "WIRED RECEIVER" and "SETTINGS" modes are available.

The appearance of the Start Menu in the absence of the Electronic Switch is shown in Fig. 12.

The numbers in Fig. 12 represent:

- 1 - status bar
- 2 - current mode
- 3 - indication of the selected wire pair (reading "OFF" if the Electronic Switch is not connected)
- 4 - battery status
- 5 - clock (in "hh-mm" format)
- 6 - main area of the display (now listing the available modes)
- 7 - assignment of hotkeys (if the Electronic Switch is not connected, only the "WR" key is available that turns on the "WIRED RECEIVER" mode)

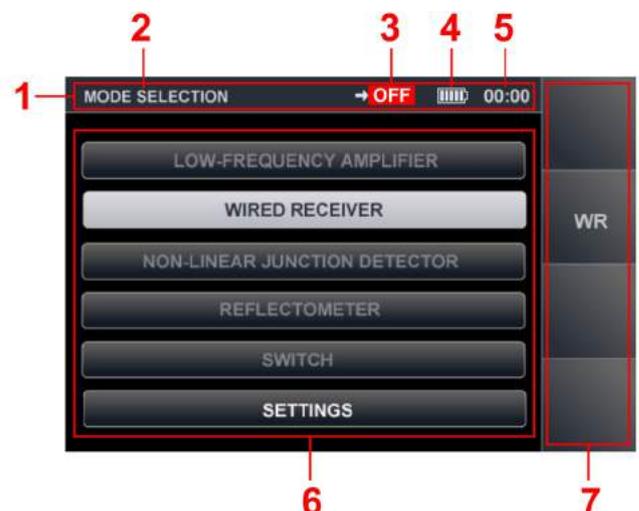


Fig.12

The modes will be shown differently in the main area (6, Fig.12) depending on whether the Switch is connected or not.

Fig.13 shows three possible appearances of the same menu item, depending on the presence or absence of the Electronic Switch, and cursor position:

- 1 – mode unavailable (Electronic Switch not connected)
- 2 – mode available (Electronic Switch connected)
- 3 – highlighted by the cursor

Fig.14 shows the Start Menu, with the Electronic Switch connected to the Main Unit.

The numbers in Fig. 14 match those in Fig.12.

As is seen from the picture, with the Electronic Switch connected to the Main Unit, all the items in the modes list (6, Fig. 14) are available, and so are all the hotkeys (7, Fig 14.).

To select a mode, move the cursor to the corresponding list item using the \uparrow and \downarrow keys, and press "ENTER".

If the Electronic Switch is connected to the Main Unit, and hotkeys are active in the Start Menu (7, Fig.14), use "F1", "F2", "F3" and "F4" for quick access to the modes "LOW FREQUENCY AMPLIFIER", "WIRED RECEIVER", "NONLINEAR JUNCTION DETECTOR", and "REFLECTOMETER", respectively. The keyboard hotkeys are located to the right of the display, next to the corresponding hotkey legends on the screen. The hotkey assignments change depending on the current mode of operation.



Fig.13

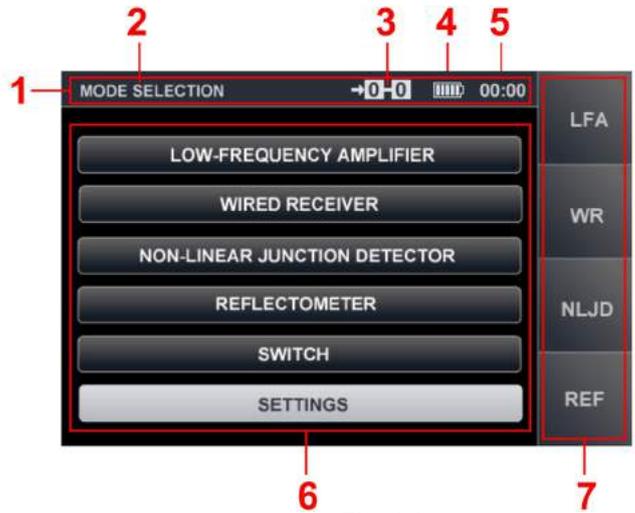


Fig.14

2.3 SETTINGS

The "SETTINGS" mode is always available, regardless of whether the Electronic Switch is connected to the Main Unit or not. In this mode, the date, time, and interface language can be set. To enter the settings, select the menu item using the vertical arrow keys and press "ENTER".

The "SETTINGS" menu is shown in Fig. 15.

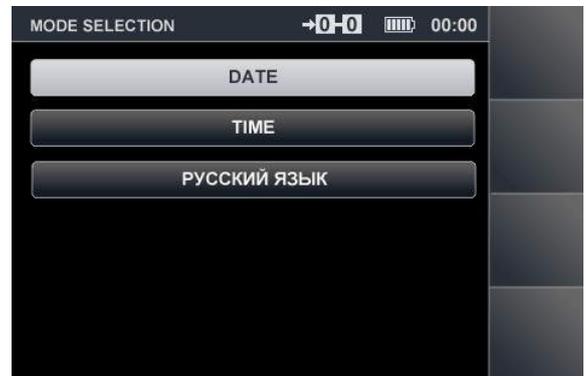


Fig.15

2.3.1 Date Setup

Set the date using the \uparrow and \downarrow keys.

Move the cursor to the "DATE" field and press "ENTER". The date setting menu will appear on the screen (Fig.16), with the date shown in the format "DD-MM-YYYY".

Using the \leftarrow and \rightarrow keys, move the cursor to the "DAY" field.

With the \uparrow and \downarrow keys, set the required value and press "ENTER" to confirm.



Fig.16

Similarly, set the required values for "MONTH" and "YEAR". If "ESC" is pressed before confirming the entered values, they will not be saved, and the device will exit the clock setting mode. All confirmed values will remain in the device's memory on exiting the setting menu, and will stay saved even when the power is switched off.

2.3.2 Time Setup

To set the time, in the "SETTINGS" menu move the cursor to the "TIME" field using the \uparrow and \downarrow keys, and press "ENTER". The time setting menu will appear on the screen (Fig.17), with time shown in the format "HH-MM". Time is set in the same manner as the date (2.3.1). To confirm the selected values, press "ENTER".



Fig.17

To return to "SETTINGS", press "ESC".

2.3.3 Interface Language Setup

To set the language, select "LANGUAGE" in the "SETTINGS" menu using the \uparrow and \downarrow keys, and press "ENTER". The interface language will change from Russian to English. To set Russian, select the menu item "РУССКИЙ ЯЗЫК" and press "ENTER".

Upon setting the language in the "SETTINGS" mode, press "ESC" to return to the Start Menu.

2.4 ELECTRONIC SWITCH CONTROL MODE ("SWITCH")

The "SWITCH" mode is only available when the Electronic Switch is connected to the Main Unit. This mode is intended for testing low-current lines. It allows running tests over all possible two-wire combinations in a multiple-wire cable (up to 8 cores, in the current version).

As the "SWITCH" mode is the main one for testing low-current lines, it is readily accessible from the Start Menu, as well as from "LOW FREQUENCY AMPLIFIER", "WIRED RECEIVER", "NONLINEAR JUNCTION DETECTOR", and "REFLECTOMETER" modes.

2.4.1. Main Screen of the "SWITCH" Mode

To access the "SWITCH" mode from the Start Menu (Fig.18), using the \downarrow and \uparrow keys highlight "SWITCH" and press "ENTER". The main menu of this mode will appear on screen (Fig.18).

The numbers in Fig. 18 represent:

- 1 – current mode
- 2 – wire pair connected to the input of the device
- 3 – wire pair selection
- 4 – red frame highlighting the current menu item that can be adjusted
- 5 – voltage in the selected wire pair (DC and AC)
- 6 – engaged contacts of the Electronic Switch connector (RJ45)
- 7 – hotkey assignments

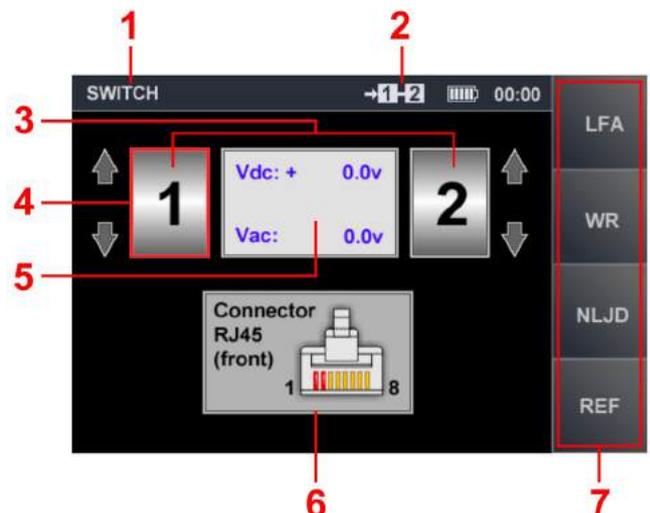


Fig.18

2.4.1.1 Selecting a Wire Pair

To connect a wire pair from the screen of the «SWITCH» mode, do the following:

- using the  and  keys, position the red frame (4 Fig.18) at the left window of the wire pair (3, Fig.18); then, using the  and  keys, set a wire number; now the first wire in the pair is connected;
- using the  and  keys, position the red frame (4 Fig.18) at the right window of the wire pair (3, Fig.18); then, using the  and  keys, set a wire number; now the pair of wires is connected to the device.

Please bear in mind that the selected numbers cannot be the same.

2.4.1.2 Display of Wire Pair Selection

The numbers of the wires connected to the device are shown on display (2, Fig.18) in all the operation modes, until another pair of wires is connected to the device. Also, the RJ45 connector is represented graphically on display (6, Fig.18), with the selected two contacts marked red.

2.4.1.3 Display of Voltage in the Selected Wire Pair

The display shows measurements of the AC and DC voltages in the pair of wires currently connected to ST300 (5, Fig.18).

If a measured value exceeds 3V, the firmware automatically disables any of the active modes ("NONLINEAR JUNCTION DETECTOR", "REFLECTOMETER") or applying a bias voltage in the "LOW FREQUENCY AMPLIFIER" mode. To enable these features, the line under testing must be de-energized.

2.4.1.4 Switching to Other Modes

Switching to other modes from the main "SWITCH" menu can be performed in two ways:

- by pressing "ESC" to return to the Start Menu and activating the necessary mode as described in 2.2;
- by accessing the desired mode directly from the "SWITCH" mode menu using the hotkeys:
 - to "LOW-FREQUENCY AMPLIFIER" – by pressing "F1";
 - to "WIRED RECEIVER" – by pressing "F2";
 - to "NONLINEAR JUNCTION DETECTOR" – by pressing "F3";
 - to "REFLECTOMETER" – by pressing "F4";
 - to "CABLE LOCATOR" submode – by pressing "FUNC";
 - to Automatic Measurement Mode – by pressing "MODE".

2.4.2 Additional Modes

The "SWITCH" mode has two sub-modes, i.e., "AUTOMATIC MEASUREMENT MODE" and "CABLE LOCATOR".

2.4.2.1 Automatic Measurement Mode

This mode is used for automatic measuring of AC and DC voltages on all possible two-wire combinations of the tested multi-core cable.

To activate this sub-mode from the "SWITCH" mode screen, press "MODE". The sub-mode menu (Fig.19) will appear on the screen. In the list of wire pairs, the one selected in the main menu will be highlighted by default. Voltages on these two wires will be measured, and the results shown in the table. Measurements on other two-wire combinations will not be performed.

To measure voltages on all the pairs of wires, press «F4» («Scan All»). The full measurement cycle is a matter of seconds. The measurement results will be shown in the table. If a measurement exceeds 3V, the corresponding line in the table will be marked red. Once the measurement cycle is complete, and all the table lines have filled in with values, further measurements will only be performed on the highlighted pair.

- The figures in Fig. 19 represent:
- 1 – current mode
 - 2 – wire pair currently connected
 - 3 – wire pair column
 - 4 – DC values column
 - 5 – AC values column
 - 6 – cursor
 - 7 – hotkey assignments

Use the arrow keys to navigate the table; the number of the selected wire pair is indicated top of the screen (2, Fig.19). To exit the sub-mode to the "SWITCH" mode screen, press "MODE" or "ESC". The pair of wires highlighted with the cursor before exiting, will remain selected.

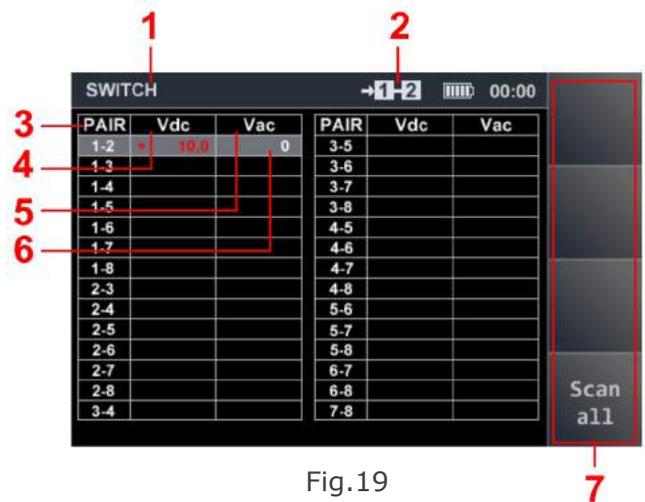


Fig.19

When the automatic measurement mode is activated again, the table will be showing the latest measurements, and the cursor will be set at the pair of wires selected in the main menu. To start a new measurement cycle, press "F4".

2.4.2.2 "CABLE LOCATOR" Mode

This mode serves for tracing cables in walls and other building structures, identifying the tested lines in non-shielded bundles, and finding the junction box contacts to which the line is connected.

Caution! In order to operate ST300 in the cable locator mode, connect its casing to the ground using Cable (26, Fig.1). To do this, plug the one end with the pin plug into the "PHONE" socket (6, Fig.2), and attach the other end equipped with a crocodile clamp, to a ground rod, or grounded casing of any equipment.

This mode is implemented with the aid of a signal generator integrated into ST300 Main Unit, and an autonomous Receiver (1.3.4). The tested line is to be connected to the Main Unit through the Electronic Switch. Upon activation of the cable locator mode, a two-tone test signal is applied to the line. With the aid of the receiver tuned at the test signal frequency, it is possible to trace the cable line behind wall paneling, dropped ceilings, and in cable trunking, in a non-contact manner (registering the electromagnetic radiation around the cable created by the test signal). If contacts in a junction box are to be identified, it is possible to connect the receiver with the tester probe (5, Fig.1) directly to the terminal board.

To activate the Cable Locator mode from the "SWITCH" mode screen, press "FUNC".

The screen will change to "LOCATOR" (Fig.20), and the test signal generator will turn on automatically.

In Fig.20 the numbers represent:

- 1 – current mode
- 2 – sub-mode
- 3 – wire selection for the application of a test signal
- 4 – graphics showing the contact in the RJ45 socket, to which the test signal will be applied (red marking)

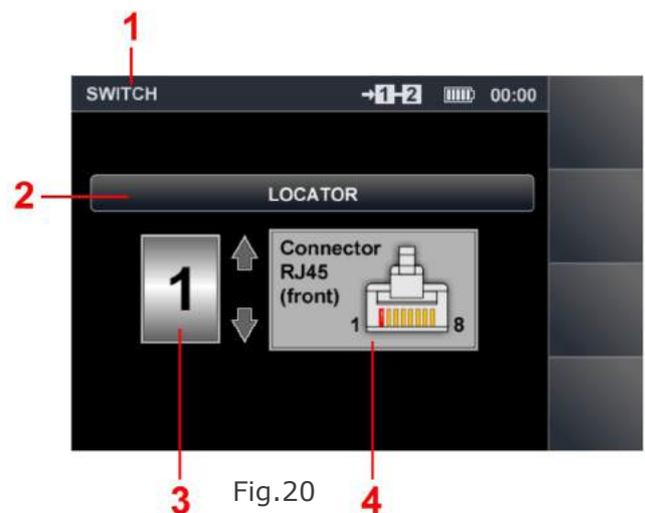


Fig.20

Set the wire number using the \uparrow and \downarrow keys. The selected wire number will be shown in the window (3, Fig.20) and in the graphics (4, Fig.20). The selected pair value in the corresponding field (2, Fig.19) will not change. To exit the mode to the "SWITCH" screen, press "ESC". The test signal generator will stop. All the settings made in the "SWITCH" mode will be saved.

2.5 "LOW FREQUENCY AMPLIFIER" MODE

The "LOW FREQUENCY AMPLIFIER" ("LFA") mode is intended for the detection of,

- low-frequency signals from hard-wired eavesdropping electronics connected to low-current lines;
- acousto-electric conversion ("microphone effect") involving devices that are connected to low current circuits in the inspected room.

In the "LFA" mode, signals can be monitored:

- by their graphical representation on the screen (oscillogram or spectrogram);
- by sound (through headphones or speaker).

2.5.1. Main Screen of the "LFA" Mode

The "LFA" mode only becomes available upon connecting the Main Unit with the Electronic Switch. The mode is accessible from the Start Menu (Fig.18), or from the "SWITCH" mode.

To enter the "LFA" mode from the Start Menu, choose "LOW FREQUENCY AMPLIFIER" using the \uparrow and \downarrow keys, and press "ENTER". In the "LFA" mode, two ways of data representation are implemented, i.e., oscilloscope (Fig.21) and spectrum analyzer (Fig.22). On entering the "LFA" mode, it is "OSCILLOSCOPE" (Fig.21) by default. To toggle between the two forms of representation, press "F4".

In Fig. 21:

- 1 - current mode
- 2 - data representation form
- 3 - time scale value (in μ s or ms)
- 4 - measured signal amplitude
- 5 - vertical scaling of the oscillogram
- 6 - oscilloscopic screen
- 7 - selected gain
- 8 - selected bias voltage
- 9 - hotkey assignment

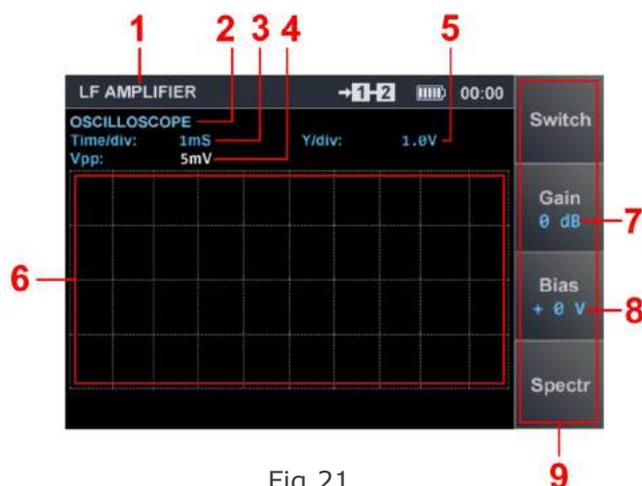


Fig.21

The oscillogram can be scaled horizontally with the \leftarrow and \rightarrow keys, and vertically with the \uparrow and \downarrow keys.

To change data representation to "SPECTRUM ANALYZER", press "F4".

A spectrogram will appear on the screen. Fig. 22 shows the spectrum analyzer in the ultra low frequency mode.

In Fig. 22:

- 1 - current mode
- 2 - data representation form
- 3 - frequency marked by the cursor
- 4 - hairline cursor
- 5 - signal amplitude at the selected frequency
- 6 - spectrum analyzer screen
- 7 - selected gain value
- 8 - selected bias voltage
- 9 - hotkey assignment

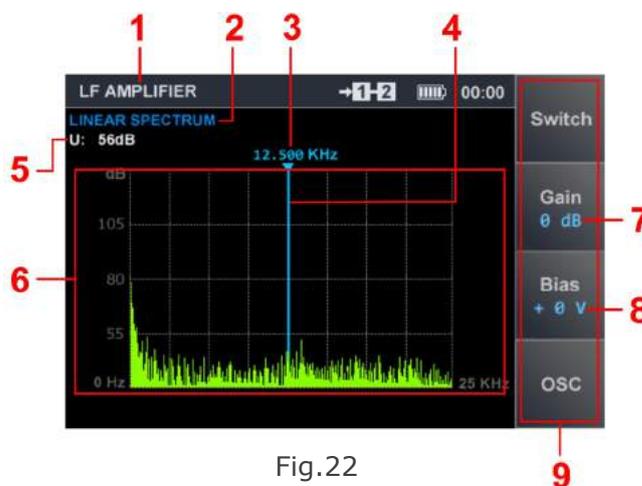


Fig.22

The displayed spectrogram (Fig.22) does not scale and spans over the whole range (0-25kHz). It can be navigated by moving the hairline cursor (4, Fig.22) with the \leftarrow and \rightarrow keys. The current frequency is always shown numerically above the cursor (3, Fig.22).

