Laptiev O., Savchenko V., Shuklin G., Stefurak O.

Detection and blocking of means of illegal obtaining of information at objects of information activity

Tutorial

Kyiv – 2020

STATE UNIVERSITY OF TELECOMMUNICATIONS

DEPARTMENT OF INFORMATION AND CYBERNETIC SECURITY SYSTEMS

Detection and blocking of means of illegal obtaining of information at objects of information activity

Textbook on the subject

Methods and means of technical protection of information

For students Educational-scientific Institute of Information security

Approved for publication by the Academic Council of the Educational and Scientific Institute of Information Protection (Minutes № 3 of 16.09.2020).

Kyiv-2020

CONTENT

Introduction……...4

1. Terms……5

2. Classification of embedded devices and their unmasking features…..……...6

3. Technical means of searching for ED and other means of covert recording of information……8

4. The content and sequence of work on the preparation and conduct of comprehensive special inspections of the premises…….....……10

5. Methods of work at the preparatory stage……...……...…...14

6. Methods of performance of works at the stage of direct carrying out of complex check……17

6.1. Search for embedded devices with a radio frequency transmission channel…..18

6.1.1. Scanning of the radio frequency range, analysis of the electronic situation in the room, detection of radio-emitting ED using SHC DigiScan……...19

6.1.2. Localization of the location of radio-emitting ED using the search device ST 031 «Piranha»…….24

6.1.3. Search and detection of active radio emitting ED using the field detector PROTECT 2103……...30

6.2. Search for embedded devices that use wired communications…….....32

6.3. Search for embedded devices that use low-frequency magnetic radiation…….34

6.4. Search for embedded devices that use infrared radiation……...36

6.5. Search for passive embedded devices……36

6.6. Research of premises for the presence of acoustic and vibroacoustic channel of information leakage ……40

6.7. Visual inspection and physical search of embedded devices…….44

7. Methods of work at the final stage of a comprehensive inspection of the premises...48

Conclusion……...50

References……...51

ADDITIONS

Addition 1. A variant of the plan for conducting a comprehensive special inspection of the premises.

Addition 2. Methods of searching for embedded devices using the search software and hardware complex SHC DigiScan.

Addition 3. Methods of searching for embedded devices using the search device ST 031 «Piranha».

Addition 4. Methods of searching for embedded devices using a nonlinear locator NR-900 EM.

Addition 5. Method of searching for embedded devices using the PROTECT 1203 field indicator.

Addition 6. A variant of the act of complex special inspection of premises.

Addition 7. Variant of recommendations for improving the security of inspected premises and facilities.

Addition 8. The list of normative-legal documents on the basis of which the activity on rendering services on TPI is carried out.

INTRODUCTION

In the face of competition in the international market, the scale of industrial intelligence is growing sharply. The fruits of scientific and technological progress are increasingly used. Industrial intelligence is becoming a more flexible and sophisticated means of obtaining information.

The state by its laws and bylaws has defined the very concept of trade secret, the right of entrepreneurs to protect it from disclosure and theft of information. The administrative and criminal liability of citizens of Ukraine for violation of property rights of the owner of closed commercial information is determined. However, the safety of people and the still imperfection of the law allow criminals to seize with impunity from the owners of their valuable commercial information, which brings huge material and moral losses. Theft of information is carried out through the use of technical means of covert removal of information, the so-called embedded devices.

Embedded devices (ED) are special technical means that are secretly installed in premises, cars, office equipment and other objects of espionage, and are intended for covert recording of information (CRI) of acoustic or specific nature.

The variety of areas and methods of listening has led to the development of various organizational and technical methods of protection. The most important and effective method of technical protection of information is to perform comprehensive special inspections of premises and other facilities with the search and neutralization of CRI.

The purpose of conducting comprehensive special inspections – search for embedded devices, study the level of security of the premises and issue recommendations to improve its information security.

The method of identifying sources of acoustic or video information regulates the nature, list and sequence of performed instrumental and physical search of embedded devices, research of the level of security of inspected objects, as well as reporting and accounting documentation, which is drawn up based on inspection results.

This Methodology uses the recommendations and terminology given in the «Regulations on technical protection of information in Ukraine», State Standard of Ukraine DSTU 3396.2-97, «Instructions on the conditions and rules of activities in the field of technical protection of information and control over their compliance».

The purpose of comprehensive special inspections is to stop (prevent) leakage of information protected from the inspected premises by means of CRI, which will prevent damage that may be caused to the owner, the protected user in case of unauthorized use of this information.

1. TERMS

One of the main ways of comprehensive information protection is a set of organizational and technical measures to inspect the premises in order to identify technical channels of information leakage; disposal of detected embedded devices; development of recommendations and measures to close the identified channels of information leakage; selection, installation, adjustment of technical means of information protection and technical means of control of efficiency of measures of information protection.

The basis of technical information protection is based on the following principles:

- legality (compliance of the enterprise with the laws and regulations of Ukraine);
- confidentiality in the performance of works;
- responsibility to clients and partners, exact fulfillment of all obligations;
- ensuring high quality of services, first-class characteristics and consumer properties of products and services provided at their minimum cost;
- the strictest control of reliability and quality of production and the performed services at all stages of work: from development of the idea and a choice of accessories and technical means to registration of results of work;
- quick response to market demands, providing services based on the best domestic and foreign technologies and technical solutions.