To change data representation to ("OSCILLOSCOPE"), press "F4".

2.5.1.1. Cable Settings

Before proceeding with «LFA» mode operations, it is necessary to select the appropriate wire pair. This can be done either in the «SWITCH» mode (2.4.1), or in the automated «LFA» mode menu (2.5.2).

If the number of wires has been reduced in the settings, the excluded contact numbers will remain unavailable for selection until the settings are changed.



Fig.23

EXAMPLE

A four-wire cable equipped with a 6P4C modular connector (RJ14/RJ11, see Fig.23) is to be tested. The cable is connected through an adapter to the 8-contact (RJ45) socket of the Electronic Switch. In this case, four contacts of the Electronic Switch input will not be engaged. By applying the corresponding settings, they can be eliminated from the testing procedure, which will reduce the testing time significantly.

To open the cable setting menu from one of the above modes, press "FUNC". The user is offered the following choice of cable types:

- twisted-pair cable (one, two, three, or four pairs);
- any multiwire cable (up to eight wires in a bundle).

Figs. 24-26 show the cable settings menu.

In Fig. 24, twisted-pair cable settings are shown, the numbers representing:

- 1 - twisted-pair cable heading
- 2 - graphics showing the RJ45 input socket of the Electronic Switch (with the engaged contacts marked red and inactive contacts marked black)
- 3-6 - numbers of twisted pairs in cable, with the current selection highlighted white.
- 7 - heading of a straight cable

Fig. 24 represents the connection of a cable comprising four twisted pairs.

For cable settings, use the following controls:

◀ and ▶ keys, for setting the cable type;

⬆ and ⬇ keys, for setting the number of twisted pairs, or cores in a cable; press "ENTER", to confirm selection;

"FUNC" or "ESC", to exit to the main screen.

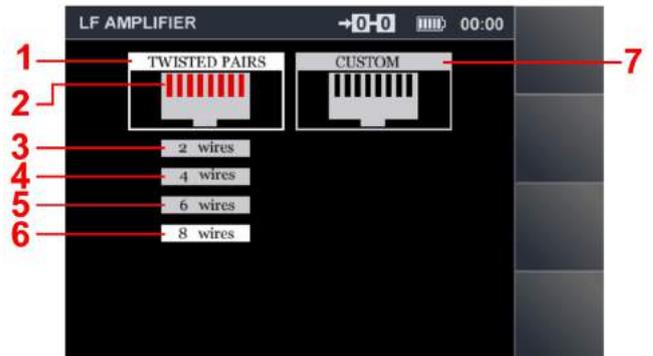


Fig.24

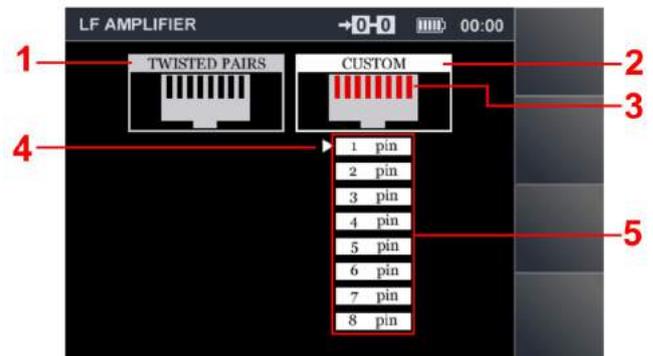


Рис.25

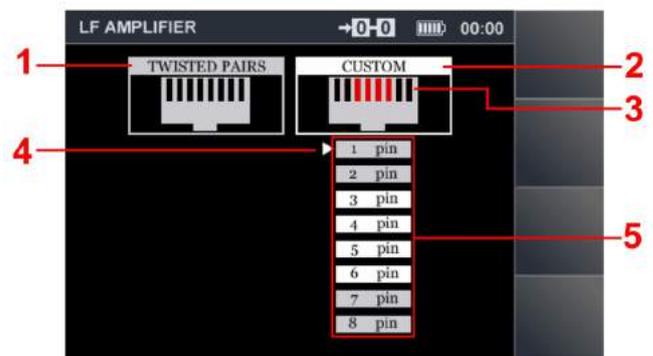


Fig.26

Figs. 25-26 show the menu for entering straight cable settings. The numbers in Figs. 25-26:

- 1 – twisted-pair cable heading (in Figs. 25-26, deselected)
- 2 – straight cable heading (in Figs. 25-26, active)
- 3 – graphics showing the RJ45 input socket of the Electronic Switch (with the engaged contacts marked red and inactive contacts marked black)
- 4 – current cursor position, where the values can be adjusted – graphics showing the RJ45 input socket of the Electronic Switch (with the engaged contacts marked red and inactive ones marked black); the numbering of wires corresponds to that of the RJ45 contacts

Fig. 25 shows the connection of a straight cable consisting of eight wires (all the RJ45 contacts engaged).

Fig. 26 shows the connection of a straight cable consisting of four wires and equipped with a 6P4C connector (standard telephone cable). Only the 4 central contacts (Nos. 3, 4, 5, 6) of the Electronic Switch socket are engaged.

Before “LFA” mode operations, it is necessary to select the appropriate wire pair. This can be done either in the “SWITCH” mode (2.4.1.), or in the automated “LFA” mode menu (2.5.2). If the number of wires has been reduced in the settings, the excluded contact numbers will remain unavailable for selection until the settings are changed.

EXAMPLE

A straight four-wire cable is to be tested. The settings are chosen as shown in Fig. 26, with only the 4 central contacts of the Electronic Switch socket are engaged. In this case, the following wire combinations will be available for connection: 3-4; 3-5; 3-6; 4-5; 4-6; 5-6.

2.5.1.2. Gain Control

To set the necessary gain in the main screen of the “LFA” mode:

- press “F2” (the “GAIN” button will be highlighted, and gain control will become available);
- with the  and  keys set the required gain; the adjusted value will be shown on display (7, Fig. 21; 7, Fig.22);
- press “F2” (the button will darken, indicating that gain control is no longer available).

The set gain value will remain unchanged until it is adjusted again or the device is turned off.

2.5.1.3. Setting a Bias Voltage

To apply a bias voltage to the tested pair of wires, while in the main screen of the “LFA” mode:

- press “F3” (the “Bias” button will be highlighted, and bias voltage adjustment will become available);
- set the required bias voltage with the  and  keys; the adjusted value will be shown on display (8, Fig. 21; 8, Fig.22);
- if need be, toggle the sign of bias voltage with the  and  buttons;
- to instantly set bias voltage to 0, press “ENTER”;
- press “F3” (the button will darken indicating that bias voltage adjustment is no longer possible).

For tasks involving bias voltages, the gain is limited at 25dB. If the gain was previously set above 25dB, it will be automatically reduced to 25dB when a bias voltage is applied to the line.

If the voltage on a tested pair of wires is beyond +/-3V, the application of bias voltage to this pair will be blocked. The “F3” hotkey will look as follows:



To apply a bias voltage in such case, it will be necessary to disconnect the cable in question from the power source.

Once set, the bias voltage value will remain the same until it is adjusted or the device is turned off.

2.5.1.4. Switching to Other Modes

“ESC” – exit from the “LFA” mode to the Start Menu.

“F1” – go to the “SWITCH” mode.

“FUNC” – go to the cable settings menu.

“MODE” – go to the automated “LFA” mode.

2.5.2. Automatic Mode of the LF Amplifier

To optimize the testing procedure, an automatic routine is available in the “LFA” mode (the automated “LFA” mode). This allows testing all the possible two-wire combinations in a multiwire cable without exiting to the main screen of the “SWITCH” mode. The gain and bias voltage values for each pair will remain as previously set in the main menu.

To go to the automatic mode from the main menu of “LFA”, press “MODE”.

The menu of the automated “LFA” mode is shown in Fig. 27.

The numbers in Fig.27 represent:

- 1 – current mode
- 2 – selected wire pair
- 3 – wire pairs column
- 4 – constant voltages column
- 5 – alternating voltages column
- 6 – table cursor
- 7 – selected gain value
- 8 – selected bias voltage value
- 9 – hotkey assignment

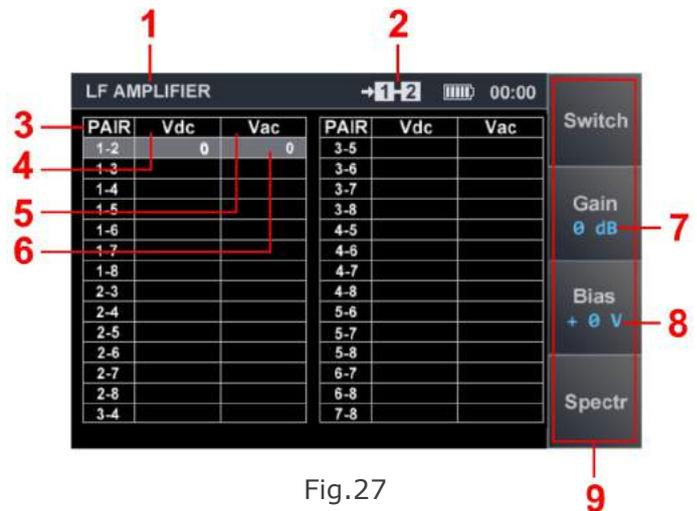


Fig.27

Use the arrow keys to navigate the table.

When a pair of wires is selected by moving the table cursor to the corresponding table line, the Electronic Switch will automatically connect this pair through to the Main Unit’s input. The Main Unit will then measure the voltage on this pair of wires, and the result will be entered in the table. If a DC or AC voltage measured on a pair exceeds 3V in absolute value, the bias voltage, if set, will not be applied to the line.

The hotkey field (8, pic 23) will look in this case as follows:



The corresponding table entry will read, **>3V**.

To apply a bias voltage in such case, it will be necessary to disconnect the cable in question from the power source. The gain and bias voltage are to be set as described in 2.5.1.2 and 2.5.1.3, respectively.

For automatic testing over all two-wire possible combinations in a multiwire cable, press “F4” (“Scan All”). The device will be testing all the two-wire combinations consecutively, pausing at each pair for a few seconds, so the user can analyze the sound output.

While in this routine, at any moment the table cursor will be highlighting the pair that is currently being tested. When the cycle is complete, the table cursor will return to its starting position (where it had been before the automatic procedure was engaged).

For signal monitoring, headphones or inbuilt speaker can be used.

For a more detailed research, the user may go the main screen of the "LFA" mode, by pressing "MODE" or "ESC". The signal may then be studied with the oscilloscope or spectrum analyzer. To return to the automatic mode table view, press "MODE".

2.6 "WIRED RECEIVER" MODE

The "WIRED RECEIVER" mode ("WR") serves for the detection of signals from eavesdropping electronics, transmitting over both high- and weak-current lines in the frequency range from 100kHz to 150MHz.

In the "WR" mode, signals can be monitored:

- by their graphical representation on the screen (oscillogram or spectrogram);
- by sound (through headphones or speaker).

For connecting the device to electric mains, a special adaptor is supplied with ST300 (see 1.3.5). For connection to weak-current multiwire, the Electronic Switch is used. If the weak-current line is two-wired, using the mains adaptor (1.3.5) is also acceptable.

When the mains adaptor is used for connection, the message OFF appears instead of the pair number.

If the Electronic Switch is used for connection, the wire pair number is shown in its usual place: 1-2

Caution! Connecting the Electronic Switch to live power mains is strictly forbidden and will result in damaging the Electronic Switch!

2.6.1 Main Screen of the "WIRED RECEIVER" Mode

The "WR" mode is accessible:

- from the Start Menu (see 2.2), by using the "F2" hotkey or through the menu;
- from the main screen of the "SWITCH" mode (see 2.4.1.), by using the "F2" hotkey.

Upon activation of the "WR" mode the user is offered a choice of two frequency ranges, i.e., 100kHz - 30MHz or 100kHz - 150MHz. Using the ∇ and \triangle keys, select one and press "ENTER". The main screen of the «WIRED RECEIVER» mode will appear (Fig. 28), with the spectrum over the selected frequency range.

In Fig. 28:

- 1 - current mode
- 2 - frequency marked by the cursor
- 3 - hairline cursor
- 4 - wire pair connected
- 5 - signal amplitude at the selected frequency
- 6 - previously measured spectrum (green)
- 7 - peak signal amplitude over all cycles at the given frequency (dark red)
- 8 - band segment relative to full band
- 9 - lower and upper limits of the selected frequency segment
- 10 - hotkey assignments

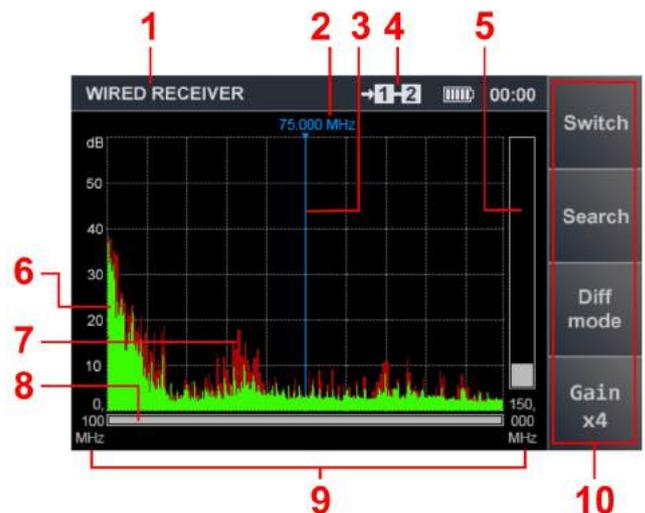


Fig.28

The graph is constantly updated, and can be scaled horizontally for a closer scrutiny of segments of interest. For scaling, position the hairline cursor using the  and  keys, at the signal of choice (or at the centre of the required segment); then, using the  key, narrow down the frequency range to be viewed. The selected frequency range segment is indicated both numerically (9, Fig.28) and graphically (8, Fig.28). Please bear in mind, that peak signal data ("dark red" spectrum) will not be saved when the viewed segment is changed.

For reverse scaling (expanding the range), use the  key. The monitored frequency range will be centered on the hairline cursor position.

If need be, the user can change the receiver gain, selecting one of the three available options (x1, x2, x4). The current gain value is shown one the "GAIN" hotkey graphic (10, Fig.28).

With the Electronic Switch connected to the Main Unit, the "SWITCH" mode can be accessed from the main menu of the "WR" mode. This allows engaging a different pair of wires (if a multiwire cable is being tested) or entering other operation modes of ST300 ("LOW FREQUENCY AMPLIFIER", "NONLINEAR JUNCTION DETECTOR" and "REFLECTOMETER").

Upon return to the "WR" mode from the abovementioned modes through the main screen of the "SWITCH" mode, all the previous receiver settings (viewed frequency range, and gain) will be retained. Upon return to the Start Menu (2.2), settings made in the "WR" mode will be discarded.

The following actions and controls are available in the main menu of the "WR" mode:

"ESC" – exit to the Start Menu

"F1" – exit to the "SWITCH" mode (if the Electronic Switch is connected)

"F2" – automatic mode activation

"F3" – differential mode activation

"F4" – receiver gain adjustment

"ENTER" – activation of monitoring at a set frequency

  – hairline cursor positioning

  – decreasing/ expanding frequency range

2.6.2 Differential Wired Receiver Mode

In this mode, signals levels registered during the previous cycles are set as the zero baseline, and current levels only in excess of that baseline are displayed. Thus, the operator is presented with a differential spectrum. The differential mode can be useful while searching, to get external interference out of the way.

Fig.29 shows the display in the WR differential mode. In Fig. 29:

- 1 – current mode
- 2 – wire pair connected
- 3 – differential mode indication
- 4 – signal amplitude at the selected frequency
- 5 – frequency marked by the cursor
- 6 – hairline cursor
- 7 – peak signal amplitude over all cycles at the given frequency (dark red)
- 8 – differential spectrum (purple)
- 9 – band segment relative to full band

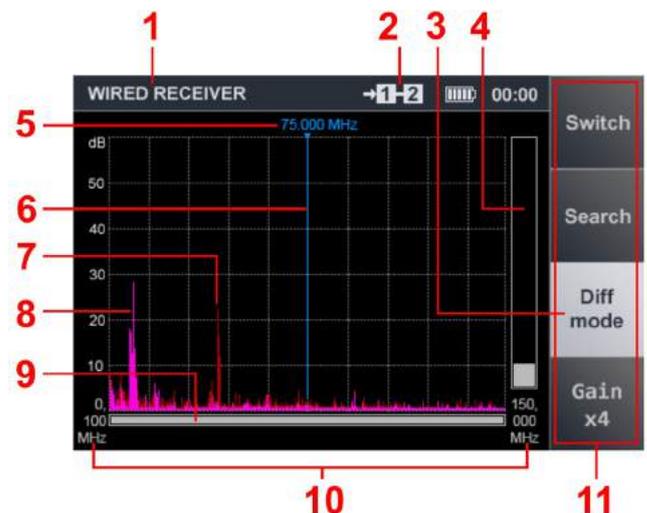


Fig.29

- 10 – lower and upper limits of the selected frequency segment
- 11 – hotkey assignments

Upon activation of the differential mode, the frequency segment setting and gain setting made in the main menu of the "WR" mode will be retained. Signal peak data (dark red spectrum) will not be saved.

In the differential mode all the features of the receiver main menu are available, i.e., access to the Main Menu and the "SWITCH" mode, gain control and the adjustment of the frequency segment width, activation of signal monitoring at a set frequency and automated search.

Please bear in mind, that upon exit from the receiver differential mode to the Main Menu (2.2.), any settings made in the "WR" mode will be discarded.

Upon exit from the differential mode to the "SWITCH" mode ("F1" key) and then return to the "WR" mode ("F2" key), the main screen of the "WIRED RECEIVER" mode will be displayed (and not the differential mode screen).

To deactivate differential mode, press "F3". The "Diff mode" hotkey on display will be deselected. The settings of the frequency segment and gain, made in the differential mode, will be saved.

2.6.3 Monitoring Signal at a Set Frequency

This mode is intended for a detailed evaluation of signals detected in the overview modes (2.6.1-2.6.2). Monitoring at a set frequency allows listening to the demodulated signal, and analyzing it with the oscilloscope.

Monitoring at a given frequency is accessible from the main menu of the "WR" mode, and from the differential mode.

To activate the set frequency mode from the main "WR" menu, set the hairline cursor at the signal of interest using the \leftarrow and \rightarrow keys, and press "ENTER".

In Fig.30, the display is shown in the set frequency mode, the numbers representing:



Fig.30

- 1 – current mode
- 2 – wire pair connected
- 3 – signal amplitude at the selected frequency
- 4 – frequency selected with the cursor
- 5 – hairline cursor
- 6 – results of the previous scanning (grey)
- 7 – peak signal amplitude over all cycles at the given frequency (dark red)
- 8 – band segment relative to full band
- 9 – lower and upper limits of the selected frequency segment
- 10 – hotkey assignments

The actions and controls during signal monitoring at a set frequency:

- \leftarrow \rightarrow – receiver frequency tuning
- "F1" – exit to the "SWITCH" mode (if the Electronic Switch is connected)
- "F2" – toggle modulation type (AM/FM)
- "F3" – activate oscilloscope
- "F4" – set receiver gain
- "ENTER" and "ESC" – exit to the main screen of the "WIRED RECEIVER" mode

Upon exit from the set frequency monitoring mode to the "SWITCH" mode and then return to the "WR" mode, the main menu of the "WIRED RECEIVER" mode will be displayed (and not the set frequency monitoring menu). The settings of the frequency segment and gain, made previously, will be saved.

2.6.4 "OSCILLOSCOPE" Mode

A demodulated signal monitored at a set frequency can be analyzed in the "OSCILLOSCOPE" mode. To that end, press "F3" while in the mode of monitoring at a set frequency. The "OSC" hotkey field will be highlighted.