For high-quality performance of the solved tasks, it is necessary to have at the disposal the most modern special search equipment, methodical and normative literature, professional experts.

To date, considerable experience has been gained in organizing and conducting search operations to identify embedded in the premises, objects, electronic devices and other means of information processing for unauthorized receipt of information.

Analysis of the accumulated domestic and foreign experience in the field of information security allows us to conclude that the most complete in scope and range of work are **comprehensive special inspections of premises**, the methodology of which is presented in this *textbook*.

The main tasks of complex special inspections:

- detection and neutralization of implemented CRI tools;
- detection of unclosed potential technical channels of information leakage (TCIL) (ie those that under certain conditions can be used for unauthorized removal of information);
- identification of measures necessary to close (eliminate) identified potential TCIL;
- collection of information on the tactics of application of CRI and their characteristics;
- works on search and neutralization of ED are performed by individuals, organizations and enterprises that have a special permit (license) for the right to carry out activities in the field of technical protection of information (TPI) in accordance with plans, specifications, agreements, directives, etc.

The following are subject to inspection:

- elements of construction of premises;
- technical means of providing information activities (hereinafter - technical means);
- interior items and other items.

Basic principles of organizing and conducting comprehensive special inspections:

- legality - compliance with the provisions of laws and other legal acts governing relations in the field of information protection;
- confidentiality of preparation and performance of works;
- systematic (periodicity) of inspections;
- interrelation with other measures in the general system of information protection;
- complexity of applied methods and technical means;
- sufficiency of the performed works for a reliable assessment of the security of the premises;
- the complexity of the developed organizational, engineering and technical protection measures;
- adequacy of recommended protection measures to prevent leakage of information on identified potential TCIL.

The methodology and the order of search of ED is established taking into account their classification, characteristics of the object which is subject to check, structure of the used search technical means.

2. Classification of embedded devices and their unmasking features

Embedded devices (ED) are secretly installed technical devices designed to secretly capture the following types of information:

- acoustic (speech) information in the premises;
- video information indoors;
- telephone conversations;
- information processed in special technical means: PCs, faxes, copiers, etc.

Embedded devices can be classified on several grounds:

1. By the method of capturing information:
   - ED capture of speech information using acoustoelectric transducers;
   - ED removal of speech and other information circulating in the electrical circuits of technical means;
   - ED capture of information of a species nature using covert video surveillance systems.
2. By frequency range of the transmission channel:
   - microphones and other acoustoelectric transducers of the speech frequency range;
   - supertonal microtransmitters (0.1 - 1 MHz);
   - radio microphones and radio transmitters (0.02 - 1.5 GHz);
   - infrared (IR) wave transmitters (750 - 1150 nm);

These frequency bands correspond to the main types of ED.

3. By type of power supply:

- EDs that do not require a power source (dynamic microphones and other acoustoelectric transducers that have a microphone effect);
- ED with power from an autonomous source (battery, chemical element, etc.);
- ED with power from the mains or communication line, which are under voltage.

4. By mode of operation at a controlled time:

- active - are in the on state;
- passive - are in the off state.

5. By type of activation (inclusion) in the work:

- constantly included;
- with acoustic start - are included on excess of level of acoustic noise over the set value;
- with remote inclusion;
- with program-temporary inclusion.

6. On the used information transmission channel:

- ED using radio frequency transmission channel;
- ED using conductive transmission channels;
- ED using transmission channels based on low-frequency electromagnetic fields;
- ED using infrared transmission channels.

A wide range of principles of action, methods and technologies used to capture and transmit information has led to a significant number of heterogeneous features by which you can detect the embedded device.

The essence of the search for ED is to identify, localize and recognize the unmasking features that are inherent in almost all embedded devices:

1) the electromagnetic fields of the radio frequency transmission channel are emitted;

2) information signals in leading communications;

3) low frequency electromagnetic radiation with a predominance of the magnetic component;

4) infrared radiation modulated by a speech signal;

5) the presence of semiconductor devices in passive ED, which respond to the probing high-frequency signal;

6) unmasking signs that are determined visually.

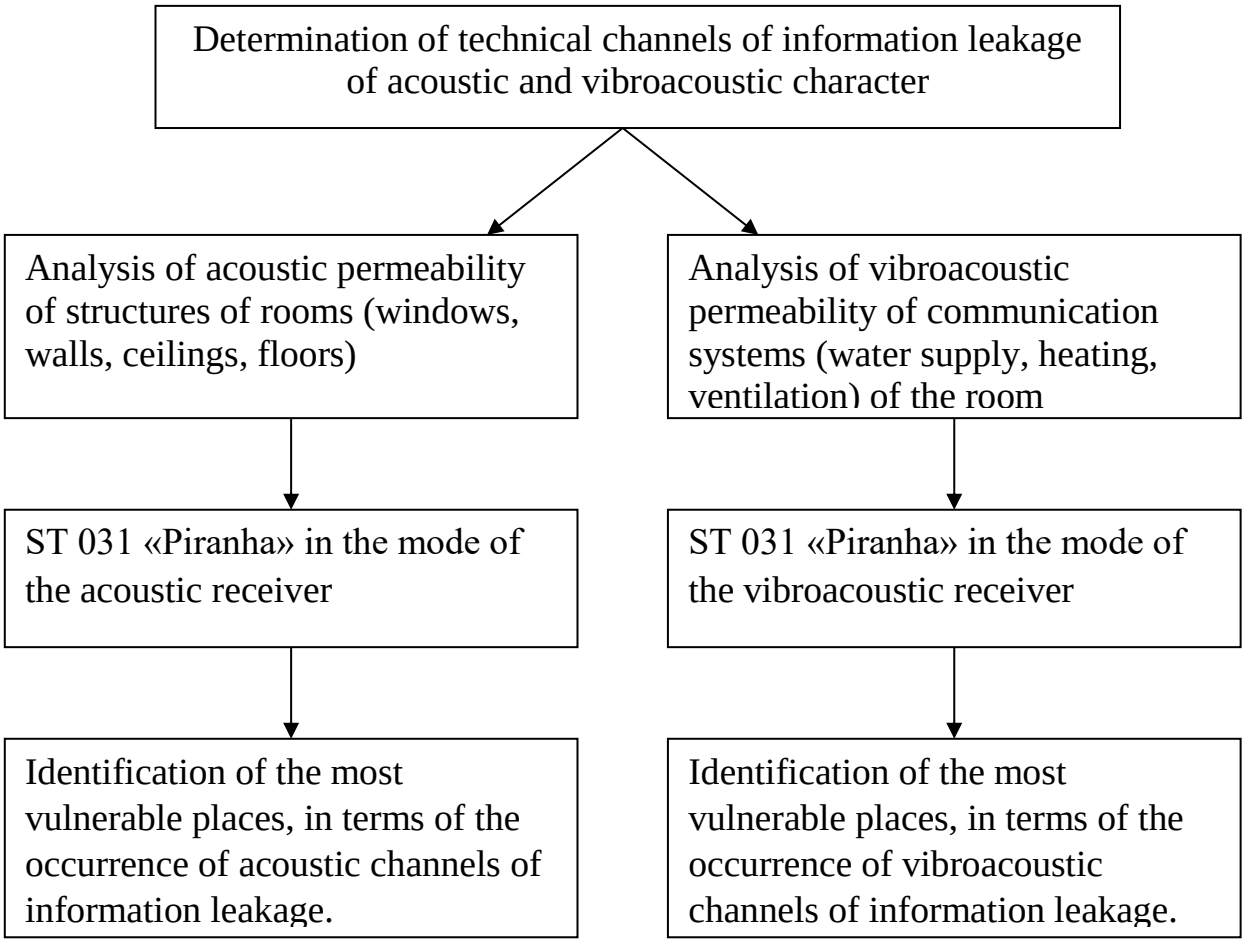
According to the unmasking features are determined:

- composition of special search tools and tools for detecting unmasking signs with the greatest reliability;
- sequence and list of works on search of ED at each stage of carrying out complex special check of rooms;
- features of instrumental search of ED at application of each type of search equipment;
- features of physical (visual) search of ED with use of a complex of search mirrors and other tool;
- features of identification and localization of the location of the ED.

In the process of inspecting the premises, they are also inspected for the presence of possible technical channels of information leakage (TCIL). In particular, such channels are acoustic permeability of building structures, vibroacoustic conductivity of communication systems, water supply and heating pipelines, ventilation systems and others. In Pic. 1 presents the classification of the surveyed information leakage channels, the search equipment used and the expected results of the instrumental control.

3. TECHNICAL MEANS OF SEARCHING FOR ED AND OTHER MEANS OF COVERT RECORDING OF INFORMATION

To perform instrumental control during search operations and examination of the premises for the presence of possible channels of information leakage during the performance of a special comprehensive inspection, special search equipment is used. The list of used equipment and its purpose are presented in table 1.



Pic. 1. Detection of acoustic and vibroacoustic TCIL and type of search equipment

List of special search equipment

Table 1

№	Name of equipment	Purpose of the equipment
1	2	3
1.	Search software and hardware complex DigiScan (or similar) consisting of: - portable computer; - special software DigiScan-2000; - scanning receiver AR-3000 A.	Analysis of the electronic environment on the object, which is tested in a wide frequency range of 0.1 - 2036 MHz, search for radio emitting ED with any type of modulation, as well as ED using both open radio channel and radio channel with spectrum inversion.
2.	Multifunctional search device ST 031 «Piranha».	Detection and localization: - radio-emitting ED, - ED, which work with radiation in the IR range; - ED, which use the transmission lines of various communications for transmission; - EMF sources with a predominance of the magnetic component of the field; - routes of laying of hidden wiring; - possible acoustic and vibroacoustic channels of information leakage.
3.	Nonlinear locator NR 900 EM.	Search for ED containing semiconductor components, regardless of their functional state, including passive ED, sound recording means, ED built into interior elements and building structures - floors, ceilings, walls.
4.	Portable frequency meter RFM-32.	Auto-capture of the frequency of the electromagnetic field with the highest signal level and analysis of the frequencies of operating radio transmitters in a wide frequency range of 10 - 3000 MHz.
5.	PROTECT 1203 field indicator	Operational search and localization of all types of emitting ED, including digital transmitters, as well as transmitters with spectrum inversion.