The display appearance in the "OSCILLOSCOPE" mode is shown in Fig. 31, where the numbers signify:

- 1 – current mode
- 2 – wire pair connected
- 3 – "OSCILLOSCOPE" ON indication
- 4 – hotkey assignments
- 5 – time scale value (in μ s or ms)

Controls in the "OSCILLOSCOPE" mode:

- ◀▶ - horizontal scaling (with time scale value displayed: 5, Fig.31)
- "F1" – exit to the "SWITCH" mode (if the Electronic Switch is connected)
- "F2" – toggle modulation type (AM/FM)
- "ESC" and "F3" – deactivate the oscilloscope
- "F4" – set receiver gain

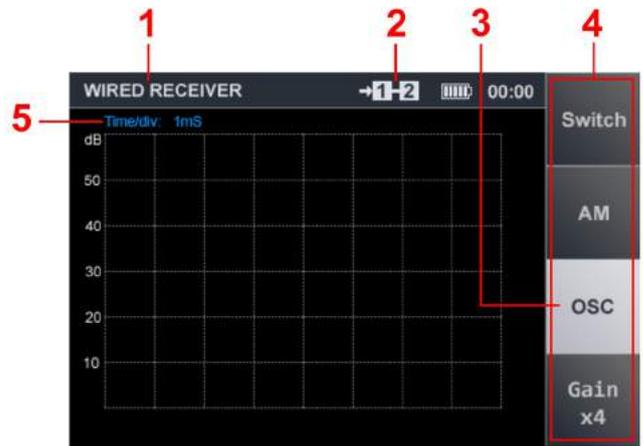


Fig.31

2.6.5 Automatic Mode of the Wired Receiver

In the automatic mode, the wired receiver registers all the signals whose amplitudes exceed the adaptive threshold of detection.

Important! The search is conducted within the frequency segment set by the user, and based on the results obtained in the differential mode (if the automatic mode was entered into from the differential mode).

The automatic mode can be activated from the main menu of the "WR" mode, and from the differential mode menu, by pressing "MODE".

A table will appear, shown in Fig. 32, where the numbers represent:

- 1 – current mode
- 2 – number of signals detected
- 3 – wire pair connected
- 4 – table cursor
- 5 – position of the detected signal in the list
- 6 – frequency of the detected signal (MHz)
- 7 – relative magnitude of the detected signal (dB)
- 8 – bar showing the table cursor position as related to the total number of table lines
- 9 – signal magnitude bar
- 10 – hotkey assignments

Actions and controls in the automatic mode:

"ENTER" – activate monitoring at a set frequency

◀▶ ◀ ▶ - navigate the table

- "F1" – exit to the "SWITCH" mode (if the Electronic Switch is connected)
- "F2" – toggle modulation type (AM/FM)
- "F3" – activate the oscilloscope
- "F4" – set receiver gain
- "ESC" – exit to the previous screen



Fig.32

OPERATING MANUAL

For a more detailed analysis of the detected signal in the automatic mode, it can be monitored at a set frequency. To do that, select the signal in question by moving the table cursor to the corresponding line, and press "ENTER".

Fig. 33 shows the display while monitoring signals at a set frequency in the automatic mode. The font in the highlighted table line (5-7, Fig.29) will change color from white to green. The signal magnitude bar (9, Fig.33) will change color from grey to green.

Actions and controls during set frequency monitoring in the automatic mode:

"ENTER" – activate/deactivate set frequency monitoring

⬆️ ⬇️ – navigate the table

⬅️ ➡️ – receiver frequency tuning

"F1" – exit to the "SWITCH" mode (if the Electronic Switch is connected)

"F2" – toggle modulation type (AM/FM)

"F3" – activate the oscilloscope

"F4" – set receiver gain

"ESC" – exit to the previous screen.



Fig.33

2.7 "NONLINEAR JUNCTION DETECTOR" MODE

This mode serves for the detection of electronics illicitly connected to the tested cable line. The "NONLINEAR JUNCTION DETECTOR" feature reveals both active and inactive (turned off, inoperative, etc.) hard-wired eavesdropping devices in electric contact with the tested line, planted both within the inspected room or facility, and beyond.

The operating principle of a wired nonlinear junction detector (such as implemented in ST300) is in many ways similar to that of an ordinary nonlinear junction detector. Utilizing a built-in transmitter, ST300 sends a probing signal through the tested line. The device's receiver registers the reflected signals at the 2nd and 3rd harmonic frequencies.

Theoretically, the absence of a response at these frequencies should mean that there are no electronics planted on the line in question, while the presence of a response indicates that there are non-linear anomalies. Moreover, if the response level at the 2nd harmonic frequency is higher than the 3rd, there is a high likelihood that an electronic device is connected to the line. If, on the other hand, the level at the 3rd harmonic frequency is greater than at the 2nd, a metal-oxide-metal structure (MOM) is likely: most probably, burnt contacts or a twisted wire connection.

In practice, one rarely gets a clear and unambiguous picture, with signals either at the 2nd or the 3rd harmonic frequency only. As a rule, if there are nonlinear junctions, both signals will be in evidence. For that reason, any kind of response at the 2nd and 3rd harmonics is a serious alert, no matter which signal of the two is stronger.

The nonlinear junction detector of ST300 can be controlled both manually and automatically.

The manual NLJD mode is mostly used for testing two-wire cables, or studying the graphics on a particular pair after a multiwire cable has been scanned in the automatic mode.

For testing multiple-wire cable, the automatic use of NLJD is advisable.

For a proper use of the nonlinear junction detector of ST300, all the telephony equipment and other conventional electronics must be disconnected from the line to be tested.

2.7.1 Main Screen of the "NLJD" Mode (Manual Mode)

The nonlinear junction detector can be controlled manually from the main screen of the mode. The mode is accessible:

- from the Start Menu, through the menu or by pressing "F3" (2.2)
- from the main screen of the "SWITCH" mode, by pressing "F3" (2.4.1).

The main screen of the "NONLINEAR JUNCTION DETECTOR" mode is shown in Fig. 34.

In Fig. 34:

- 1 - current mode
- 2 - wire pair connected
- 3 - current assignment of F1 hotkey
- 4 - bar showing the set magnitude of the probing signal
- 5 - response at the frequency of the probing signal
- 6 - response at the second harmonic frequency of the probing signal
- 7 - response at the third harmonic frequency of the probing signal



Fig.34

Main menu controls:

- ⬆️⬆️ - increase/decrease magnitude of the probing signal
- "MODE" - activate automated nonlinear junction detector mode
- "FUNC" - set cable type
- "F1" - exit to "SWITCH" mode
- "ESC" - exit to Start Menu

As there can be both parallel and series connections of illicit devices, each pair of wires analyzed with the NLJD is to be tested in two states:

- open-circuited at the 'far' end: search for parallel connections;
- short-circuited at the 'far' end: search for series connections.

For short-circuit testing of multiwire cables equipped with an RJ45 socket, a Short-Circuiter socket (23, Fig.1) supplied with ST300 is to be used. If voltage applied to a selected wire pair is beyond +/-3V, the pair cannot be tested in the nonlinear junction detector mode. The presence of excessive voltage is indicated by the sign **→OVER** in place of the selected pair number (2, Fig.34). To proceed with testing, disconnect the cable from the power source (de-energize the tested circuit).

2.7.1.1 Cable Settings

For cable settings, press "FUNC". The procedure of setting the cable type and number of connected wires is identical to the one described in 2.5.1.1. To exit cable settings to the main screen of the "NONLINEAR JUNCTION DETECTOR" mode, press "ESC" or "FUNC".

2.7.2 Automatic Mode of the Nonlinear Junction Detector

In the automatic mode of the nonlinear junction detector, the data are displayed in table form, where opposite each wire pair are dynamic bar graphs showing the responses at the second and third harmonic frequencies of the probing signal. Thus the user can see the full picture of possible nonlinearities on all the two-wire combinations in the multiwire cable.

To switch from manual control of the NLJD to automatic control, press "MODE".

The device's display in the automatic NLJD mode is shown in Fig. 35.

The numbers in Fig. 35 represent:

- 1 – current mode
- 2 – wire pair connected
- 3 – wire pairs column
- 4 – graphics showing relative response levels at the second (red) and third (blue) harmonic frequencies of the probing signal (similarly to 5-6, Fig.34)
- 5 – table cursor
- 6 – current assignment of F4 hotkey

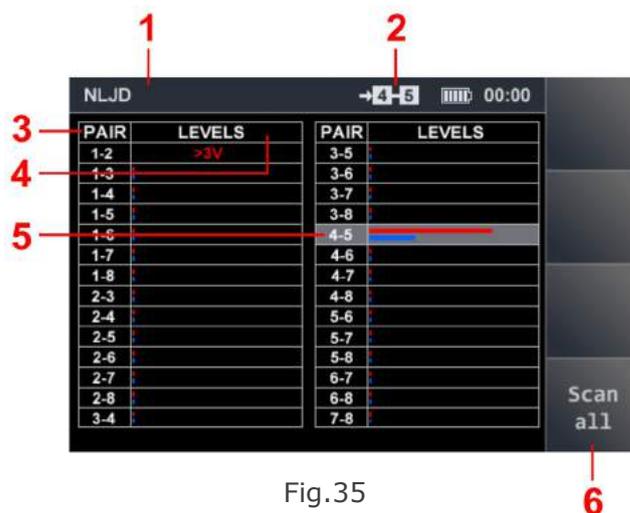


Fig.35

While in the automatic mode, the probing signal magnitude cannot be changed; it will be used as set previously in the manual mode.

When the automatic mode is entered, the selection of wire pair remains the same as in the manual mode; testing results for other pairs are not shown. To move the table cursor, use the keys.

2.7.2.1 Cable Settings

For cable settings, press "FUNC". The procedure of setting the cable type and number of connected wires is identical to the one described in 2.5.1.1. To exit cable settings to the main screen of the "NONLINEAR JUNCTION DETECTOR" mode, press "ESC" or "FUNC".

2.7.2.2 Automatic Scanning

To start automatic testing of all the possible wire combinations, press "F4" ("Scan All"). When the cycle is complete, the "LEVELS" column will be filled with graphic data.

If the voltage in a pair exceeds 3V in absolute value, the corresponding entry in "LEVELS" column will read, ">3V", and the pair in question will not be tested. If the table cursor is positioned at this line, the sign will appear in place of the selected pair number (2, Fig.35).

In this event, to proceed with testing, disconnect the cable from the power source (de-energize the tested circuit).

For the detection of series connections, the line must be short-circuited. For short-circuit testing of multiwire cables equipped with an RJ45 socket, the Short Circuiter (23, Fig.1) supplied with ST300 is to be used.

To exit from the automatic mode of NLJD control to the manual mode, press "MODE" or "ESC". Upon exit, the highlighted pair number will be retained as current.

2.8 "REFLECTOMETER" MODE

The "REFLECTOMETER" mode of ST300 serves for testing double- and multiple-wire cable with the purpose of detecting unsolicited electric (galvanic) connections and defects (e.g., twisted connections). The search method is based on transmitting a sinusoidal signal, that is reflected from a defect or anomaly and returns with a delay, its phase different from the initial signal. The procedure is repeated at multiple frequencies, resulting in a spectrum with alternating peaks, showing the distance to a defect in the tested cable. ST300 can determine said distance with a +/-0.5m precision.

As with any reflection meter, the precision depends on how correctly the velocity factor is set. Velocity factor (VF) is a characteristic of conductive media that indicates how much more slowly an electromagnetic wave travels in the medium than does light in vacuum, and depends on the specifics of the conductive line, i.e., its cross-section and the electric properties of its materials (capacitance and inductivity per length).

The velocity factor for a given cable can be found in special reference directories, cable passport, or online. Please bear in mind that ST300 programming utilizes the reciprocal value of the velocity factor!

For proper use of the reflection meter of ST300, any known devices must be disconnected from the circuit, so the cable only is tested. Both ends of the cable must be accessible, and wires must not be short-circuited at the far end. If the line in question has ramifications, it must be tested segment by segment.

2.8.1. Main Screen of the "REFLECTOMETER" Mode

The "REFLECTOMETER" mode can be activated from the Start Menu (2.2) or from the main screen the "SWITCH" mode (2.4.1). The main screen of the "REFLECTOMETER" mode is shown in Fig. 36.

In Fig. 36:

- 1 – current mode
- 2 – wire pair connected
- 3 – table of measurements #1 ("Set 1")
- 4 – table of measurements #2 ("Set 2")
- 5 – hotkey assignments

Two tables are displayed on the screen. The user can perform two consecutive measurement cycles and compare the results. Grey highlighting of the table fields means that the table is active (available for measurements).

Using the two tables is convenient when testing two pairs in one multiple-wire cable, or two different twin-wire cables, or testing one pair of wires from the opposite ends.

The reflection meter mode requires the connection of two wires. If one of the pair is not connected, the wire number will be shown as 0 (see 2, Fig. 36; both zeroes indicate that neither is connected; measurements on such a pair will not be taken, and the corresponding cell in the active table will read, "No defects". The message "No data" in the table means that the table is inactive, and no measurements have yet been performed.

Fig.37 shows the main screen of the "REFLECTOMETER" mode, with two wires connected.

In Fig. 37:

- 1 – current mode
- 2 – wire pair connected
- 3 – table line numbers
- 4 – distance to a detected defect (irregularity)
- 5 – level of the signal reflected from the defect (irregularity)
- 6 – table of measurements #2 (inactive)
- 7 – hotkey assignments

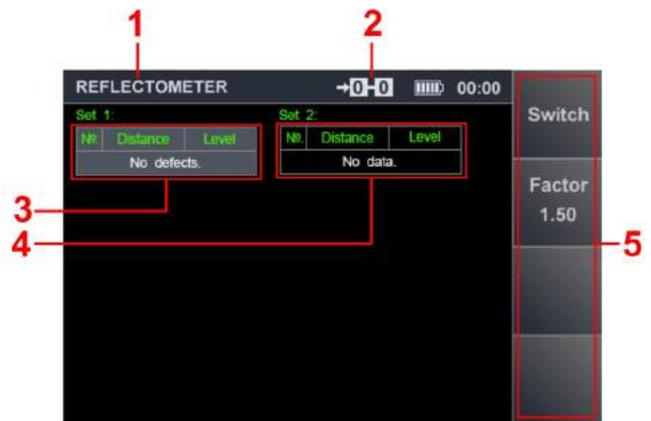


Fig.36



Fig.37

Controls in the "REFLECTOMETER" mode:

- ◀▶ – table selection
- "ENTER" – start a new measurement cycle in the active table
- "F1" – exit to the "SWITCH" mode
- "ESC" – exit to the Start Menu
- "F2" – set reciprocal velocity factor
- "FUNC" – go to the cable setting menu
- "MODE" – go to the automatic mode

If voltage in the connected wire pair is beyond +/-3V, the pair cannot be tested in the reflection meter mode. The presence of excessive voltage is indicated by the sign **→ OVER** in place of the selected pair number (2, Fig.37). To proceed with testing, disconnect the cable from the power source (de-energize the tested circuit).

2.8.1.1 Setting the Velocity Factor (Inverse Value)

A reciprocal value of the velocity factor is used throughout. By default it is set at 1.5 (so the velocity factor equals approximately 0.66, which corresponds to an SQR-2 type cable).

To set a different reciprocal of the velocity factor, press "F2" (Fig.38).

Use the ◀▶ and ▶▶ keys to change the digit position, and the ⏏ and ⏏ keys to adjust the value. To return to the main screen, press "F2", "ESC" or "ENTER".

The new reciprocal of the velocity factor will be shown as the subscript of the "F2" hotkey (7, Fig.37).



Fig.38

For any known value of velocity factor (VF) found in reference sources and sometimes given in percentages, the reciprocal (1/VF) is to be used, which should always be >1. For instance, if VF = 66 percent, the calculation is 1/0.66, which is approximately equal to 1.5.

2.8.1.2 Cable Settings

To set the type of cable, press "FUNC". Proceed to set the cable type and the number of wires connected, in the same manner as described in 2.5.1.1. To exit from the cable settings menu to the main screen of the "REFLECTOMETER" mode, press "ESC" or "FUNC".

2.8.1.3 Measurements in the Main Screen

Before starting measurements, set the pair of wires to be tested. This can be done in the "SWITCH" mode (2.4.1), or using the table view in the "REFLECTOMETER" mode (2.8.2), or in other modes with a similar option. Cable type and the number of cores are also to be indicated (2.8.1.2). It is important that the numbers of wires selected for testing are not excluded as a result of an erroneous setting, otherwise no measurements will be taken, and the active table will read "No defects".

The measurement cycle will start automatically on entering the main screen of the "REFLECTOMETER" mode. During the measurement cycle which may take up to 15 sec, the active table will read "Measuring" and show running dots.

Upon completion of measurements, the results will be shown in the active table (3-5, Fig.37).

A new measurement cycle can be started by pressing "ENTER". Data in the active table will be updated.

Caution! Under the conditions of strong inductive and/or capacitive reactance, the induced voltage in the tested cable (even if it is de-energized) may turn out to be too high. If this happens, the reflection meter will be disabled, and the message "Noise" will appear in the active table. For further tests on the cable, the causes of such powerful interference must be found and eliminated.

Use the  and  keys to change the active table.

The inactive table will retain its last measurement cycle data, and a new measurement cycle will start automatically in the active table.

Data of the last measurement cycle will be discarded from the active table, if

- the automatic mode is started, or
- the reciprocal velocity factor value is changed, or
- a different cable type is set.

Any data in the inactive table will be kept.

Upon exit from the "REFLECTOMETER" mode to the Start Menu of ST300 (2.2), or to the "SWITCH" mode (2.4), any data obtained the "REFLECTOMETER" mode will be discarded.

2.8.2 Automatic Reflectometer Mode

The automatic reflection meter mode is an optimized way of testing a multiple-wire cable. The operator can keep track of testing results on all two-wire combinations simultaneously. For each pair of wires, the table will be showing data on:

- magnitude of the signal reflected from an irregularity;
- levels of mutual inductance/capacitance between the wires of each pair.

This should be enough for the user to make a quick assessment of the results as they appear during the automatic test. Once the testing has ended, the data obtained can be analyzed automatically. As a result, one learns about the 'paired' wires in a twisted pair cable, approximate length of the cable, and number of anomalies, with the indication of the wire pairs where they have been discovered and approximate distances to those anomalies.

The automatic mode is especially useful while testing a multiple-core cable consisting of twisted pairs.

To activate the automatic mode, press "MODE" while in the main screen of "REFLECTOMETER" (2.8.1). A table will appear on the screen.

If the automatic mode is activated while no wires are connected to the device's input (connected pair field reads "0-0"), no measurements will be taken. Upon first activation of the automatic mode, the table will be empty (Fig.39).

Depending on the type of cable and number of wires in it, the pair legend may change:

- 1-2** the pair is being tested and is a single twisted pair (as opposed to two wires from different twisted pairs); the cable type is set to 'twisted-pair';
- 1-3** the pair is being tested, and the two wires are from different twisted pairs;
- 1-2** the pair is not being tested (if at least one wire so numbered has been excluded as a result of setting the cable type).

In Fig.39 the automatic mode table is shown, with the cable type set to four twisted pairs. This kind of cable is typically used in LANs.

In the figure, all the eight wires of the cable are connected, and the pairs 1-2, 3-6, 4-5, and 7-8 are paired together (highlighted blue). The color scheme of such cable is shown in Appendix #1.

Controls in the automatic mode:

- "F2" - set the velocity factor (reciprocal value)
- "F3" - activate automatic analysis of the test data
- "F4" - activate automatic testing
- "MODE" and "ESC" - exit to main screen
- "FUNC" - cable settings
-     - table navigation
- "ENTER" - one-time measurement on the pair (highlighted by table cursor).

| REFLECTOMETER | | | | → 0-0 | 00:00 |
|---------------|------------|------|------------|-------------|-------|
| Pair | Level/Dist | Pair | Level/Dist | Switch | |
| 1-2 | | 3-5 | | | |
| 1-3 | | 3-6 | | | |
| 1-4 | | 3-7 | | | |
| 1-5 | | 3-8 | | | |
| 1-6 | | 4-5 | | | |
| 1-7 | | 4-6 | | | |
| 1-8 | | 4-7 | | | |
| 2-3 | | 4-8 | | | |
| 2-4 | | 5-6 | | Analysis | |
| 2-5 | | 5-7 | | | |
| 2-6 | | 5-8 | | | |
| 2-7 | | 6-7 | | | |
| 2-8 | | 6-8 | | Scan all | |
| 3-4 | | 7-8 | | | |

Fig.39

To start testing press "F4" ("Scan All"). Measurements will be taken consecutively on each two-wire combination, highlighted grey in the table while being tested, and with running dots in the "Level/Dist" cell. When the measurements are complete, the corresponding cell in the "Level/Dist" column will show mutual inductive and/or capacitive reactance between the wires of the pair, and distance to the anomaly with the most potent response. The next table line will then become active, and measurements will continue until all two-wire combinations have been thus analyzed.