The choice of these technical devices and their characteristics was justified taking into account the achievement of the following goals:

- the maximum possible reliability of the obtained results;
- the ability to integrate different search methods;
- maximum completeness of instrumental control - the ability to detect all unmasking features and all types of ED and other means of CRI;
- reducing the levels of probability of skipping and the probability of "false alarm";
- the use of advanced methods and technologies of instrumental control that allow you to search with maximum efficiency;
- sufficiency of a set of equipment for instrumental search of all modern ED.

4. THE CONTENT AND SEQUENCE OF WORK ON THE PREPARATION AND CONDUCT OF COMPREHENSIVE SPECIAL INSPECTIONS OF THE PREMISES

The purpose of conducting a special comprehensive inspection of the premises is:

1. termination, prevention of leakage of information protected from the inspected premises;
2. search (detection, localization and identification) of secretly established ED and other means of CRI;
3. examination of premises to identify possible TCIL;
4. development and issuance to the customer of recommendations on elimination of TCIL and increase of safety of the inspected premises;
5. submission to the customer of final and reporting documents on the performed works.

A special comprehensive inspection is organized by the head of the enterprise (Contractor), providing services for technical protection of information and search of embedded devices, on the basis of the Agreement with the Customer. The set of verification measures is performed by specialists of the Contractor's enterprise, which has the relevant state license for this type of activity of the Department of Special Telecommunication Systems and Information Protection of the Security Service of Ukraine.

All measures to conduct a comprehensive special inspection are divided into three stages:

1. Preparatory stage.
2. Stage of direct inspection.
3. The final stage.

The works that make up the content of the ***preparatory stage*** are presented in table 2.

Contents of the preparatory stage of the inspection

Table 2

№	Content of works
1	2
1.	Clarification of the list of protected information and the degree of its importance
2.	Analysis of the preconditions of suspicion, identification of the probable subject that intercepts information, assessment of its capabilities and tactics of action
3.	Preliminary inspection of the premises and the controlled area
4.	Preliminary data collection and analysis of the electronic situation in the area of search operations
5.	Study of plans of premises, schemes of communications, communication, the organization of protection, etc.
6.	Development of a plan for a comprehensive special inspection of the premises: - coordination of the target installation: for counteraction of which subject search measures should be carried out; - coordination of the scale and location of search activities; - coordination of the time of the inspection; - coordination of the cover option under which the inspection will be conducted (testing of measures to preserve the confidentiality of the inspection); - coordination of measures to activate the implemented means of CRI; - coordination of options for action in identifying the means of CRI.
7.	Development of the list of works, the list of the necessary equipment and the tool
8.	Distribution of the involved forces and means on objects and types of works
9.	Clarification of private methods of using the involved equipment in specific conditions of the future inspection
10.	Making a plan for a comprehensive special inspection of the premises and its approval by the Customer
11.	Preparation of forms, schemes, preparations of other documents necessary for carrying out all complex of works
12.	Preparation of equipment for search and research work

Part of the work of this stage involves the participation of the head of the enterprise, which should be inspected. Arrangements for the coordination of some stages of the inspection should be carried out outside the walls of the inspected premises to preserve the confidentiality of future inspections.

A version of the plan for a comprehensive special inspection of the premises is presented in Addition 1.

Stage of direct comprehensive special inspection of premises.

The content of the second stage of work on conducting a comprehensive special inspection of the premises includes the direct conduct of the planned search activities in the premises. Before the start of the search work, the streets and territories adjacent to the investigated premises are inspected. Special attention is paid to people who use headphones, cars with people who are in one place for a long time, cars with an external antenna, an adapter inserted into the cigarette lighter, tinted or curtained windows. In the inspected room, if possible, doors, windows, curtains, blinds are closed to exclude visual contact with a possible observer from the street or adjacent premises. To mask the noise generated by the search equipment, the available sound equipment (radio, player, etc.) is included. The content and sequence of work carried out at this stage are presented in table 3.

The content of the stage of performing an inspection

Table 3

№	Content of works	Search equipment used
1	2	3
1.	Visual inspection of fencing structures, interior items	RFM -32; set of mirrors.
2.	Implementation of the planned measures to intensify the implemented ED and other means of CRI	
3.	Scanning of the radio frequency range, analysis of the electronic situation in the room, detection of radio-emitting ED	SHC DigiScan; ST 031 «Piranha»; PROTECT 1203; RFM -32.
4.	Inspection of lines and equipment of wired communications: - power and lighting power grid; - office and subscriber telephone network; - fire and security alarms; - other wired communications, including unexplained purpose	ST 031 «Piranha»
5.	Detection of sources of low-frequency magnetic fields, routes of laying hidden (unmarked) wiring	ST 031 «Piranha»
6.	Checking the radiation in the infrared wave	
7.	Check of elements of building designs, interior objects with use of a nonlinear locator for search of passive ED	NR 900 ME
8.	Research of sound permeability of elements of constructions, check of engineering communications for presence in them of acoustic and vibroacoustic signals from rooms	ST 031 «Piranha»

1	2	3
9.	Physical search of ED based on the results of instrumental control, as well as search of ED with visual unmasking features	RFM -32; set of mirrors.

Private methods of conducting search operations using specific equipment are presented in Additions 2-5.

The final stage of a comprehensive special inspection of the premises.

At the final stage, the work is performed mainly outside the inspected enterprise, on the premises of the organization conducting the inspection. The content of the final stage is presented in table 4. In addition, Addition 6 presents a version of the act of a comprehensive special inspection of the premises. Addition 7 presents a version of the recommendations for improving the security of premises and facilities.

Contents of the final stage of the inspection

Table 4

№	Content of works
1	2
1.	Processing of inspection results, registration of measurement protocols, carrying out of necessary engineering calculations.
2.	Determination of technical characteristics, consumer properties of the identified ED, approximate time and method of their implementation.
3.	Drawing up a description of the work and research with the addition of the necessary schemes and plans of the premises.
4.	Development of recommendations for improving the security of the premises being inspected: - compilation of a list and diagrams of identified technical channels of information leakage for each room; - assessment of the degree of existing protection of each room from the secret receipt of information on the identified channels of its leakage; - development of additional measures and methods of protection for each channel and premises (organizational, engineering, technical); - compiling a list of technical means and systems recommended for installation to protect information from leakage through technical channels; - development of proposals on ways to use the recommended technical means and systems and combine them into a single, compact information security system.
5.	Drawing up an act of a comprehensive special inspection of the premises.
6.	Submission of final and reporting documents to the head of the enterprise for approval.

5. METHODS OF WORK AT THE PREPARATORY STAGE

The essence of the preliminary stage is to collect initial data about the object, a preliminary inspection of the object, planning and coordination of activities performed during the inspection.

The purpose of the preparatory stage is to develop an inspection plan, its approval by the Customer, as well as the preparation of search equipment and accounting documentation.

The list of works performed at the preparatory stage is provided in section 4 of this Methodology.

Some of the measures of this stage, not related to the inspection of the object, are recommended to be carried out in a neutral area to exclude suspicion from possible observers. All planned and ongoing activities should be carried out without publicity, without attracting the attention of employees who are not familiar with the issue of inspection.

At the beginning of the preparatory stage, the list of protected information, the degree of its importance, the physical media of protected information, possible leakage channels are specified. The peculiarities and procedure of access to the information protected at the Customer's enterprise, the measures of technical protection of information, the composition of technical means of information processing are also subject to clarification. Together with the Customer, the preconditions for suspicion of information leakage are analyzed, it is specified: whether the cause of possible losses is possible leakage of confidential information through technical channels, the probable entity that intercepts information is determined, its capabilities and tactics are assessed. The used equipment for TPI, modes and the order of its use are specified.

To perform quality planning, a preliminary inspection of the premises and the surrounding area. When inspecting the controlled area, the following data are clarified:

- the presence of the protected area, its area, fence, the order of protection (patrolling) of the territory, the presence of parking lots, the ability to monitor or remove information from cars parked near the territory; the presence of adjacent buildings, their purpose and removal from the object being inspected, the possibility of observation or removal of information from these buildings is assessed;
- the electronic situation near the object under inspection is investigated and previously analyzed: frequencies and levels of the most powerful radio signals around the perimeter of the controlled territory are measured and documented with the help of a portable RFM-32 frequency meter. Measurement data: location, frequency, signal level are marked on the diagram for further analysis and comparison with the electronic situation inside the inspected room. For a more detailed study of the electronic situation in the area of the object is used to scan the frequency range using the software and hardware complex SHC DigiScan. In this case, all data on frequencies and signals are entered into the electronic database, which significantly reduces the complexity of the work during the test.

During a preliminary inspection of the premises, the following data are clarified:

- room area, type and structure of building structures (walls, ceilings, floors, ceilings, windows);
- preliminary definition of possible technical channels of information leakage;
- the most probable places are found out by a secret of installation of ED and other means of CRI;
- availability and condition of furniture in the inspected room, availability of office equipment, the order of its use;
- regular cleaning, as well as wiping dust in hard to reach places.

Together with the Customer:

- the results of preliminary inspections on search of ED are specified;
- the time of the last repair of the premises, who carried out, the approximate amount of repair work, who of the employees supervised and supervised the execution of repair work; the possibility of embedding in the building structures of embedded devices is assessed;
- find out from the Customer what interior items and accessories have been installed in the room for the last three months (paintings, flower pots, furniture, etc.), as well as their origin.

If it is necessary to clarify the initial data obtained during the preliminary inspection, the study of floor plans, communication schemes, communications, security organization, etc. At the same time the adjacent premises are specified, the adjacent premises are investigated: what enterprise, a profile of economic activity, adjacent communication systems (heating, ventilation, etc.). Particular attention is paid to the study of communication systems, highways laying telephone lines, the possibility of unauthorized access to them by a possible attacker, specifies the type of office mini - ATS, who is responsible for its programming and other issues to pre-determine possible TCIL.

At the same time, the Customer clarifies the cases of external intelligence in relation to the object, suspicious visitors, external observers and other preconditions of suspicion, assesses possible threats to physical or electronic security.

After that, a preliminary agreement is made with the Customer to develop an inspection plan:

- the target installation is agreed: for counteraction of which object search actions should be carried out;
- coordination of the scale and location of search activities;
- coordination of the time of the inspection;
- coordination of the cover option (legend) under which the inspection will be carried out;
- coordination of measures to test the confidentiality of the inspection;
- coordination of measures to intensify the implemented ED and means of CRI;
- coordination of options for action in case of detection of ED.