Fig. 40 shows the table with data obtained on a cable consisting of four twisted pairs and free of any defects. In Fig. 40:

- 1 – current mode
- 2 – wire pair connected
- 3 – reverse value of velocity factor
- 4 – two-wire combinations column
- 5 – resulting data column
- 6 – highlighting of two wires from different twisted pairs (white)
- 7 – highlighting of two wires from the same twisted pair (light blue)
- 8 – distance to the irregularity with maximum reflection; for a defect-free cable, the anomaly returning the strongest reflected signal is its "far end"
- 9 – graphic representation of the measured mutual inductance/capacitance between the wires in a pair

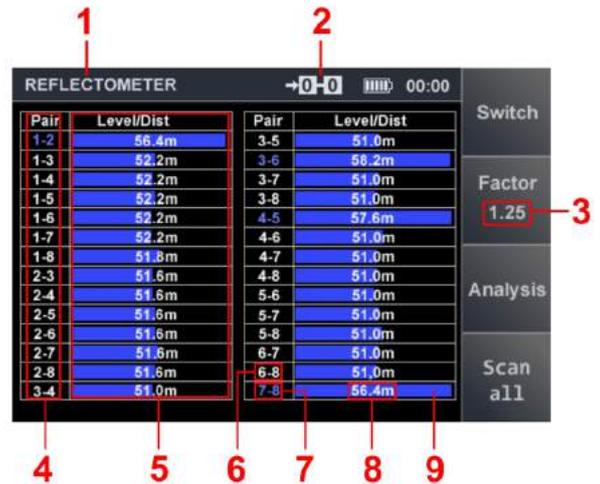


Fig.40

Based upon the results of the measurement cycle, the maximum mutual inductance/capacitance level registered is taken for 100 percent, and the rest are scaled proportionately in the graphics.

For a new measurement cycle, press "F4".

Upon completion of the automatic measurement cycle, separate measurements can be taken on any given pair of wires. To do that, use the arrow keys to move the table cursor to the corresponding table line. Measurements will start automatically. The measuring process will be signaled by running dots. When done, the distance to a discovered anomaly and the amount of mutual inductance/capacitance in the pair will be shown.

Upon completion of measurements, the obtained data can be analyzed automatically. To start automatic analysis, press "F3". The approximate cable length, and numbers of wires that are paired together (*i.e.*, belong to the same twisted pairs) will be shown on the screen. Furthermore, if anomalies are found, the corresponding wire pairs will be indicated, as well as distances to the anomalies. Figure 41 exemplifies the results of such an analysis.

In Fig. 41:

- 1 – approximate cable length; it is marked as N/A, if there has been no response neither from anomalies, nor from the other end of the cable;
- 2 – numbers of wires that are paired together (belong to the same twisted pairs); marked as N/A if the cable type selected (as described in 2.5.1.1) is not "twisted-pair";
- 3 – number of anomalies found; N/A if none.

If anomalies have been found during testing, information on those will be displayed.

To return to the measurement data table, press "ESC".

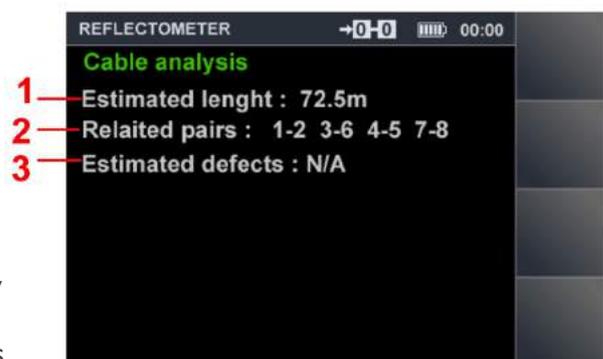


Fig.41

In the automatic mode table, only distances to anomalies with the strongest reflection are shown. This is sufficient for a preliminary assessment as to whether there are any crude connections to the cable, and for identifying the suspect pair of wires.

For more detailed information on all the responses registered during the testing of the pair in question, select the corresponding line in the table, wait for the measuring process to start (running dots will appear) and press "MODE" or "ESC".

The main screen of the "REFLECTOMETER" mode (Fig.37) will appear, and measuring will start immediately in the active table. The numbers of wires (2, Fig.37) will correspond to those previously set in the automatic mode table. To return to automatic measurements, press "MODE". The obtained results will remain in the table, and the table cursor will be set at the pair of wires that has been tested from the main screen.

3. BASIC SEARCH ROUTINES WITH ST300

A basic search routine is a set of actions aimed at finding eavesdropping devices of a certain type. One basic search routine may utilize one or more operation modes of ST300, as well as its accessories, and other detection equipment. Basic search routines form the basis for more complex procedures of testing different cable lines.

Basic search routines with ST300:

- detection of low-frequency signals in low-current lines;
- detection of high-frequency signals in power mains and low-current lines;
- nonlinearity detection in lines;
- anomaly detection in lines;
- cable tracing;
- locating a detected wire-connected eavesdropping device.

As cable lines are the subject of analysis with ST300, before describing basic search routines with the device, let us take a look at typical ways of connecting it to various cables.

3.1 PHYSICAL CONNECTION TO THE TESTED LINE

Recommended ways of connecting the device to the tested lines are described below, depending on the object of analysis and the specifics of the cable line.

Fig.42 shows a **1A** type connection of the device to power mains equipped with a standard socket.

The connection is made with:

- Mains Adaptor (13, Fig.1)
- Cable with electric plug (6, Fig.1).

Operation mode used: "WIRED RECEIVER".

Targeted Threats: active hard-wired high-frequency transmitters (transmitting within the operational frequency band of ST300's receiver).

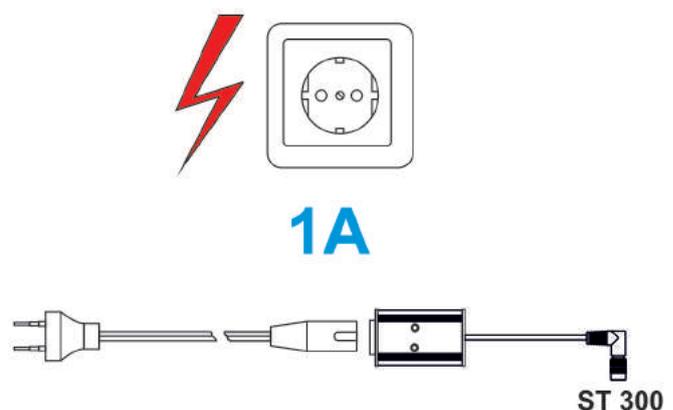


Fig.42

Fig.43 exemplifies situations when the Adaptor (13, Fig.1) and cable with crocodile clamps (2 and 12, Fig.1) will be needed for connection to power mains or low-current cabling.

Operation mode: "WIRED RECEIVER".

2A – mains cabling not equipped with a socket;

2B – line accessible through a terminal box (power switchboard).

Targeted Threats: active hard-wired high-frequency transmitters (transmitting within the operational frequency band of ST300's receiver).

2C – connection to contacts of an opened telephone socket (without disconnecting the telephony devices);

2D – connection to contacts of an opened computer network socket without disconnecting the computer or VoIP equipment.

Targeted Threats: active hard-wired high-frequency transmitters (transmitting within the operational frequency band of ST300's receiver), hidden wiretap vulnerabilities ("lawful intercept" modes) of office PBX's and VoIP-telephony devices.

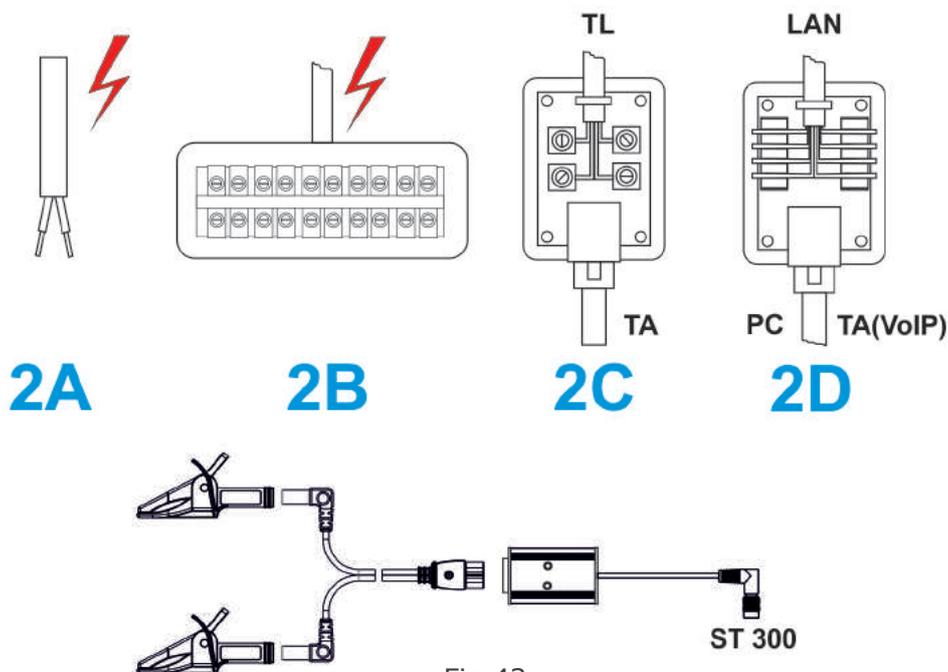


Fig.43

Fig.44 illustrates the connection of ST300 to low-current lines with the aid of the Electronic Switch. The Electronic Switch is connected to the line through a cable (4, Fig.1) and crocodile clamps (12, Fig.1).

Operation Modes of ST300:

- "WIRED RECEIVER"
- "LOW FREQUENCY AMPLIFIER"
- "NONLINEAR JUNCTION DETECTOR"
- "REFLECTOMETER"
- "CABLE LOCATOR"

3A – connection to a low-current line through a junction box;

3B – connection through contacts of an opened telephone socket (without disconnecting any telephony devices);

3C – connection to contacts of an opened computer network socket without disconnecting the computer or VoIP equipment.

Targeted Threats:

- active hard-wired low-frequency microphones
- active hard-wired high-frequency transmitters
- hidden wiretap vulnerabilities ("lawful intercept" modes) of office PBX's and VoIP-telephony equipment
- other active or passive electronic devices directly connected to the tested line

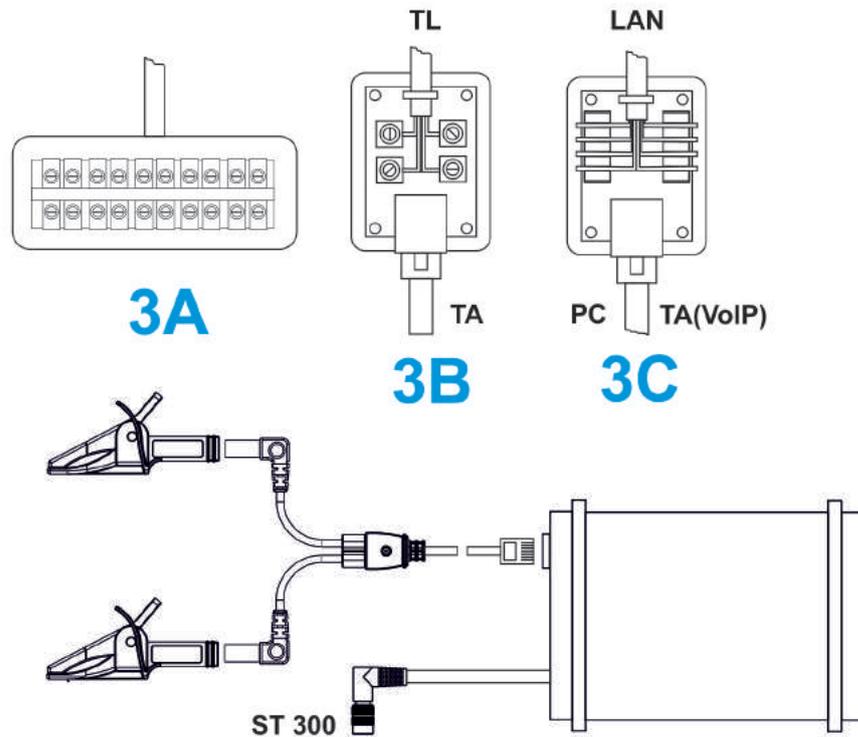


Fig.44

Fig.45 shows the connection (**4A**) of the Electronic Switch to a multiple-core low-current line that is not equipped with any socket or connector. The Adaptor (25, Fig.1) is used.

Operation Modes of ST300:

- "WIRED RECEIVER"
- "LOW FREQUENCY AMPLIFIER"
- "NONLINEAR JUNCTION DETECTOR"
- "REFLECTOMETER"
- "CABLE LOCATOR"

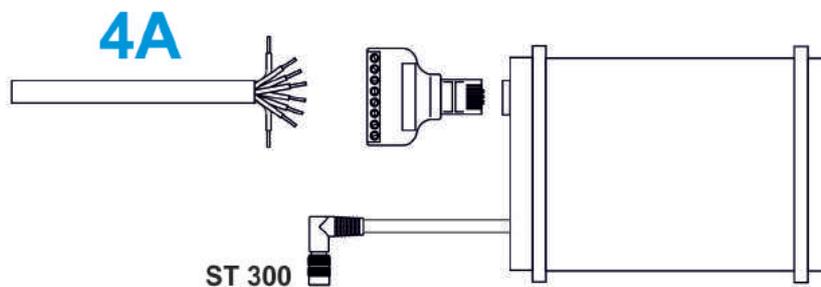


Fig.45

Targeted Threats:

- active hard-wired low-frequency microphones
- active hard-wired high-frequency transmitters
- hidden "lawful intercept" modes of office PBX's and VoIP-telephony devices
- other active or passive electronic devices directly connected to the tested line

Fig.46 illustrates the connection of ST300 to multiple-core weak-current cabling equipped with modular connectors.

Operation Modes of ST300:

- "WIRED RECEIVER"
- "LOW FREQUENCY AMPLIFIER"
- "NONLINEAR JUNCTION DETECTOR"
- "REFLECTOMETER"
- "CABLE LOCATOR"

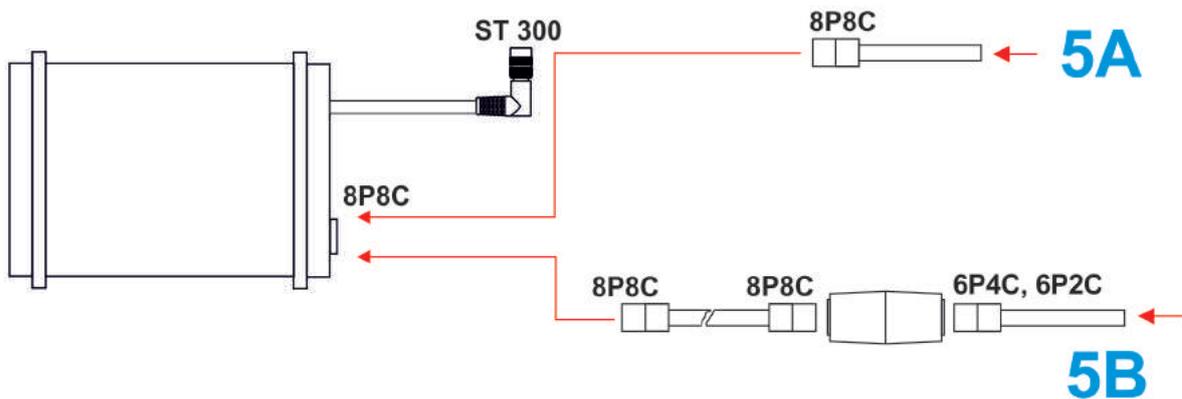


Fig.46

5A – connection to a cable equipped with an 8P8C plug. Connection with the tested line is established directly through the 8P8C socket of the Electronic Switch.

5B – connection to a cable equipped with a 6-position plug (6P6C, 6P4C, or 6P2C). For connection through the 8P8C socket of the Electronic Switch, the Pass-Through Socket (20, Fig.1) and Cable (3, Fig.1) are used.

Targeted Threats:

- active hard-wired low-frequency microphones
- active hard-wired high-frequency transmitters
- other active or passive electronic devices directly connected to the tested line

Fig.47 illustrates the connection of ST300 to multiple-core low-current cabling equipped with modular connectors.

Operation Modes of ST300:

- "WIRED RECEIVER"
- "LOW FREQUENCY AMPLIFIER"
- "NONLINEAR JUNCTION DETECTOR"
- "REFLECTOMETER"
- "CABLE LOCATOR"

6A – a single 8-position socket (8P8C) is connected through a patch cord to the 8P8C socket of the Electronic Switch;

6B – connection to a single 6-position socket (6P4C or 6P2C). The line to be tested is connected to the 8P8C socket of the Electronic Switch through the Pass-Through Socket (20, Fig.1) and Telephone Cable (8, Fig.1).

Targeted Threats:

- active hard-wired low-frequency microphones
- active hard-wired high-frequency transmitters
- other active or passive electronic devices directly connected to the tested line

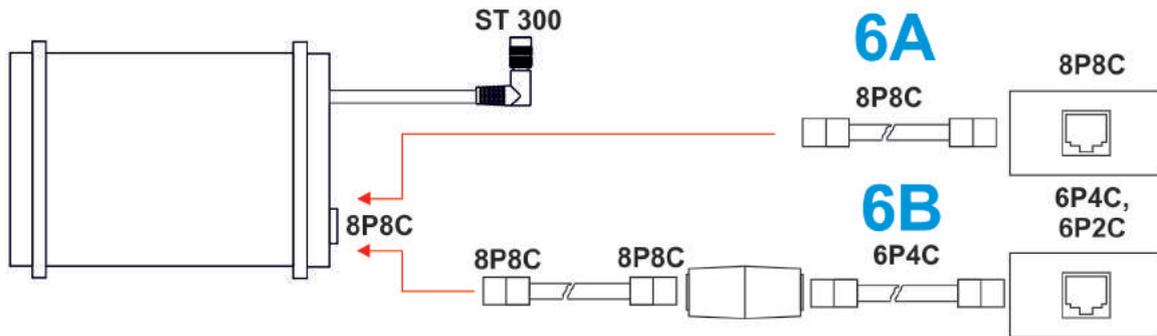


Fig.47

Fig.48 shows parallel connections of ST300 to multiple-core low-current cabling equipped with modular connectors.

Operation Modes of ST300:

- wired receiver
- low frequency amplifier

7A – connection to a single 8P8C socket. The line to be tested is connected to the 8P8C socket of the Electronic Switch with the aid of the Splitter (22, Fig.1) and Cable (3, Fig.1). The client device is connected to the Splitter through a standard cable.

7B – connection to a double (parallel) 8P8C socket. The line to be tested is connected to the 8P8C socket of the Electronic Switch through the Cable (3, Fig.1). The client device is connected to the Splitter through a standard cable.

7C – connection to a double (parallel) 6-position (6P4C or 6P2C) socket.

The line to be tested is connected to the 8P8C socket of the Electronic Switch through the Cable (3, Fig.1), Pass-Through Socket (21, Fig.1) and Telephone Cable (8, Fig.1). The client device is connected to the Splitter through a standard cable.

7D – connection to a single 6-position (6P4C or 6P2C) socket. The line to be tested is connected to the 8P8C socket of the Electronic Switch through the Cable (3, Fig.1), Pass-Through Socket (20, Fig.1), Telephone Cable (8, Fig.1) and the Splitter (21, Fig.1). The client device is connected to the Splitter through a standard cable.

Targeted Threats:

- hard-wired low-frequency microphones
- active hard-wired high-frequency transmitters
- other active or passive electronic devices directly connected to the tested line
- hidden "lawful intercept" modes of office PBX's and VoIP-telephony devices

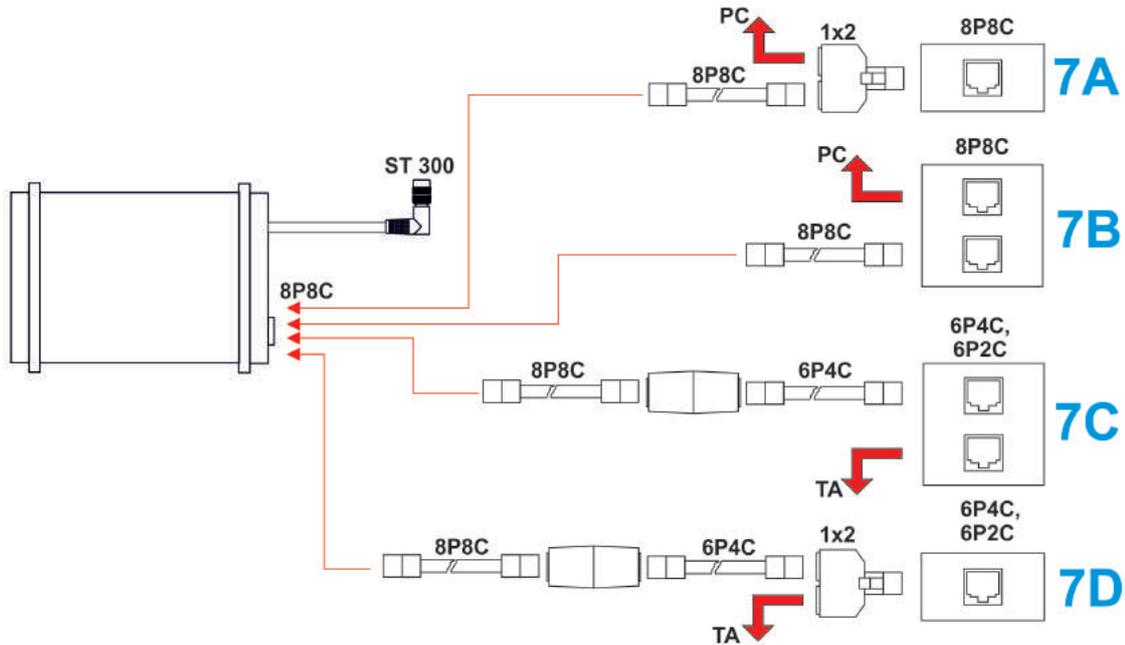


Fig.48

3.2 ELECTRONIC CONNECTION TO THE TESTED LINE

Once connected to the Electronic Switch physically, the tested line needs to be put through to ST300 electronically by selecting "CABLE SETTINGS" (2.5.1.1). This will allow making the most of the device's capabilities.