The following can be planned as measures to intensify the implemented ED and means of CRI:

- announcement to the employees of the enterprise about an important meeting scheduled for the scheduled time of the inspection;
- planning for the day of inspection of important negotiations, which will then be unexpectedly moved to another room or to another time;
- creating or simulating the acoustic background of the work environment during the test using audio recorders to play previously recorded language.

After clarification of the initial data and approvals, a list of works on the inspection of the premises is developed, based on which the composition of the search equipment and tools for each type of work is determined. Additional equipment for implementation of measures to intensify the implemented ED is being specified. Particular attention when planning should be paid to the scope of a particular type of work. The completeness and depth of search activities, as well as the possibility of performing control operations on the basis of alternative search methods in order to reduce the likelihood of missing embedded devices are determined in advance.

Based on the analysis of the safety model of the studied object and taking into account the available resources, the sequence of planned works is specified and the distribution of forces and means by objects and types of works is carried out. At the same time, the most probable and open technical channels of information leakage are checked first.

Based on the data obtained during the preliminary inspection, the specific methods of using search equipment in the specific conditions of the future inspection are specified.

Based on the results of previous research and coordination of the above issues, a plan for a comprehensive special inspection of the premises is drawn up (Addition 1).

Together with the plan the accounting documentation - forms, schemes, preparations of other documents necessary for carrying out all complex of works is prepared.

At the preparatory stage is also the preparation of equipment for exploration and research work, which includes:

- complexity check;
- checking the battery charge level;
- checking the efficiency of the equipment in each of the planned modes of operation;
- condition of covers, containers, packaging for concealed transportation to the object being inspected.

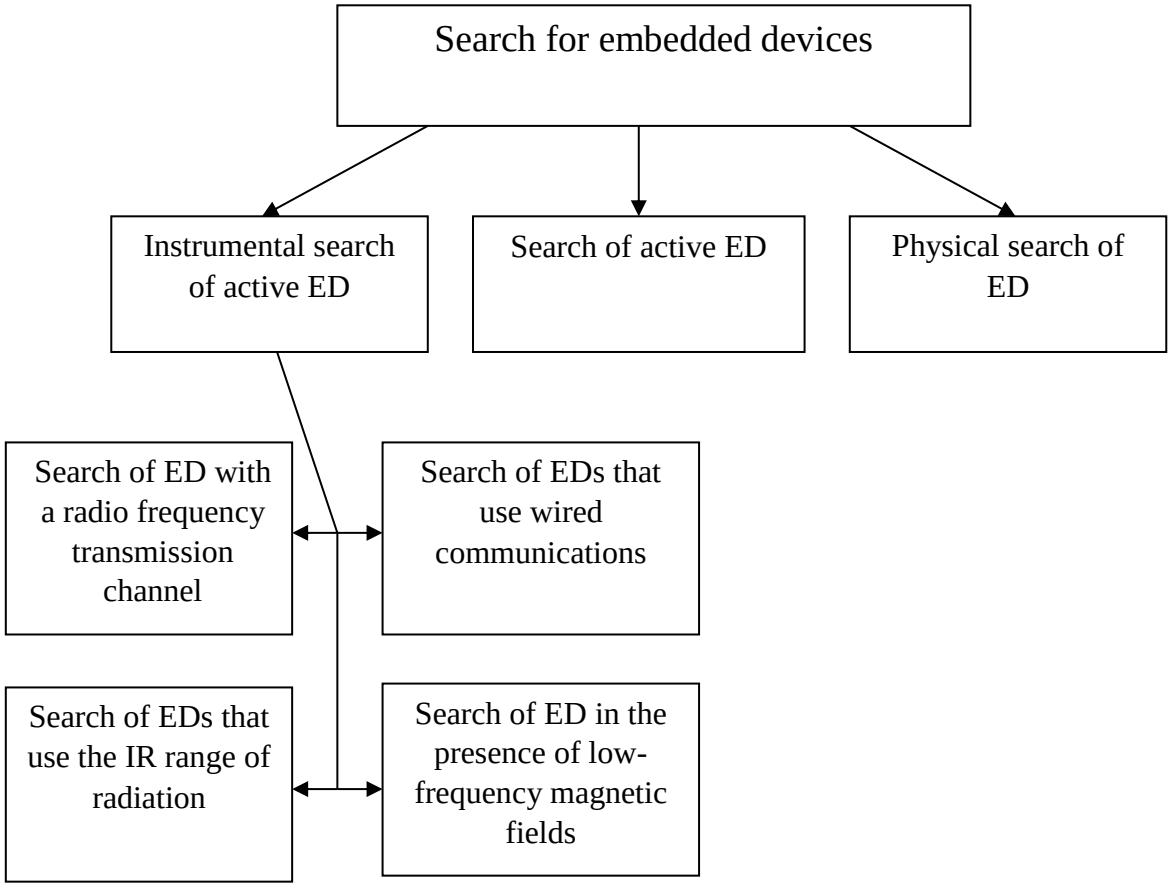
Thus, the preparatory stage is important in conducting a special comprehensive inspection, and high-quality and complete implementation of all measures will significantly increase the reliability of search results, reduce labor costs and duration of work at the stage of direct comprehensive inspection.