The settings include the cable type (twisted-pair or straight), number of cores in the cable, and type of connection. The most common types of cable lines, and the corresponding settings, are shown in Figs.49-51.

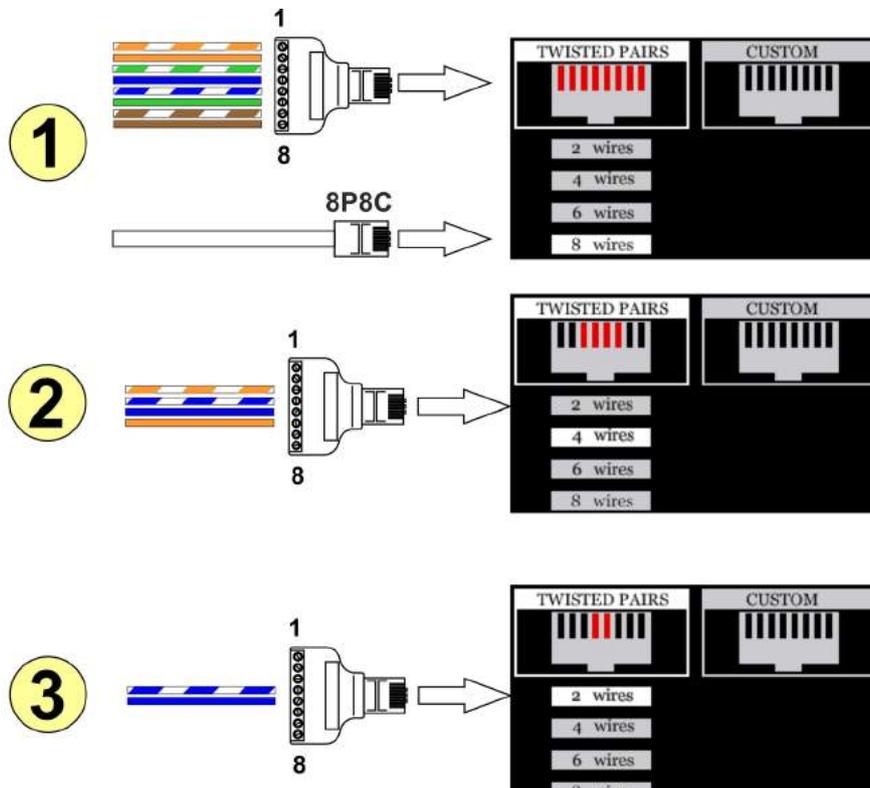


Fig.49

Fig. 49 shows cable settings when a cable consisting of one or more twisted pairs is connected.

In Fig. 49 (1) cable connection to a local computer network (UTF/FTP) is shown.

If the cable is not equipped with an RJ45 plug, its cores can be connected to the Electronic Switch through the Adaptor (25, Fig.1). Attention must be paid to connect wires of the appropriate colors to the corresponding contacts of the Adaptor. The contemporary color scheme (TIA/EIA 568B) is shown in Fig.49 (1).

If the cable is equipped with an RJ45 plug, it must be connected directly to the Electronic Switch.

In the menu of the **"CABLE SETTINGS"** mode, set the required parameters: **"TWISTED PAIRS"** for cable type, and **"8 wires"** for the number of wires.

Fig. 49 (2) shows the connection of a cable comprising two twisted pairs and not equipped with a plug. Such cables are often used in analogue, digital, and hybrid telephone lines. The standard color scheme for connection of the wires to the Adaptor's contacts is shown in the above figure. Select **"TWISTED PAIRS"** for cable type, and **"4 wires"** for the number of wires.

Fig. 49 (3) shows the connection of a cable consisting of one twisted pair and not equipped with a plug. Such cables are used in analogue and digital telephone lines. The standard color scheme for connection of the wires to the Adaptor's contacts is shown in the above figure. Select **"TWISTED PAIRS"** for cable type, and **"2 wires"** for the number of wires.

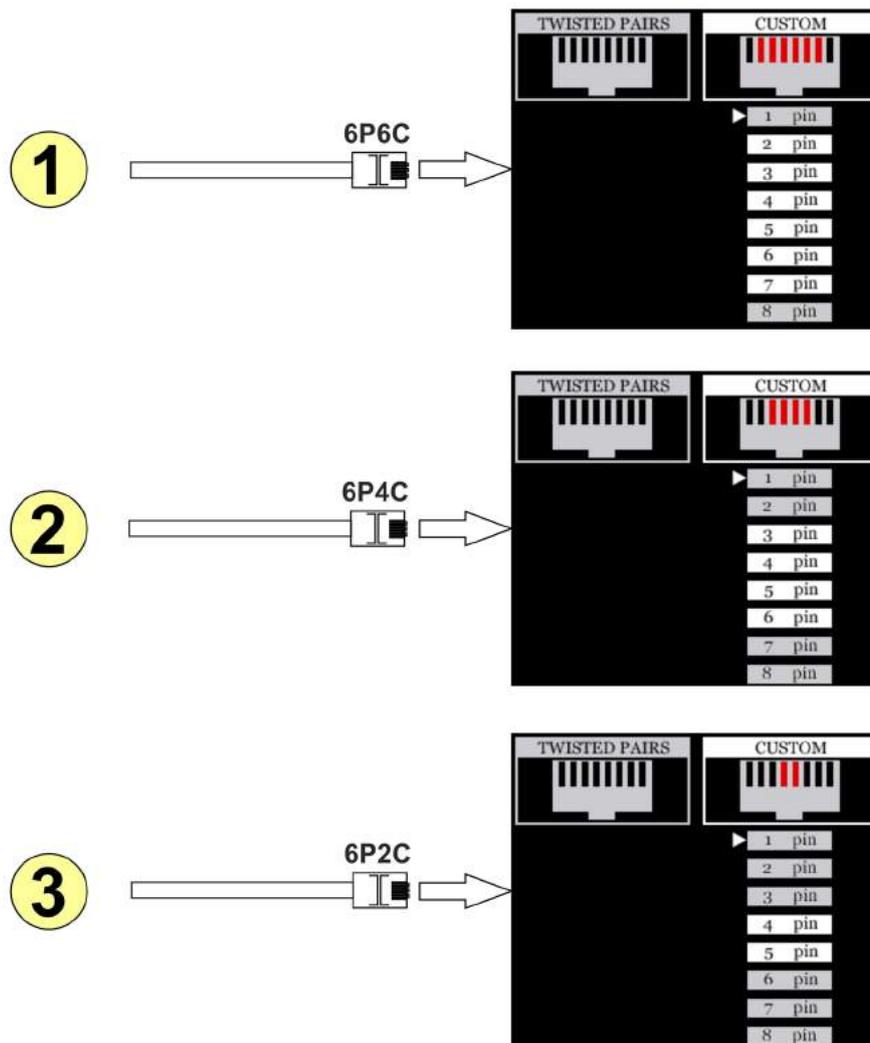


Fig.50

Fig. 50 exemplifies settings when a flat or circular cable is connected, that consists of 'non-paired' wires (as opposed to twisted pairs) and is equipped with a 6P6C plug. Cables of this kind may be used for communications in an office environment.

The table below shows the correspondence between the contact numbers in a 6-position connector of the connected line, and those of the 8-position socket of the Electronic Switch of ST300. This is to be used when selecting contact numbers in the "**CABLE SETTINGS**" mode.

| Contact No in the Electronic Switch Socket (ST300) | Engaged Contacts of a Plug or Socket (Tested Line) | | |
|--|--|------|------|
| | 6P6C | 6P4C | 6P2C |
| 1 | | | |
| 2 | 1 | 1 | 1 |
| 3 | 2 | 2 | 2 |
| 4 | 3 | 3 | 3 |
| 5 | 4 | 4 | 4 |
| 6 | 5 | 5 | 5 |
| 7 | 6 | 6 | 6 |
| 8 | | | |

Fig. 50 (1) shows the connection of a 6-core cable equipped with a 6P6C plug. In "**CABLE SETTINGS**" set "**CUSTOM**" for cable type, and **2,3,4,5,6,7** for the numbers of contacts connected to the socket of the Electronic Switch.

Fig. 50 (2) shows the connection of a 4-core cable equipped with a 6P4C plug. In "**CABLE SETTINGS**" set "**CUSTOM**" for cable type, and **3,4,5,6** for the numbers of contacts connected to the socket of the Electronic Switch.

Fig. 50 (3) shows the connection of a 2-core cable equipped with a 6P2C plug. In "**CABLE SETTINGS**" mode set "**CUSTOM**" for cable type, and **4,5** for the numbers of contacts connected to the socket of the Electronic Switch.

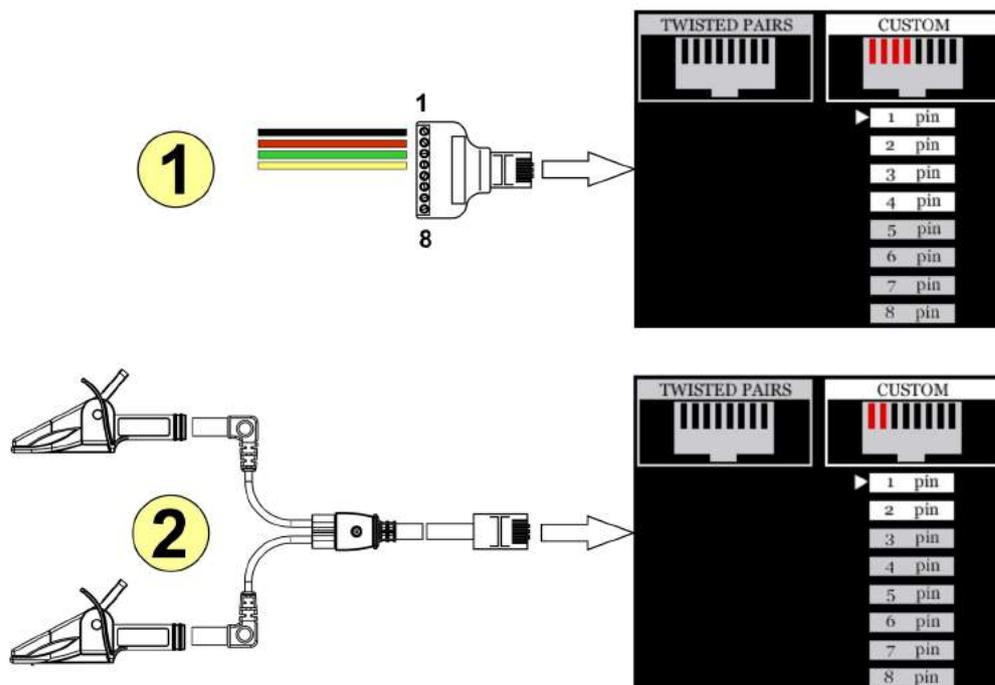


Fig.51

Fig. 51(1) illustrates the settings when a flat or circular cable is connected that consists of 'non-paired' wires (rather than twisted pairs) and is not equipped with any connectors. In this case the Adaptor (25, Fig.1) is needed for connection to the Electronic Switch of ST300. Cable wires can be connected to the Adaptor's contacts in an arbitrary way, starting with contact #1. For a 4-core cable such as shown in the figure, set "**CUSTOM**" for cable type in the "**CABLE SETTINGS**" menu, and **1,2,3,4** for the numbers of contacts connected to the socket of the Electronic Switch.

Fig. 51(2) illustrates the settings when connection to the Electronic Switch is made through the Test Cable (4, Fig.1) supplied with ST300. This cable is used for testing low-voltage lines through telephone junction boxes. The cable has an RJ45 plug (8P8C) and contacts #1 and #2 are engaged. In this case, in the "**CABLE SETTINGS**" menu, "**CUSTOM**" is to be set for cable type, and **1,2** will be the numbers of contacts in the socket of the Electronic Switch.

3.3 SEARCH FOR LOW-FREQUENCY TRANSMISSIONS IN LOW-CURRENT LINES

Object of Search:

Detection of signals from hard-wired dynamic and electret microphones.

Operation Modes of ST300:

- "LOW FREQUENCY AMPLIFIER" ("LFA");
- "SWITCH".

Additional Equipment:

- Test Sound Player.

Low-frequency signals in low-voltage lines can be detected with ST300 in both manual and automatic modes.

The manual mode is best suited for testing two-wire lines (2.5.1).

The automatic mode is used for testing multiple-wire cables (2.5.2).

3.3.1. SEARCH FOR LOW-FREQUENCY TRANSMISSIONS: MANUAL "LFA" MODE

Let us take as an example a 4-wire analogue telephone line going from an office PBX, with an analogue telephone as the end user device. In such a line, typically, the two central contacts of a 6P4C connector are engaged.

A standard telephone cable would be connected to those through its red and green wires, while the remaining two wires (typically black and yellow) would stay unused. It is these two idle wires that the transmissions from a listening device (dynamic or electret microphone) may go through, without interfering in any way with the operation of the telephone line. The microphone may be connected to the line in question somewhere within the confines of the room where conversations are supposed to be intercepted, or planted in the telephone itself.

From a practical viewpoint, the main difference between dynamic and electret microphones is that the latter require electric power (constant voltages from 9 to 20V) for operation, and are usually fed through the same wires that are used for transmitting picked-up speech. This is called phantom powering.

During the sweep, an electret microphone may be turned off. To activate it, bias voltage must be applied to the line (of both "normal" and "reverse" polarity). For identifying the illicit transmissions, a test sound must be played in the room, for which purpose a Test Sound Player (1.3.6) is supplied with ST300.

EXAMPLE

The tested line is connected to an office PBX. A telephone device is connected to the line through a socket (the phone receiver is "on the hook"). The line is power-fed from the PBX and operates normally.

PROCEDURE

Connect the Electronic Switch to the Main Unit of ST300 (1.3.3).

Connect the telephone line to the Electronic Switch (7D, Fig.48).

Turn on ST300 and go to the Start Menu (2.1 - 2.2).

From to the Start Menu go to the main screen of "LFA" mode.

Activate the "CABLE SETTINGS" mode ("FUNC" button).

Set the cable parameters (2.5.1.1) as shown in Fig.50 (2).

Go back to the main screen of the "LFA" mode (buttons "FUNC" or "ESC").

Go to the main screen of the "SWITCH" mode ("F1" button).

Set the wire combination as "4"-"5". (2.4.1), which corresponds to a connection of the two engaged wires of the telephone line. Voltage on the line will be displayed (5, Fig.18), with the phone receiver "on the hook"; typically, from 20 to 60V DC is to be expected.

Set the wire combination as "3"-"6". (2.4.1), which corresponds to a connection of the two idle wires of the telephone line. Voltage on the inactive pair will be displayed (5, Fig.18).

Under normal conditions, voltage on this pair should be equal to zero. However, that is no guarantee that no microphones are attached to the line, and only means that there is no active electret microphone. On the other hand, if the voltage exceeds 3V, that is all the more reason for concern: barring strong enough inductance or capacitance affecting the line, the presence of a listening device is likely.

Keeping the "3"-"6" pair connected, go to the main screen of the "LFA" mode ("F1" button). Choose "OSCILLOSCOPE" for data representation.

Bring your Test Sound Player in the room. Turn it on and choose "click" as the test sound type. Adjust the volume (1.3.6).

Connect headphones to the "PHONE" socket of the Main Unit (6, Fig. 2) and put them on.

if there is no voltage on the tested pair

While in the main screen of the "LFA" mode, press "F2" ("GAIN"). By pressing the  key gradually increase the gain up to maximum (60dB), all the while monitoring the signal with your headphones.

If at some point while increasing the gain, the test sound can be heard in the headphones, or changes in the oscillogram correlate with the test sound, a dynamic microphone transmitting in the speech frequency band is attached to the tested pair.

If the test sound cannot be heard in the headphones while increasing the gain, and there is no obvious connection between changes in the oscillogram and the test sound, there is no dynamic microphone with transmissions in the speech frequency band planted on the line.

Using the  key, set the gain at "0".

Disable gain control (press "F2").

Enable bias voltage control (press "F3").

Apply positive bias voltage gradually increasing it with the  key all the way to maximum (+26V) while monitoring the signal with headphones.

Set the bias voltage to "0" (press "ENTER").

Apply negative bias voltage gradually decreasing it with the  key all the way to the minimum (-26V) while monitoring the signal with headphones.

If, while increasing the magnitude of the bias voltage of either sign, the test sound can be heard in the headphones, or changes in the oscillogram correlate with the test sound, an electret microphone transmitting in the speech frequency band is attached to the pair of wires so tested. If, while increasing the magnitude of the bias voltage of either sign, the test sound cannot be heard in the headphones, and changes of the oscillogram do not correlate with the test sound, there is no electret microphone attached to the line, that transmits in the speech frequency band.

if voltage on the tested pair exceeds 3V

An electret microphone, powered and active, may be attached to the line. Since there is no point in applying a bias voltage, this feature will be disabled. In order to detect transmissions from an active microphone,

- press "F2" ("GAIN"), while in the main screen of the "LFA" mode,
- increasing the gain with the  key, monitor the sound with headphones.

If at some point while increasing the gain, the test sound can be heard in the headphones, or changes in the oscillogram correlate with the test sound, that is proof enough that a dynamic microphone transmitting in the speech frequency band is attached to the tested pair.

If the test sound cannot be heard in the headphones while increasing the gain, and there is no obvious connection between changes in the oscillogram and the test sound, it is safe to assume that there is no dynamic microphone attached to the line, and one should look for other causes of the abnormal voltage.

3.3.2. Search for Low-Frequency Transmissions: Automatic "LFA" Mode

For explanatory purposes, let us assume the following:

EXAMPLE

A 8-wire cable consisting of four twisted pairs is being tested. The cable is spare and 'off-duty' at the time of the sweep. It goes from a server into the room under inspection, and is equipped with an RJ45/8P8C connector.

Such a cable is a potential threat, because it can be used for transmissions from dynamic and electret microphones attached to it illicitly within the room.

As the tested line is not connected to any end user devices, there should be no voltage on it.

PROCEDURE

Connect the Electronic Switch to the Main Unit of ST300 (1.3.3).

Connect the cable to the Electronic Switch (6A, Fig.47).

Turn on ST300 and go to the Start Menu (2.1 – 2.2).

From to the Start Menu, go to the main screen of "LFA" mode.

Activate the "CABLE SETTINGS" mode ("FUNC" button) (2.5.1).

Set the cable parameters (2.5.1.1) as shown in Fig.49 (1).

Exit to the main screen of the "LFA" mode (buttons "FUNC" or "ESC").

Bring your Test Sound Player in the room. Turn it on and choose "click" as the test sound type. Adjust the volume (1.3.6).

Connect headphones to the "PHONE" socket of the Main Unit (6, Fig. 2) and put them on.

Activate the automatic LFA mode (press "MODE") (2.5.2).

Enable gain control ("F2" button) and with the  key set the gain to maximum (60dB).

Disable gain control ("F2" button).

Launch automatic scanning ("F4" button). The device will be consecutively testing all the two-wire combinations, pausing for a few seconds at each pair, so the user can analyze the sound output. The two-wire combination currently tested will be highlighted by table cursor.

Having run the full cycle, scanning will stop.

If the test sound can be heard during the scanning cycle, it means that a dynamic microphone is attached to the pair of wires tested at that point. When the scanning cycle is complete, select the corresponding table line with the arrow keys to listen to the signal again. For a more detailed analysis, press "MODE" to go to the main screen of the LFA mode. The signal can then be studied in the oscilloscope mode or spectrum analyzer mode. The wire pair selection made in the automatic mode will be retained.