6. METHODS OF PERFORMANCE OF WORKS AT THE STAGE OF DIRECT CARRYING OUT OF COMPLEX CHECK

The methodology and procedure for instrumental search of ED is determined by the classification of unmasking features, as well as the types and characteristics of search technical means that are used and should ensure high efficiency of detection, localization and identification of ED.

The whole process of searching for ED logically combines instrumental search and physical search (Pic. 3). Instrumental search for active ED (paragraphs 6.1 - 6.4) is carried out by their unmasking features, which include:

- electromagnetic fields of the radio frequency transmission channel;
- acoustic-electrical conversion signals in wired communications;
- low frequency electromagnetic radiation with a predominance of the magnetic component;
- infrared radiation modulated by speech signals.



Pic.3. The relationship of search activities according to the classification of unmasking features of embedded devices

Instrumental search of passive ED is carried out by the method of nonlinear location on the basis of the analysis of harmonics of reflections of the probing microwave signal (paragraph 6.5).

Visual inspection and physical search of ED is the main type of search and is carried out on the basis of results of instrumental search and taking into account the revealed unmasking signs (paragraph 6.6).

In addition to these works on the search for ED, a study of the sound permeability of building elements, checking the sound conductivity of engineering communications for the presence of acoustic and vibroacoustic channels of information leakage from the premises being inspected (paragraph 6.7).

6.1. SEARCH FOR EMBEDDED DEVICES WITH A RADIO FREQUENCY TRANSMISSION CHANNEL.

The search for ED and other CRI devices with a radio frequency transmission channel is carried out on the basis of radio monitoring. Radio monitoring means a detailed study of the radio situation at the object being inspected, constant monitoring of radio signals and their frequencies.

The main purpose of radio monitoring in the inspection of business objects is to detect the radio signal, determine its frequency, bandwidth, study the signal for correlation functions, amplitude and spectral characteristics, detect the presence of harmonics, classify the detected signal (friendly or dangerous) and enter the results into the database.

Radio monitoring ensures the continuity of receipt, reliability and relevance of data acquisition. Continuity is achieved by the continuity of the monitoring tools, certainty - the documentary nature of the incoming information, relevance - the timeliness of obtaining the necessary data for decision-making.

As the main means of radio monitoring **the automated search software and hardware complex (SHC) DigiScan (or modern analogue of SHC Delta)** as a part is used:

- portable computer;
- special software DigiScan - 2000;
- scanning receiver AR -3000 A.

As additional means of radio monitoring to search for sources of radio radiation are used:

- multifunctional search device ST 031 «Piranha» in the mode of high-frequency detector-frequency meter - to localize the location of the ED;
- field indicator PROTECT 1203 - to detect active EDs embedded in interior items, as well as to detect EDs on moving objects;
- portable frequency meter RFM-32 - for preliminary assessment of the electronic situation in the controlled area, comparison of signal levels inside and outside the object being tested, as well as to detect active EDs embedded in interior items, as well as to detect EDs on moving objects.

6.1.1. SCANNING OF THE RADIO FREQUENCY RANGE, ANALYSIS OF THE ELECTRONIC SITUATION IN THE ROOM, DETECTION OF RADIO-EMITTING ED USING SHC DIGISCAN.

Automated search software and hardware complex SHC DigiScan, consisting of a laptop with special software DigiScan -2000 and scanning receiver AR 3000 A, designed to detect radio signals from embedded devices, determine their frequency, bandwidth, study of signals by correlation functions, amplitude and spectral characteristics, detection of signal harmonics, classification of the detected signal (friendly or dangerous) and entering the results into the database.

The order of deployment, inclusion of the complex is presented in Addition 2 of this technique.

The complex works under the control of the universal search software DigiScan-2000, which implements the following advanced detection methods:

- dynamic threshold;
- signal band measurement;
- checking the presence of signal harmonics;
- passive correlation;
- passive correlation with sounding;
- active amplitude correlation;
- active spectral correlation;
- selection of signals on the total level of danger.

After turning on the SHC to scan the frequency range, the operator must set the following parameters:

1) threshold level and attenuator for each segment of the frequency range;
2) receiver operation parameters: for AR-3000 A the recommended exchange rate is 9600 baud. poll interval 25 ms, number of requests 2;
3) search parameters: the range, the step of the main panorama, the danger threshold are checked (recommended values: 20 - 2036 MHz; 180 kHz; 2 - respectively);
4) analysis parameters:

- the need for additional testing of signals in the modulation of AM;
- harmonics are checked (it is recommended to check 2nd and 3rd harmonics);
- correlation: passive, passive with sounding (for secrecy of check) or active (it is recommended to use when it is possible to unmask search actions);

5) sound settings:

- enable the «Automatic gain control» parameter;
- sound: with passive correlation set the parameter «None», with active CD or MIDI player;
- recording of a sound sample of dangerous signals - 3 s;

6) alert settings:

- sealing alarm: check the box «Upon detection»;
- beep: select a short waf-file.

DigiScan -2000 works in two modes: Search and Manual mode.