If the testing table shows voltage beyond $-3V/+3V$ on any pair(s), and the test sound could be heard in the headphones as the cycle ran through the pair(s) in question, that is a likely sign of active electret microphone(s) attached to the pair(s).

If the testing table shows voltages in excess of $3V$ on any pair(s), but the testing sound has not been heard in the headphones, one should look for causes of such abnormal voltage.

If the test sound could not be heard in the headphones at any point during the scanning cycle, it is unlikely that a dynamic microphone is connected to the line. The line should be further tested for electret microphones by applying a bias voltage and then reversing it.

Enable gain control ("F2" button) and set minimum gain (0dB) with the  key.

Disable gain control ("F2" button).

Enable bias voltage control ("F3" button).

With the  key set bias voltage to +14V.

Disable bias voltage control ("F3" button).

Launch automatic scanning ("F4" button). The device will be consecutively testing all the two-wires combinations, pausing for a few seconds at each pair, so the user can analyze the sound output. Having run the full cycle, scanning will stop.

If the test sound can be heard during the scanning cycle, it means that a electret microphone is attached to the pair of wires tested at that point. When the scanning cycle is complete, select the corresponding table line with the arrow keys to listen to the signal again. For a more detailed analysis, press "MODE" to go to the main screen of the LFA mode. The signal can then be studied in the oscilloscope mode or spectrum analyzer mode. The wire pair selection made in the automatic mode will be retained.

If the test sound could not be heard in the headphones at any point during the scanning cycle, scanning should be repeated with a reverse bias voltage.

Enable bias voltage control ("F3" button).

Press the  key to reverse the bias (change polarity).

Disable bias voltage control ("F3" button).

Launch automatic scanning ("F4" button). The device will be consecutively testing all the two-wire combinations, pausing for a few seconds at each pair, so the user can analyze the sound output. Having run the full cycle, scanning will stop.

If the test sound can be heard during the scanning cycle, it means that a electret microphone is attached to the pair of wires tested at that point. When the scanning cycle is complete, select the corresponding table line with the arrow keys to listen to the signal again. For a more detailed analysis, press "MODE" to go to the main screen of the LFA mode. The signal can then be studied in the oscilloscope mode or spectrum analyzer mode. The wire pair selection made in the automatic mode will be retained.

If the test sound could not be heard in the headphones at any point during the scanning cycle, it is unlikely that an electret microphone is connected to the line.

3.4. SEARCH FOR HIGH-FREQUENCY TRANSMISSIONS IN CABLING

Object of Search:

– detection of transmissions from eavesdropping electronics sending data over power mains and weak-current lines within the band from 100kHz to 150MHz.

Operation Modes of ST300:

- “WIRED RECEIVER” (“WR”)
- “SWITCH”.

Additional Equipment:

- Adaptor for Testing Power Mains
- Test Sound Player.

High-frequency signals in power mains and low-voltage lines can be detected with ST300 in both manual and automatic modes. The difference is in the way they are analyzed.

In the manual mode, all transmissions within the band are shown in a spectral diagram. A signal of interest can be tuned into by moving the marker to its position in the spectral diagram.

In the automatic mode, data on the detected transmissions are shown in a table rather than graphically. To tune into a specific frequency, the table cursor should be moved to the corresponding line. When the number of detected transmissions is high enough, the automatic mode may prove much more convenient than the manual one.

For the analysis of detected signals, monitoring at a set frequency and oscilloscopic representation can be utilized in both manual and automatic receiver modes.

3.4.1. Search for High-Frequency Transmissions in Power Mains

Search for high-frequency transmitters is the most efficient when the two modes, automatic and manual, are used in combination. A typical example is given below.

EXAMPLE

An office room is being inspected, with several electric outlets into which various office equipment, desk lamps, and other electric and electronic devices, are plugged. It is known that a single cable carries electricity to this room, and to this room only, from an electric trip switch fuse box in the facility. The switch corresponding to the cable in question is accessible, so the line can be de-energized.

The presence of high-frequency transmitters is suspected, that may be connected either to the electricity line, or to user appliances in the room.

PROCEDURE

De-energize the cable using the corresponding switch in the switch fuse box.

Use the Tester Screwdriver (7, Fig.1) to make sure there is no voltage in the line.

Disconnect all devices from the sockets.

Connect the Mains Adaptor (13, Fig.1) to the Main Unit of ST300.

Connect the Mains Adaptor to an electrical outlet through the Cable (6, Fig.1).

Turn on ST300 and go to the Start Menu (2.1 – 2.2). As the Main Unit is not connected to the Electronic Switch, only “WIRED RECEIVER” and “SETTINGS” will be available in the menu.

Activate the “WR” mode (“F2” button).

Select the monitoring band (100kHz-30MHz or 100kHz-150MHz). The main screen of the “WR” mode will appear (2.6.1).

Use the button “F4” to set the gain at “x2”.

All activity in the band, while the line is in a de-energized state, will be displayed on the screen. Since no eavesdropping devices powered from the line can be active at this time, all these signals can be considered 'safe', and brought about by external factors (random noise, broadcasting signals, etc). To eliminate these signals from further testing, a differential mode of the receiver is used.

Activate "DIFFERENTIAL MODE" ("F3" button) (2.6.2).

A differential panoramic display of activity in the band will appear. From this point on, all the signal levels measured previously are set as the new zero baseline, and only the newly appeared signals will be shown. When voltage is supplied to the line, any high-frequency transmitters attached to it will be activated. It is their activity that will be displayed.

Power the line again using the switch in the switch fuse box. If new signals appear in the differential spectrum, turn on automatic receiver mode ("F2" button – "Search"). Data on the detected signals will be shown in a table (2.6.5), with the first line selected by default.

Bring your Test Sound Player in the room. Turn it on and choose "click" as the test sound type. Adjust the volume (1.3.6).

Connect headphones to the "PHONE" socket of the Main Unit (6, Fig. 2) and put them on.

Adjust the volume in the headphones (4, Fig.2). Listen to the AM-demodulated output.

Change demodulation to FM ("F2" button). Listen to the FM-demodulated output.

For frequency tuning, activate the mode of monitoring at a set frequency ("ENTER") (2.6.5). Using the  and  keys, select the frequency with peak magnitude (9, Fig.33). To deactivate set frequency monitoring, press "ENTER" again.

To analyze a demodulated signal with the oscilloscope, press "F3". Press "F3" again to return to the automatic mode with its table view.

Go to the next table line ( key).

Repeat the monitoring procedure, toggling AM/FM-modulation with the "F2" button.

Proceed in this manner to analyze all the detected signals.

If no new signals are detected in the differential panorama upon supplying voltage to the line, there are no active eavesdropping devices connected to it. However, there can be remotely controlled ones that are currently on standby. These can be searched for using active detection methods, such as non-linear junction detection.

If new signals do appear in the differential representation of the band when voltage is applied again to the line, and the test sound can be heard through the headphones, an active high-frequency transmitter attached to the line is in the room. As ST300 is active in the same room as the transmitter, the activity of the latter may be detected not only at its carrier frequency, but at sub-harmonics as well. The highest of the 'new' peaks is likely to correspond to the carrier frequency.

If new signals do appear in the differential representation when voltage is supplied again to the line, but the test sound cannot be heard through the headphones at any point while they are being analyzed, a digital (or encoding) high-frequency transmitter may be active on the line. Such signals would require further analysis and their sources should be found.

If, upon supplying voltage to the line, a radical increase of the background level is registered within the band from 10 to 100MHz, this may signal the activity of a PLC-modem. Once all the detected signals have been analyzed, one should check how the differential representation changes when the office appliances are plugged in, one after another. This way it can be established which appliance is the source of the suspect signal.

Exit the automatic mode ("ESC" button). A differential diagram will be representing activity in the powered line with no appliances plugged in.

Exit the differential mode ("F3" button). The current diagram will be representing activity in the powered line with no appliances plugged in.

Reenter the differential mode ("F3" button). The differential diagram will be representing activity in the powered line, with all the previously detected signals set as the new 'zero' baseline.

Connect a piece of equipment in the room to the tested line. If new signals appear in the differential panoramic display, activate the automatic mode ("F2" button) and analyze each newly detected signal in the table, as described earlier.

Having analyzed all the new signals, exit the automatic mode ("ESC" button) and disable the differential mode ("F3" button). Activate the differential mode ("F3" button) again to obtain a new differential diagram.

Connect another appliance to the line. Analyze any new signals in the same manner as with the first appliance plugged in.

Proceed to test all the office equipment in the room.

Any appliances showing suspect signals must be disassembled and searched according to special procedures.

3.4.2. Search for High-Frequency Transmissions in Low-Current Lines

When it comes to testing for high-frequency transmitters, the distinguishing feature of low-current lines from power mains is that most of them are made of multiwire. To optimize testing with ST300, the Electronic Switch is used. This allows testing all the two-wire combinations in a much faster way, without connecting them manually every time. Otherwise, using the wired receiver for testing low-current lines is not much different from what is described in 3.4.1 above.

EXAMPLE

The line to be tested is connected to an office PBX. A telephone device is connected to the line through a socket (the phone receiver is "on the hook"). The line is power-fed from the PBX and operates normally.

A HF transmitter may be planted in the telephone itself or connected to the line somewhere within the room, where conversations are supposed to be intercepted.

PROCEDURE

Connect the Electronic Switch to the Main Unit of ST300 (1.3.3).

Connect the line to be tested to the Electronic Switch (7D, Fig.48).

Bring your Test Sound Player in the room. Turn it on and choose "click" as the test sound type. Adjust the volume (1.3.6).

Connect headphones to the "PHONE" socket of the Main Unit (6, Fig. 2) and put them on.

Turn on ST300 and go to the Start Menu (2.1 - 2.2).

Activate the "WR" mode ("F2" button).

Select the monitoring band (100kHz-30MHz or 100kHz-150MHz).

The main screen of the "WR" mode (2.6.1) will appear.

Use the button "F4" to set the gain at "x2".

Go to the main screen of the "SWITCH" mode ("F1" button) to select a two-wire combination.

When the connection scheme 7D (Fig. 48) is used, the engaged contacts of the Electronic Switch are #3, 4, 5, 6. Therefore, the combinations to test are:

3-4; 3-5; 3-6;

4-5; 4-6;

5-6.

It should be noted that the transmitter may be fed with power through the pair "4" - "5" otherwise used legitimately, and transmit data through any of the above combinations, including 4-5.

In the main screen of the "SWITCH" mode, set the pair "3"-"4" (2.4.1.1).
Go to the main screen of the "WR" mode ("F2" button).

The screen will display band activity for the pair "3"-"4".

Activate the automatic mode ("F2" button).
Analyze all the detected signals at AM- and FM-demodulation, as described in 3.4.1 above.
Exit the automatic mode ("ESC" button) to the main screen of the "WIRED RECEIVER" mode.
Go to the main screen of the "SWITCH" mode ("F1" button).
Set the next two wire combination ("3"-"5").
Go to the main screen of the "WR" mode ("F2" button).

The screen will display band activity for the pair "3"-"5".

Activate the automatic mode ("F2" button).
Analyze all the detected signals at both AM- and FM-demodulation, as described in 3.4.1 above.
Proceed in this manner to test all the two-wire combinations named above.

If, during such analysis, the test sound can be heard in the headphones, it means that there is an active high-frequency transmitter in the room, attached to the line. In this event, without changing the combination that yields the test sound output, disconnect the telephone from the tested line. If the suspect signal is no longer heard in the headphones and disappears from the screen, its source is in the telephone.

If, upon disconnecting the telephone, the signal is still there, that means its source is connected to the line somewhere in the room (as correlation with the test sound is in evidence).

Digital signals not correlating with the test sound also should be treated with caution, as those may carry data from digital (or encoding) transmitters. It is advisable to test such signals further in the the oscilloscopic mode (2.6.4).

It should be established if the detected signal is induced externally, or its source is connected to the tested line. To do that, without changing the combination, disconnect the line from the PBX. If the signal disappears, its source is attached to the line. If not, the signal is an 'induced' one and therefore not dangerous.

3.5. NONLINEARITY DETECTION IN A CABLE

Object of Search:

– detection of electronics electrically attached (whether in parallel or series configuration) to the tested cable.

Operation Modes of ST300:

- "NONLINEAR JUNCTION DETECTOR" ("NL")
- "SWITCH".

Additional Equipment:

Short-Circuiter (23, Fig.1)

Using ST300 in the "NL" mode on a powered line is strictly forbidden!

The use of the Electronic Switch is required.

The tested line must be disconnected from any equipment at the far end. All known equipment must be disconnected from the line.

For the detection of parallel-connected devices, the line must be open-circuited at the far end. For the detection of series-connected devices, the line must be short-circuited.

Two-wire cables are best tested in the manual "NLJD" mode.

Multiple-wire cables are best tested in the automatic "NLJD" mode.

3.5.1. Nonlinear Junction Detector of ST300 in Use: Manual Mode

The manual mode is typically used in two situations:

- for testing a specific pair of wires where the suspect signal has been discovered while checking a multiple-wire cable;
- for testing a two-wire cable.

EXAMPLE

Let us illustrate the procedure assuming a two-wire analogue telephone line of an office PBX is to be tested. Further assumptions are the following:

The two central contacts of a 6P2C plug are in use. The eavesdropping device may be connected in either series or parallel configuration.

A telephone device is connected to the line through a socket (with the phone receiver "on the hook"). The line is power-fed from the PBX and operates normally.

PROCEDURE

Disconnect the line to be tested from the PBX.

Disconnect the telephone from the line.

Connect the Electronic Switch to the Main Unit of ST300 (1.3.3).

Connect the line to be tested to the Electronic Switch (6B, Fig.47).

Turn on ST300 and go to the Start Menu (2.1 – 2.2).

Go to the main screen of the "NLJD" mode ("F2" button).

Activate the "CABLE SETTINGS" mode ("FUNC" button).

Set the cable parameters (2.5.1.1) as shown in Fig. 50(3).

Exit the "CABLE SETTINGS" mode to the main screen of the "NLJD" mode (button "FUNC" or "ESC").

Go to the main screen of the "SWITCH" mode ("F1" button).

On the main screen of the "SWITCH" mode, set the wire pair "4" – "5" (2.4.1.1).

Exit the "SWITCH" mode to the main screen of the "NLJD" mode ("F3" button).

The screen will show the results of testing the active wire pair ("4"–"5") for nonlinearities in the open-circuited configuration.

The testing results are represented in the form of three horizontal bars, of which

- the upper bar graph (white) shows the reflection signal magnitude at the frequency of the test pulse; the readings are proportional to the resistance on the tested wire pair;*
- the middle bar graph (red) shows the reflection magnitude at the second harmonic frequency of the test pulse (indicative of semiconductor content);*
- the lower bar graph (blue) shows the reflection magnitude at the third harmonic frequency of the test pulse (indicative of metal-oxide-metal structures).*

When no devices are connected to the tested pair of wires, there should be no readings on any of the three bars.

Therefore, readings on the red bar graph will indicate that there is electronics attached to the tested wire pair.

Readings on the blue bar graph, that indicate the presence of MOM-diodes, may be brought about by oxidation of contacts in the socket, twisted connections, etc. However, one should take such readings seriously, as eavesdropping devices may have elements that yield a response at the third harmonic frequency of the test pulse (e.g., anti-parallel diode connections).

Therefore, if the red and blue bar graphs show any responses at all, quite regardless of their relative magnitudes, one should analyze the current pair of wires further.

If open-circuit testing has shown nothing on either red or blue bar graph, this means that no electronics in parallel connection to the line have been discovered. Now the wire pair should be short-circuited and tested for series connections.

Keeping the main screen of the "NLJD" mode on, short-circuit the tested wire pair at the opposite end with the Short-Circuiting Socket (23, Fig.1).

If there are readings on the red and/or blue bar graphs, there is a series connection of a non-linear element to the wire pair.

3.5.2. Nonlinear Junction Detector of ST300 in Use: Automatic Mode

The automatic "NLJD" mode is used for testing multiple-wire cables.

EXAMPLE

For illustration purposes, let us assume that a multiple-wire cable consisting of four twisted pairs is being tested. As unsolicited connections can be both parallel and series, the line should be tested in both open-circuit and short-circuit modes.

The cable in question is plugged into a 8P8C socket, and equipped with a 8P8C plug at the other end. The line is kept as a spare, not connected to any known equipment.

PROCEDURE

Connect the Electronic Switch to the Main Unit of ST300 (1.3.3).

Connect the line to be tested to the Electronic Switch (6A, Fig.47).

Turn on ST300 and go to the Start Menu (2.1 – 2.2).

Go to the main screen of the "NLJD" mode ("F2" button).

Activate the "CABLE SETTINGS" mode ("FUNC" button).

Set the cable parameters (2.5.1.1) as shown in Fig. 49 (1).

Exit the "CABLE SETTINGS" to the main screen of the "NLJD" mode (button "FUNC" or "ESC").

Activate the automatic mode ("MODE" button). A table will appear on the screen.

Launch scanning ("F4" button).

Having run the full cycle of testing all the two-wire combinations, scanning will stop. The table will have filled in with graphic data on reflection responses at the second and third harmonic frequencies of the test pulse, for each wire pair. Thus, the operator will get a full picture as to the presence of nonlinearities throughout all the two-wire combinations, as well as relative levels of response at the second and third harmonics.

If a response on any pair is too strong (one of the graphs goes off scale), the power of the probing signal should be reduced. To do that, highlight the wire pair, go to the main screen of the "NLJD" mode ("MODE" button) and, using the  key, reduce the test pulse magnitude. Press "MODE" to return to the automatic mode.

Fig. 52 represents a nonlinearity detection in a 8-wire cable with an electronic device connected to it. The nonlinearity has been found on pair "4"- "5". The response is much stronger at the second harmonic frequency than at the third. As testing has been performed on an open-circuit, one may safely assume that there is evidence of a parallel-connected device that has semiconductor components. The absence of responses throughout the rest of the table means that no electronics have been found in parallel connection to any of the other two-wire combinations.

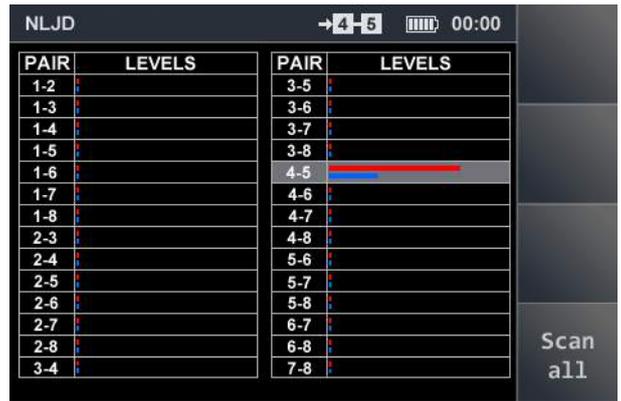


Fig.52

Now test the cable in the short circuited configuration.

For the detection of electronics in series connection,
 - with the Short-Circuiting Socket (23, Fig.1) short-circuit all the wires of the tested cable at the far end;
 - in the automatic mode, launch another scanning cycle ("F4" button).

Upon completion of the testing cycle on all the two-wire combinations, the table will be filled in with graphic data on the reflection levels.

Fig. 53 shows the results of testing a 8-wire cable that has an electronic device series-connected to one of its wires. As is seen from the figure, all the two-wire combinations involving wire #2 exhibit a nonlinearity response. As all the wires are short-circuited at the far end, it is safe to say that an electronic device is series-connected to wire #2 of the cable.

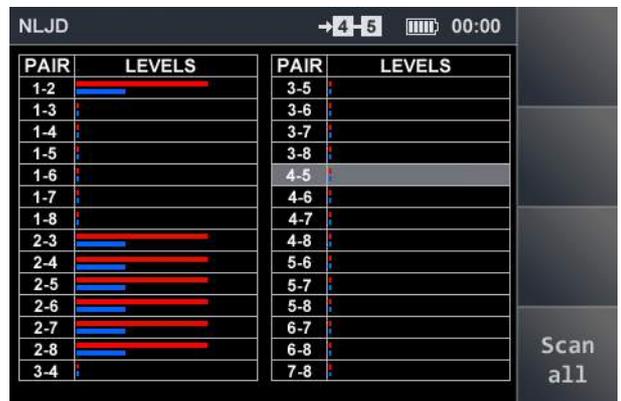


Fig.53

3.6. ANOMALY DETECTION IN A CABLE

Object of Search:

- detection of anomalies caused by unsolicited connections to a cable.

This operation is performed in the "REFLECTOMETER" mode ("REF") specifically intended for testing multiple-wire cables that consist of twisted pairs, although using it on other kinds of cables (two-wire and multiple-wire straight) is also possible.

Two methods are essential to an efficient use of the "REF" mode:

- testing from both ends of the cable; this is done from the main screen of the "REF" mode (2.8.1) - for the most part, when dealing with a two-wire cable, or a specific pair of wires in a multiple-wire cable;
- pair-by-pair comparison in the automatic "REF" mode (2.8.2) when testing a multiple-wire cable.

Using ST300 in the "REF" mode on a powered line is strictly forbidden!

The use of the Electronic Switch is required.

The tested line must be disconnected from any equipment at the far end. All known equipment must be disconnected from the line.

If the line has any known branches, each segment must be disconnected from the main line and tested separately (as the goal is to find unknown connections to a piece of cabling that is supposed to be free from any connections at the time of testing).

It is advisable to perform testing on an open-circuited line.

3.6.1. Reflection Meter of ST300 in Use: Cable Testing from both Ends

EXAMPLE

To illustrate the use of ST300 in the "REF" mode, let us assume that a multiple-core cable needs to be tested from both ends (both are accessible).

PROCEDURE

Connect the Electronic Switch to the Main Unit of ST300 (1.3.3).

Disconnect all devices from the line. Make sure there are no known connections (branches).

Connect the line to the Electronic Switch; the way of connection depends on the cable type.

Turn on ST300 and go to the Start Menu (2.1 – 2.2).

Go to the main screen of the "SWITCH" mode (2.4.1).

Set the numbers of wires to be tested, depending on their connection to the Electronic Switch (see 2.4.1.1).

Go to the main screen of the "REF" ("F4" button).

Set the reciprocal value of the velocity factor for the cable (2.8.1.1). Press "ENTER". The main screen of the "REF" mode will appear on display, and in a few seconds the active table, highlighted grey, will be filled in with measurement results.

Change the active table with the  key. The previous table will retain all the data; a new measurement cycle will start automatically, filling the newly activated table with its results. The results will be similar to the previous cycle.

Without turning off the device, or changing any settings, disconnect the line from the Electronic Switch, and bring your ST300 to the other end of the tested line.

Connect the line to the Electronic Switch. If the cable is not equipped with a connector, connect the tested wires physically to the same contacts of the Electronic Switch that were engaged in the first measurement cycle. Do not change any settings in the "SWITCH" mode!

Having connected the line, press "ENTER" to start another measurement cycle. Its results will be shown in the active table.

Compare and analyze the results of the two measurement cycles.

In Fig. 54 an example of testing a cable from both ends is shown.

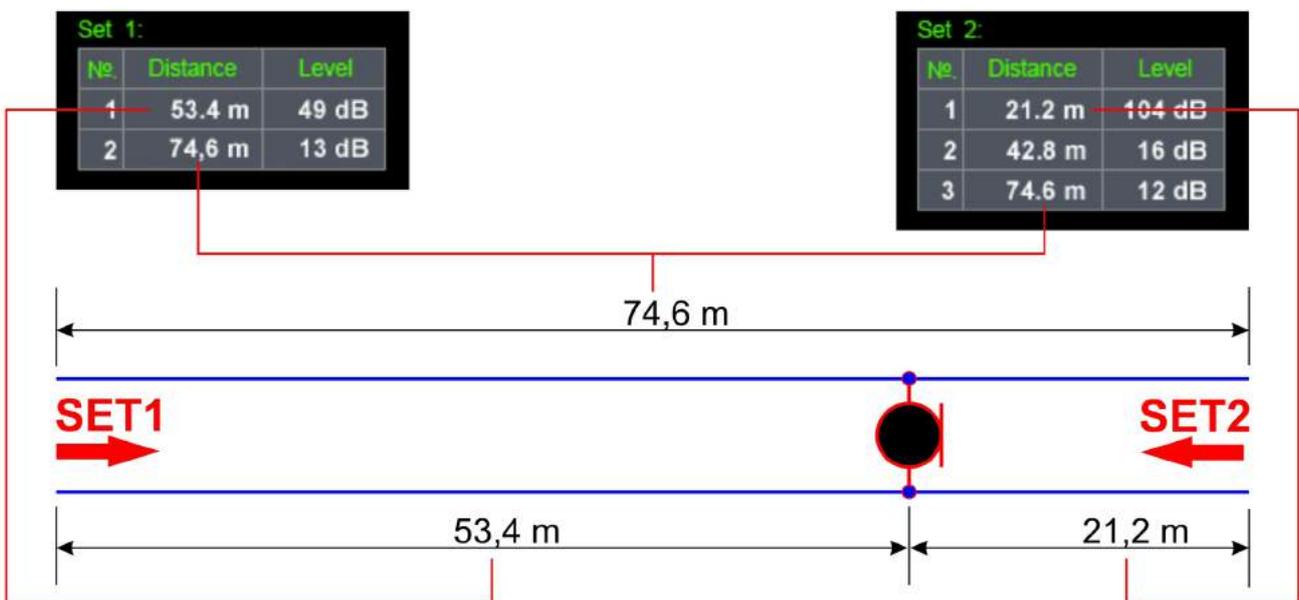


Fig.54

Conclusions from testing (Fig.54).

1. Allowing for instrument error, the total cable length is 74-75m. In both tables, the distance to the farthest anomaly is 74.6m. The response magnitudes in the first and second measurement cycles are approximately the same (13dB and 12dB, respectively).
2. In the first measurement cycle, an anomaly has been found at a distance of 53.4m. The response is stronger than that from the far end of the cable.
3. In the second measurement cycle, an anomaly has been found at a distance of 21.2m. The response is quite strong: 104dB. This is because the anomaly is relatively close to the connection of ST300. Yet another response that is comparatively weak (16dB) comes from a distance of 42.8m. This may be a harmonic of the response coming from the distance of 21.2m.
4. The response in the first measurement cycle at 53.4m and the one in the second measurement cycle at 21.2m, are returned by one and the same anomaly. In fact, adding up the two distances makes the full cable length ($21.2m + 53.4m = 74.6m$).

3.6.2. Reflection Meter of ST300 in Use: Automatic Mode

The use of the reflection meter in the automatic mode and interpretation of the results are explained below based on the example of a multiple-wire cable comprising four twisted pairs.

PROCEDURE

Connect the Electronic Switch to the Main Unit of ST300 (1.3.3).

Disconnect all devices from the line. Make sure there are no known connections (branches).

Connect the line to the Electronic Switch; the way of connection must fully accord with the color scheme of the cabling.

Turn on ST300 and go to the Start Menu (2.1 – 2.2).

Go to the main screen of the "REF" mode ("F4" button).

Activate the "CABLE SETTINGS" mode ("FUNC" button).

Set the cable parameters (2.5.1.1) as shown in Fig. 49 (1).

Exit to the main screen of the "REF" mode (buttons "FUNC" or "ESC").

Set the reciprocal value of the velocity factor for the cable (2.8.1.1) and press "ENTER".

Activate the automatic "REF" mode ("MODE" button). An empty table will appear on the screen, with twisted pairs highlighted blue.

Launch a measurement cycle ("F4" button: "Scan All").

Having run the full cycle, scanning will stop. For each two-wire combination in the table, two measurements will be shown:

- distance to the anomaly with maximum response (numerical value);
- mutual inductance/capacitance between the wires of the pair (bar graph).

Knowing the distances to anomalies, and comparing the inductive/capacitive interaction with reference values, one can see if the cabling is intact, or has been tampered with, possibly with hostile intent.

The results of testing the same multiple-wire cable but with different connections are shown in Figs. 55-59.

In Fig. 55, the results of testing a **defect-free** cable are shown.

One can note the following distinctive features:

1. Electromagnetic interaction between the wires of a twisted pair is the same in strength for all pairs, and approximately twice as strong as that between wires from different pairs;

| Pair | | Level/Dist | |
|------|-------|------------|-------|
| 1-2 | 76.8m | 3-5 | 72.6m |
| 1-3 | 73.2m | 3-6 | 77.4m |
| 1-4 | 72.6m | 3-7 | 73.2m |
| 1-5 | 72.6m | 3-8 | 73.2m |
| 1-6 | 73.2m | 4-5 | 79.2m |
| 1-7 | 73.2m | 4-6 | 72.6m |
| 1-8 | 73.2m | 4-7 | 73.2m |
| 2-3 | 73.2m | 4-8 | 73.2m |
| 2-4 | 73.2m | 5-6 | 72.6m |
| 2-5 | 73.2m | 5-7 | 72.6m |
| 2-6 | 73.2m | 5-8 | 73.2m |
| 2-7 | 73.2m | 6-7 | 72.6m |
| 2-8 | 73.2m | 6-8 | 73.2m |
| 3-4 | 72.6m | 7-8 | 76.8m |

Factor 1.25

Analysis

Scan all

Fig.55

2. Distances to anomalies with peak responses in non-paired couples of wires vary insignificantly (72.6 – 73.2m).

3. The lengths of twisted pairs are shown as different and greater than those of non-paired couples of wires (this can be explained by different coil lengths, and, accordingly, different total lengths of the wire).

Fig. 56 shows the results of testing the same cable, but **with wire #1 broken**. Comparison with the reference (Fig.55) yields the following differences:

1. Interaction in different twisted pairs is not the same: the pair "1" - "2" exhibits stronger inductance/capacitance interaction than the other three twisted pairs.

2. Distances to anomalies with peak responses in different "cross-pair" combinations of wires are different: in all of those that include wire #1, distance to the anomaly is 19.8 to 21.6m.

3. Interactions between wires from different twisted pairs are different; combinations with wire #1 show stronger interaction.

This situation requires testing all the combinations with wire #1 from both ends (3.6.1).

Fig. 57 shows the results of testing the same cable, but **with an electronic device series-connected to wire #1**. Comparison with the reference (Fig. 55) yields the following differences:

1. Interaction in different twisted pairs is not the same: the pair "1" - "2" exhibits weaker inductance/capacitance interaction than the other three twisted pairs.

2. Distances to anomalies with peak responses in different "cross-pair" combinations of wires are different: in all of those that include wire #1, distance to the anomaly exceeds distances to the end of the cable in all the other "cross-pair" wire combinations.

3. Interactions between wires from different twisted pairs are different: combinations with wire #1 show stronger interaction.

This situation requires testing all the combinations with wire #1 from both ends (3.6.1).

Fig. 58 shows the results of testing the same cable, but **with an electronic device parallel-connected to the twisted pair "1" - "2"**. Comparison with the reference (Fig.55) yields the following differences:

1. Interaction in different twisted pairs is not the same: the pair "1" - "2" exhibits stronger inductance/capacitance interaction than the other three twisted pairs.

2. Distances to anomalies with peak responses in different "cross-pair" combinations of wires are different: in all of those that include wires #1 and #2, distance to the anomaly exceeds distances to the end of the cable in all the other "cross-pair" wire combinations.

3. Interactions between wires from different twisted pairs are different: combinations with wires #1 and #2 show weaker interaction.

This situation requires testing the "1" - "2" pair from both ends (3.6.1).

| REFLECTOMETER → 0-0 00:00 | | | |
|---------------------------|------------|------|------------|
| Pair | Level/Dist | Pair | Level/Dist |
| 1-2 | 21.6m | 3-5 | 72.6m |
| 1-3 | 21.0m | 3-6 | 77.4m |
| 1-4 | 21.0m | 3-7 | 73.2m |
| 1-5 | 20.4m | 3-8 | 73.2m |
| 1-6 | 21.0m | 4-5 | 79.2m |
| 1-7 | 19.8m | 4-6 | 72.6m |
| 1-8 | 20.4m | 4-7 | 72.6m |
| 2-3 | 73.8m | 4-8 | 72.6m |
| 2-4 | 73.8m | 5-6 | 72.6m |
| 2-5 | 73.8m | 5-7 | 72.6m |
| 2-6 | 73.2m | 5-8 | 72.6m |
| 2-7 | 73.2m | 6-7 | 73.2m |
| 2-8 | 73.2m | 6-8 | 73.2m |
| 3-4 | 72.6m | 7-8 | 76.8m |

Factor 1.25
Analysis
Scan all

Fig.56

| REFLECTOMETER → 0-0 00:00 | | | |
|---------------------------|------------|------|------------|
| Pair | Level/Dist | Pair | Level/Dist |
| 1-2 | 76.8m | 3-5 | 72.6m |
| 1-3 | 77.4m | 3-6 | 77.4m |
| 1-4 | 77.4m | 3-7 | 73.2m |
| 1-5 | 77.4m | 3-8 | 73.2m |
| 1-6 | 77.2m | 4-5 | 79.2m |
| 1-7 | 77.4m | 4-6 | 72.6m |
| 1-8 | 77.4m | 4-7 | 72.6m |
| 2-3 | 72.0m | 4-8 | 72.6m |
| 2-4 | 73.2m | 5-6 | 72.6m |
| 2-5 | 73.2m | 5-7 | 72.6m |
| 2-6 | 73.2m | 5-8 | 72.6m |
| 2-7 | 73.2m | 6-7 | 73.2m |
| 2-8 | 73.2m | 6-8 | 73.2m |
| 3-4 | 72.6m | 7-8 | 76.8m |

Factor 1.25
Analysis
Scan all

Fig.57

| REFLECTOMETER → 0-0 00:00 | | | |
|---------------------------|------------|------|------------|
| Pair | Level/Dist | Pair | Level/Dist |
| 1-2 | 22.2m | 3-5 | 72.6m |
| 1-3 | 21.6m | 3-6 | 77.4m |
| 1-4 | 21.0m | 3-7 | 73.2m |
| 1-5 | 21.6m | 3-8 | 73.2m |
| 1-6 | 21.6m | 4-5 | 79.2m |
| 1-7 | 21.0m | 4-6 | 72.6m |
| 1-8 | 21.0m | 4-7 | 73.2m |
| 2-3 | 21.0m | 4-8 | 73.2m |
| 2-4 | 21.0m | 5-6 | 72.6m |
| 2-5 | 21.0m | 5-7 | 72.6m |
| 2-6 | 21.6m | 5-8 | 73.2m |
| 2-7 | 21.6m | 6-7 | 72.6m |
| 2-8 | 21.6m | 6-8 | 73.2m |
| 3-4 | 72.6m | 7-8 | 76.8m |

Factor 1.25
Analysis
Scan all

Fig.58

In Fig. 59 shows the results of testing the same cable, but **with an electronic device parallel-connected to wires #2 and #8 that belong to different twisted pairs**. Comparison with the reference (Fig. 55) yields the following differences:

1. Interaction in different twisted pairs is not the same: the pair "1" - "2" exhibits somewhat stronger inductance/capacitance interaction than the other three twisted pairs.

2. Distances to anomalies with peak responses in different "cross-pair" combinations of wires are different: in all of those that include wires #2 and #8, distance to the anomaly is smaller than distances to the end of the cable in all the other "cross-pair" wire combinations.

3. Interactions between wires from different twisted pairs are different: the "2" - "8" pair exhibits the strongest interaction, exceeding that within twisted pairs. It may also be noted that electromagnetic interaction in all the "cross-pair" combinations involving wires #2 and #8, is higher than in other "cross-pair" combinations.

This situation requires testing the "2" - "8" pair from both ends (3.6.1).

The examples above deal with testing a cable consisting of twisted pairs. One may determine whether such a cable is intact, based, among other things, on the structure of electromagnetic interactions between its wires. However, other types of cabling, whether flat or round, do not exhibit such distinct patterns of inductance/capacitance interaction as twisted-pair cables do.

In Figs. 60-62 the results of testing a segment of a round six-core cable are shown.

Fig. 60 shows the results of testing a cable consisting of six 'non-paired' **defect-free wires**.

One may note that magnitudes of inductance/capacitance interaction between the wires are not quite the same for each pair. Therefore, when testing straight (as opposed to twisted-pair) cabling, one should not pay attention to such minor differences. The main criteria for finding out whether the cable is intact will be the distances to anomalies with maximum response. For a defect-free cable, these distances should be approximately the same, and correspond to the length of the tested cable segment, as exemplified in Fig. 60.

Fig. 61 shows the results of testing the same cable, yet **with an electronic device series-connected to wire #6**.

The pattern of electromagnetic interactions between the wires is significantly different from the one shown in Fig. 60. The interactions are greater in all combinations involving wire #6. Besides, all such combinations reveal an anomaly with peak response at a distance of 16m from ST300's connection.

This situation is typical for a series connection or defect in one of the wires. All the combinations with wire #6 should undergo testing from both ends (3.6.1).

| REFLECTOMETER | | | | →0-0 | 00:00 | |
|---------------|------------|------|------------|--------|-------|----------|
| Pair | Level/Dist | Pair | Level/Dist | | | |
| 1-2 | 76.8m | 3-5 | 72.6m | Factor | 1.25 | |
| 1-3 | 76.8m | 3-6 | 77.4m | | | |
| 1-4 | 72.6m | 3-7 | 77.4m | | | |
| 1-5 | 72.6m | 3-8 | 21.0m | | | |
| 1-6 | 76.8m | 4-5 | 79.2m | | | Analysis |
| 1-7 | 76.2m | 4-6 | 72.6m | | | |
| 1-8 | 21.0m | 4-7 | 72.6m | | | |
| 2-3 | 21.0m | 4-8 | 21.0m | | | |
| 2-4 | 21.0m | 5-6 | 72.6m | Scan | | |
| 2-5 | 21.0m | 5-7 | 73.2m | | | |
| 2-6 | 21.0m | 5-8 | 21.0m | | | |
| 2-7 | 21.0m | 6-7 | 77.4m | | | |
| 2-8 | 21.0m | 6-8 | 21.0m | | | |
| 3-4 | 72.6m | 7-8 | 76.8m | | | |

Fig.59

| REFLECTOMETER | | | | →0-0 | 00:00 | |
|---------------|------------|------|------------|--------|-------|----------|
| Pair | Level/Dist | Pair | Level/Dist | | | |
| 1-2 | 36.0m | 3-5 | 36.0m | Factor | 1.50 | |
| 1-3 | 36.4m | 3-6 | 36.0m | | | |
| 1-4 | 36.0m | 3-7 | | | | |
| 1-5 | 36.0m | 3-8 | | | | |
| 1-6 | 36.4m | 4-5 | 36.0m | | | Analysis |
| 1-7 | | 4-6 | 36.0m | | | |
| 1-8 | | 4-7 | | | | |
| 2-3 | 36.0m | 4-8 | | | | |
| 2-4 | 36.0m | 5-6 | 36.0m | Scan | | |
| 2-5 | 36.0m | 5-7 | | | | |
| 2-6 | 36.4m | 5-8 | | | | |
| 2-7 | | 6-7 | | | | |
| 2-8 | | 6-8 | | | | |
| 3-4 | 36.0m | 7-8 | | | | |

Fig.60

| REFLECTOMETER | | | | →0-0 | 00:00 | |
|---------------|------------|------|------------|--------|-------|----------|
| Pair | Level/Dist | Pair | Level/Dist | | | |
| 1-2 | 36.0m | 3-5 | 36.0m | Factor | 1.50 | |
| 1-3 | 36.4m | 3-6 | 16.0m | | | |
| 1-4 | 36.0m | 3-7 | | | | |
| 1-5 | 36.0m | 3-8 | | | | |
| 1-6 | 15.9m | 4-5 | 36.0m | | | Analysis |
| 1-7 | | 4-6 | 15.9m | | | |
| 1-8 | | 4-7 | | | | |
| 2-3 | 36.0m | 4-8 | | | | |
| 2-4 | 36.0m | 5-6 | 16.5m | Scan | | |
| 2-5 | 36.0m | 5-7 | | | | |
| 2-6 | 16.0m | 5-8 | | | | |
| 2-7 | | 6-7 | | | | |
| 2-8 | | 6-8 | | | | |
| 3-4 | 36.0m | 7-8 | | | | |

Fig.61

Fig. 62 shows the results of testing the same cable, yet **with an electronic device parallel-connected to the pair "1" – "6"**.

As is seen from the figure, magnitudes of inductance/capacitance interaction between wires have not changed, as compared with Fig. 60, with the exception of pair "1" – "6", where the interaction is much stronger. Besides, this pair reveals an anomaly with peak response at 16.5m from ST300's connection.

This situation is typical for a parallel connection. The pair "1" – "6" should be tested from both ends (3.6.1).

| REFLECTOMETER | | | |
|---------------|-------|------------|-------|
| Pair | | Level/Dist | |
| 1-2 | 36.0m | 3-5 | 36.0m |
| 1-3 | 36.4m | 3-6 | 36.0m |
| 1-4 | 36.0m | 3-7 | |
| 1-5 | 36.0m | 3-8 | |
| 1-6 | 16.5m | 4-5 | 36.0m |
| 1-7 | | 4-6 | 36.0m |
| 1-8 | | 4-7 | |
| 2-3 | 36.0m | 4-8 | |
| 2-4 | 36.0m | 5-6 | 36.0m |
| 2-5 | 36.0m | 5-7 | |
| 2-6 | 36.0m | 5-8 | |
| 2-7 | | 6-7 | |
| 2-8 | | 6-8 | |
| 3-4 | 36.0m | 7-8 | |

Factor
1.50

Analysis

Scan
all

Fig.62

3.7. CABLE TRACING

Object of Search:

- tracing the cable routes in a facility (non-contact search);
- identifying the contacts of a cable in a junction box (contact search).

This is done in the "CABLE LOCATOR" mode of ST300 (2.4.2.2) with the aid of the Receiver (1.3.4).

Using ST300 in the "CABLE LOCATOR" mode on a powered line is strictly forbidden!

3.7.1. Cable Locator of ST300 in Use: Non-Contact Search

While checking cable lines in a facility, cable tracing may often be necessary, especially when the cabling undergoing tests is embedded within walls, or laid behind non-removable panelling, or in cable trunking that cannot be disassembled, etc.

Without special equipment, tracing cables may be very problematic.

With regular cable locators used in construction and decoration, one can trace straight cables, whereas cables consisting of twisted pairs still pose a problem. The reason is that the operating principle of this category of devices is based on the detection of magnetic field around the cable, and the magnetic components of two wires in a twisted pair practically cancel each other out.

The cable locator of ST300 functions in a different way, detecting the electric component of the field, so all kinds of low-voltage cables are traceable, including those consisting of twisted pairs. However, this operating principle imposes certain limitations on the use of the cable locator of ST300. For instance, tracing power mains cables is impossible.

For a correct operation of the cable locator of ST300,

- connect the line to be tested to the Electronic Switch;
- connect the Main Unit of ST300 to the ground of the power supply on site.

In the "CABLE LOCATOR" mode, a test signal is sent onto one of the wires of the connected cable. The cable is traced with the receiver picking up on the field modulated with a two-tone low-frequency signal. The Receiver unit is equipped with both light and sound indication (LED and inbuilt speaker) of the reception. A three-position sensitivity control is also provided.

When operating the Receiver, please make use of the telescopic arm supplied with ST300.

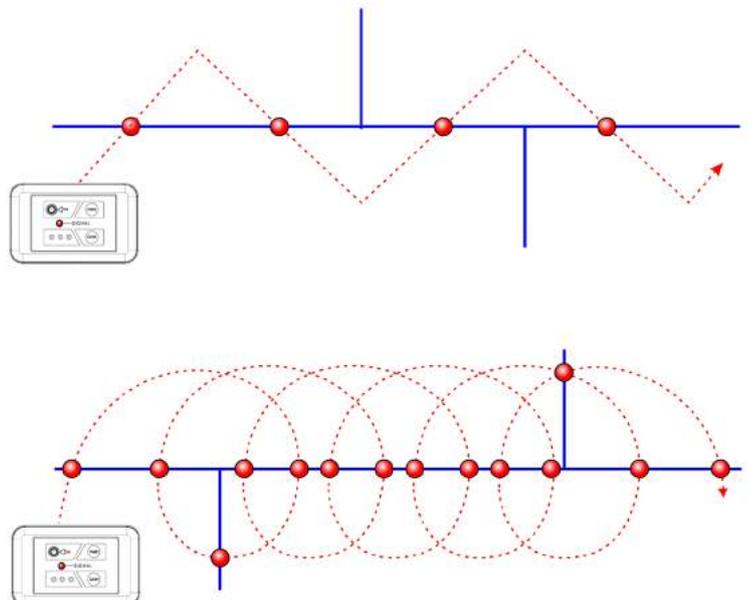


Fig.63

As the detection range is no more than 20-30cm, it is advisable, while tracing, to keep the Receiver 2-3cm away from the surface behind which the cable should be.

It is important to follow the correct trajectory. In the upper part of Fig. 63 the trajectory is incorrect: in this way, branches of the traced line (blue) may be missed out, which is unacceptable.

A recommended trajectory is shown in the lower part of Fig. 63. No branching will remain undetected. For a preciser tracing of the cable route, sensitivity of the receiver should be decreased.

PROCEDURE

Connect the Electronic Switch to the Main Unit of ST300 (1.3.3).

Disconnect all devices from the line. Make sure there are no known connections (branches).

Connect the line to be tested to the Electronic Switch (the way of connection depends on the cable type).

With the Cable (26, Fig.1) connect the "PHONE" socket of the Main Unit to the ground (e.g., to the ground contact of an electric outlet, or grounded housing of any equipment).

Turn on ST300 and go to the Start Menu (2.1 – 2.2).

Go to the main screen of the "SWITCH" mode ("F4" button).

Activate the "CABLE LOCATOR" mode ("FUNC" button).

Set the contact number through which the test signal is to be applied.

If a cable type has been set, the numbers of contacts that are not used with certain cable types (see 2.5.1.1) will be disabled.

If the cable type has not yet been set, it is important to understand which contacts of the Electronic Switch can be used, when setting the contact number in the "CABLE LOCATOR" mode. For example, if the cable is connected to the Electronic Switch through the first four contacts (1,2,3,4), it is one of these four that should be selected.

Insert batteries into the Receiver of the Cable Locator, mount it onto the telescopic arm and insert the plug (3, Fig.6) into the socket (1, Fig.5), as described in 1.3.4.

Turn on the Receiver of the Cable Locator by pressing and holding down the "POWER" button (2, Fig.5).

Using the "GAIN" button (5, Fig.5) set the Receiver to medium sensitivity, with two green LEDs lit (4, Fig.5).

Perform a functional check on the receiver and generator of the Cable Locator, by bringing the receiver up close to Main Unit of ST300. Under normal operation, a two-tone sound will be heard from the speaker.

Passing the receiver unit along the cable as shown in Fig. 63, in the direction away from the Main Unit, monitor the two-tone test sound through the speaker. The further from the Main Unit, the weaker the test signal will grow in the cable, therefore, increasing the receiver's sensitivity with the button "GAIN" (5, Fig.5) may be helpful.

Trace the whole route of the cable throughout the facility. It may be wise to mark it out with paper stickers (plastering them on walls, ceilings, etc.) or otherwise.

3.7.2. Cable Locator of ST300 in Use: Contact Search

At times it is necessary to find the connections (contact terminals, pads, etc.) of the cable to telephone junction boxes. To do that, contact search is required.

For a contact search, there is no necessity to ground the ST300 Main Unit, or use the telescopic arm with the receiver.

PROCEDURE

Before proceeding, make sure there is no voltage on the cabling to be tested!

Connect the Electronic Switch to the Main Unit of ST300 (1.3.3).

Disconnect all devices from the line.

Connect the line to be tested to the Electronic Switch (according to the cable type).

Turn on ST300 and go to the Start Menu (2.1 – 2.2).

Go to the main screen of the "SWITCH" mode ("F4" button).

Activate the "CABLE LOCATOR" mode ("FUNC" button).

Set the contact number to apply the test signal through, bearing in mind which contacts of the Electronic Switch are currently enabled.

Insert batteries into the Receiver of the Cable Locator.

Connect the plug of the Probe (5, Fig.1) into the socket (1, Fig.5) on the Receiver.

Turn on the Receiver of the Cable Locator by pressing and holding down "POWER" (2, Fig.5).

With the "GAIN" button (5, Fig.5) set the sensitivity to a minimum, indicated by one green LED (4, Fig.5).

At the other end of the cable, where it connects to the terminal or junction box, test one by one all the contacts, touching those with the Probe (5, Fig.1).

If the test two-tone signal can be heard from the speaker when a contact is touched, that contact is probably the one you are looking for. Please bear in mind, however, that the test signal can be induced on other wires of the cable, and thus be heard when other contacts are touched. In this case, find the contact where it is the loudest.

If need be, all the connections of the cable to the terminal can be found as described above.

3.8. LOCATING A DETECTED BUGGING DEVICE

Object of Search:

finding the exact locations of eavesdropping electronics detected in the following modes,

"LOW FREQUENCY AMPLIFIER"

"WIRED RECEIVER"

"NONLINEAR JUNCTION DETECTOR"

"REFLECTOMETER"

If the detected transmissions from a bugging device are not encoded (sounds of the surrounding area can be heard from the headphones), the location of the device can be determined with the aid of the Test Sound Player (15, Fig.1) supplied with ST300. This method is called "acoustic search".

If one is looking for a bugging device sending encoded transmissions, or the device has been detected not due to its transmissions, but in the "NL" or "REF" mode, the method to use is non-linear junction location. However, unlike most situations when a nonlinear junction detector is used, the sought object is not just a device that contains semiconductor parts, but one electrically connected to the cable. For this reason, alongside an NLJD, the ST300 must also be used.

3.8.1. Locating a Detected Bugging Device with Test Sound (Acoustic Method)

Let us assume that transmissions of an eavesdropping device have been detected in a line, and that their source is obviously planted in the room where the search is being carried out, because there is an established correlation between the sound output and the test sound from the Player. Now one needs to find the bugging device using the acoustic method.

PROCEDURE

For the above task, two members of the search team will be needed, one of them to move the Test Sound Player around the room, and the other to monitor the signal strength with ST300.

Without exiting the mode of ST300 in which the suspect transmissions have been revealed, connect headphones to the Main Unit. Put the headphones on and adjust the volume. Start monitoring the sounds of the surrounding area.

Decrease the volume on the Test Sound Player.

Move the Test Sound Player slowly around the room.

By monitoring the test sound through headphones, find the location where it is the loudest. The 'listening' device should be close. To tell the location with more precision, the volume of the Test Sound Player should be reduced.

The described procedure is the simplest and quickest, but it can only be used if the data sent by the eavesdropping device is unencoded.

3.8.2. Locating a Detected Bugging Device with ST300 and a Nonlinear Junction Detector

Let us assume that there have been detected signs of bugging a cable line. These can be,

- non-linearity in the tested cable, while all the known electronics have been disconnected from it
- anomaly in the cable supposedly free of any connections or ramifications
- a suspicious signal not correlating with the test sound, yet not issuing from any of the known connected devices.

PROCEDURE

Two members of the search team will be needed for the task, one of them to go the length of the cable with a nonlinear junction detector, and the other to monitor the signal from the NLJD with ST300. As the search may take the two team members far apart, make sure to have cell phones or walkie-talkies handy.

To achieve maximum efficiency of this procedure, one should use a nonlinear junction detector of the CAYMAN line (ST400 or ST401).

The operator of ST300 is to do the following,

Connect the Electronic Switch to the Main Unit of ST300 (1.3.3).

Disconnect all devices from the line.

Connect the line to be tested to the Electronic Switch (according to the cable type).

Turn on ST300 and go to the Start Menu (2.1 – 2.2).

Go to the main screen of the "SWITCH" mode ("F4" button).

In the "SWITCH" mode, set the wire numbers of the "suspect" pair.

Activate the "CABLE LOCATOR" mode ("FUNC" button).

As described in 3.7.1, trace the line where signs of possible bugging have been revealed.

Switch ST300 to the "LFA" mode ("F1" button).

Connect headphones to the Main Unit of ST300, and adjust the volume. Check on the presence of the signal from the nonlinear junction detector in the wires of the active pair. If positive, advise the other member of the team.

The operator of the nonlinear junction detector is to do the following,

Prepare the Nonlinear Junction Detector CAYMAN (ST400 or ST401) for operation.

Activate the Nonlinear Junction Detector and set it to the "SEARCH" mode.

Commence passing the NLJD's antenna along the cable route that has been traced with the aid of the Cable Locator.

If the signal from the NLJD gets re-radiated by any electronics that are close to the line but not connected to it, it is only the NLJD operator who will be getting the response, but not the ST300 operator. If, on the other hand, the re-radiating device is connected to the tested line, its presence will be noticed by both team members, i.e., the NLJD operator's device will be showing signs that there is semiconductor material within its scope, and the operator of ST300 will hear in his headphones a characteristic noise caused by the nonlinear junction detector.

Wherever both operators register such responses simultaneously, is where a hard-wired eavesdropping device is planted.

4. POWER SUPPLY AND BATTERY CHARGING

ST300 is powered from a built-in lithium polymer accumulator battery.

The device should not be operated while it is being charged from the mains.

A full charge provides 7 hours of uninterrupted operation. Battery status is shown on display (4, Fig.12).

A Charger (12, Fig.4.) is supplied with ST300. To start charging, insert the charger plug into the "DC 5V" socket (7, Fig.2) in the side of the ST300 unit, and connect the Charger to the AC mains (220V/50Hz).

The charging process is indicated by the red light of the "POWER" led on the front panel of the device. The full charging time of a discharged accumulator battery is 7 hours.

The device should not be charged while in operation.

5. TECHNICAL SPECIFICATIONS OF ST300

| | |
|--|--|
| Low-Frequency Amplifier | |
| frequency range, Hz | 20....25,000 |
| input impedance, KOhm | 200 |
| gain control range, dB | 0....60 |
| max. input signal amplitude, V | +/-13.8 |
| spectral noise density, nV/Hz | 3 |
| bias voltage range, V | +/-26 |
| data representation | oscillogram spectrogram |
| Wired Receiver | |
| frequency range, kHz | 100....150,000 |
| band scanning time, sec | 2 |
| minimum detection threshold, dBm | -50....-75 |
| dynamic range, dB | 55 |
| input impedance, Ohm | 50 |
| demodulation type | AM, FM |
| filter passband, kHz | 80 |
| maximum permissible voltage in cable, V | 250(AC) 80(DC) |
| data representation | spectrogram oscillogram table view |
| Nonlinear Junction Detector | |
| probing signal amplitude, V | 0....13 |
| probing signal frequency, Hz | 45....55 |
| separate display of odd and even harmonics | available |
| minimum nonlinearity distortion detectable, dB | -60 |
| Reflection Meter | |
| range, m | 0....100 |
| measurement accuracy, percent | +/-1 |
| operation on 'live' cabling | n/a |
| Digital Voltmeter | |
| DC measurement range, V | +/-80 |
| AC measurement range, V | 13 |
| frequency range, Hz | 0....30,000 |
| Cable Locator | |
| test signal carrier frequency, kHz | 100 |
| test signal modulation frequency, kHz | 1...2 |
| test signal amplitude, V | 13 |
| indication | LED, sound |
| contact connection to cable | possible |

| | |
|--|-------------|
| <i>Electric Supply</i> | |
| voltage of the built-in lithium polymer battery, V | 3.7 |
| power intake, Wt | 1.2....2.5 |
| time of continuous operation at maximum load, h | over 7 |
| full charging time, h | 7 |
| <i>Weight and Dimensions</i> | |
| main unit dimensions (length, width, height), mm | 175x83x36 |
| weight of the main unit, kg | 0.375 |
| package dimensions (length, width, height), mm | 390x310x170 |
| total weight with accessories and packing, kg | 4.4 |

6. REFERENCE INFORMATION

6.1. TWISTED PAIR CABLING

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

The idea is to increase consistency between two cores of a pair, as electromagnetic interference from external sources will affect them equally, and to reduce such interference.

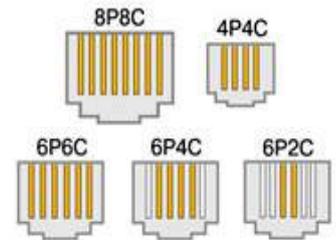
In order to reduce interaction of different pairs in a bundled twisted pair cable (due to periodic mutual proximity of conductor cores from different twisted pairs), cables of the 5th or higher category utilise twisted pairs with different numbers of windings per unit of length.

Twisted pair cables are used in modern structured cabling systems, for telecommunications and computer networking, in various transmission technologies, including Ethernet, Arcnet, and Token Ring. Owing to their inexpensiveness and ease of mounting, these cables are at present the most common choice for wired LANs.

The most typical are twisted pair cables consisting of one, two, and four twisted pairs.

6.2. RJ STANDARDS

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 best known standards of this kind are RJ11, RJ14, RJ25, and RJ45.



| connector standard name | type | no. of cores | 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 |
| RJ14 | 6P4C | 4 | connecting 4-wire telephone sets |
| RJ21 | 50-contact | | connecting PBX's or other telecom equipment (sometimes also called "Telco", or "Amphenol") |
| RJ25 | 6P6C | 6 | connecting 6-wire telephone sets |
| RJ45S | 8P4C, keyed | 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 |

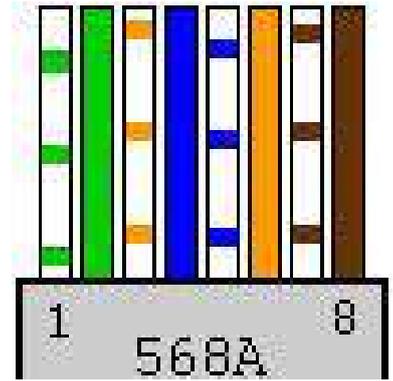
In the notation "xPyC", the letter "P" stands for "Positions" in a plug, and "C", for "Contacts" in a socket.

6.3. WIRING SCHEME OF A 4 TWISTED-PAIR CABLE

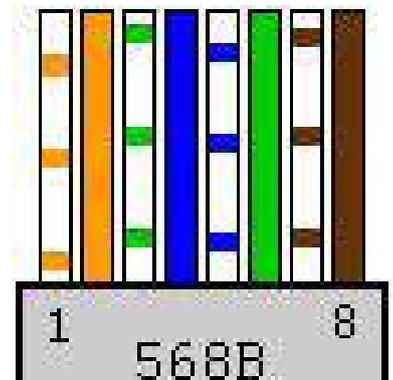
For 10Base-T and 100Base-T Ethernet standards, four cores (orange and green pairs) are used, while the remaining four are reserved for the Gigabit Ethernet (1000Base-T) standard. There are two wiring schemes, 568A and 568B. The latter is more frequent.

OPERATING MANUAL

| first connector # | wire color | second 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 |



| first connector # | wire color | second 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 |



The wiring scheme of a cable linking two network interface cards is only different in that the green and orange pairs have their places swapped at one end of the cable. To put it in simpler terms, one of the connectors is 568A, and the other 568B. This is called a "crossover" aka "null-hub" cable. The same scheme is used for cascading (connecting) hubs. Below is a table to illustrate:

| first connector # | wire color | second 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 |

6.4. WIRING SCHEME OF A 3, 2, AND 1 TWISTED-PAIR CABLE

| RJ contact | 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 |

6.5. REFERENCE INFORMATION ON TELEPHONE LINES

Types of telephone lines

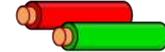
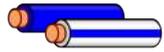
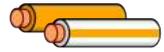
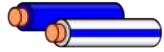
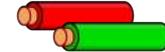
| line type | purpose | user device(s) |
|--------------------------------|---|---------------------------|
| two-wire ¹ analogue | municipal telephone line PBX analogue line | analogue telephone |
| two-wire ² digital | office PBX digital line | digital telephone |
| four-wire digital | office PBX digital lines | digital system telephone |
| four-wire hybrid ³ | office PBX hybrid lines | analogue system telephone |

¹ – analogue signals are transmitted over PBX lines of this kind.

² – in a digital PBX, the analogue electric signal in the speech frequency band is transformed into a coded digital electric signal, that only has two logical values, "0" and "1".

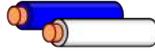
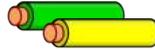
³ – in a hybrid PBX, a "non-digitized" analogue signal in the speech frequency band is transmitted without conversion. The programming of hybrid PBX's is similar to that used in digital ones. The term 'hybrid' means that both system and analogue telephone sets can be plugged in.

Wire pairs carrying telephone line data

| line type | RJ connector | contact # in the RJ connector | wire coloring | |
|-------------------|--------------|-------------------------------|--|---|
| | | | modern | obsolete |
| two-wire analogue | RJ-9 | (2-3)- analogue signal |  |  |
| | RJ-11/14/25 | (3-4) analogue signal |  |  |
| two-wire digital | RJ-11/14/25 | (3-4) digital signal |  |  |
| four-wire digital | RJ-14/25 | (3-4)- digital signal |  |  |
| | | (2-5) – PBX commands |  |  |
| four-wire hybrid | RJ-14/25 | (3-4)- analogue signal |  |  |
| | | (2-5) – PBX commands |  |  |

OPERATING MANUAL

In addition to the above standards, national standards are used in certain countries, such as Germany and Australia (see table below).

| line type | RJ connector | contact # in the RJ connector | wire coloring | |
|-------------------|--------------|-------------------------------|--|---|
| | | | Germany | Australia |
| two-wire analogue | RJ-11/14/25 | (3-4) analogue signal |  |  |
| two-wire digital | RJ-11/14/25 | (3-4) digital signal |  |  |
| four-wire digital | RJ-14/25 | (3-4)- digital signal |  |  |
| | | (2-5) - PBX commands |  |  |
| four-wire hybrid | RJ-14/25 | (3-4)- analogue signal |  |  |
| | | (2-5) - PBX commands |  |  |