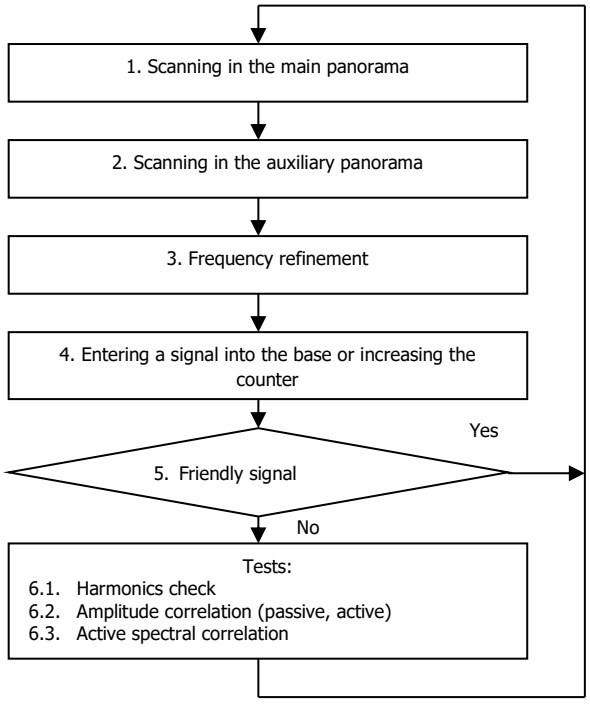
After setting the parameters, the *operator turns on the automatic scanning mode in the specified range* (command «Search» in the menu «Mode»).

In *search mode*, the program automatically scans the specified range, finds signals that exceed the specified threshold, and performs tests set by the operator. If a dangerous signal is detected, the program notifies the operator with a sound signal or displays a message on the screen and includes recording of the sound sample. The signal is entered in the «Dangerous» section of the database. All other signals are entered in the «New» section of the database. All signals fall into the «All» section, regardless of the danger. After several scans of the entire range, the operator stops the search and switches to manual mode.

In *manual mode*, the operator can analyze the search results or try to find new signals. To do this, the operator steps on the range and performs tests on the detected signals. In manual mode, the threshold set by the operator is also used. In manual mode, the operator can view the waveform and the range of signals on the displays «Amplitude» and «Spectrum».

Algorithm for finding dangerous signals.

The algorithm for finding dangerous signals is shown in the block diagram shown in Pic. 4. The current operation is displayed in the status bar at the bottom of the program.



Pic. 4. Block diagram of the search algorithm

Scanning in the main panorama. In search mode, DigiScan -2000 starts scanning in the main panorama. Receiver modulation - WFM, the scanning step is equal to the band of this modulation. For AR 3000 A, this value is 180 kHz. The blue vertical line on the main panorama is a marker that shows the current frequency. On the main panorama, a red line shows the threshold. When the threshold is exceeded, the program remembers the frequency at which the excess began (F 1) and continues scanning to the frequency at which the excess ends (F 2). The program remembers these frequencies and proceeds to a detailed scan in the auxiliary panorama.

The main panorama allows you to display from 0.1% to 100%, from the tested range. To zoom in or out, use the slider at the bottom left of the main panorama. Before starting the search, when the threshold will appear, it is recommended to set the scale to 50-100% to view the entire range.

The threshold is edited before the start of the search using the «Threshold» command of the «Mode» menu item.

Scanning in the auxiliary panorama. Receiver modulation - NFM, the scanning step is equal to the band of this modulation. For AR 3000 A, this value is 12 kHz. The current frequency marker is displayed with a blue vertical line. The scanning range in the auxiliary panorama (f 1, f 2) is automatically calculated by the values of the frequencies F 1 and F 2:

- the beginning of the range f 1 = F 1 - 90 kHz;
- the end of the range f 2 = F 2 + 90 kHz.

After the program finishes scanning in the range from f 1 to f 2, it proceeds to search for threshold exceedances. The picture shows the numbers 1-4, the first four exceedances of the threshold.

The program enters the detected signals in the list, selects the first signal from this list and enters the mode of refining the frequency of this signal.

The main panorama allows you to display from 0.1% to 100%, from the tested range. To zoom in or out, use the slider at the bottom left of the main panorama.

Frequency refinement. In this mode, the DigiScan-2000 specifies the frequency of the signal from the list obtained during the detailed scan. Scanning in the auxiliary panorama was performed with a step equal to the NFM band - 12 kHz. The bug may have a frequency offset relative to the 12kHz grid and the program may be misconfigured and skip it. To avoid this, the program checks the signal level at a frequency less than half the NFM step and more than half the NFM step. If at any of these adjacent frequencies the level is higher than at the center frequency, then this adjacent frequency will be considered the signal frequency. Thus, the accuracy of frequency measurement is increased to 6 kHz.

Entering a signal into the base or increasing the counter. Detected signals are automatically entered by the program into the database, regardless of the level of danger. If the signal is already in the database, its counter is incremented by 1.

Skip friendly signals. If the signal is already in the database and marked as friendly, the search process skips this signal and continues to check other signals or scan. Friendly signals are marked "FR" near the danger level. When working in manual mode, the mark "FR" must be set manually.

Note. Marking signals as "friendly" excludes them from testing during the search. You need to make sure that all signals are safe, otherwise you can skip the bug.

Harmonics check. In this mode, the DigiScan-2000 checks for the presence of the 2nd and 3rd harmonics of the signal. Due to limitations in the volume and power of the bug, as well as the proximity to its antenna, the signal may have harmonics multiples of the fundamental frequency. The presence of harmonics increases the level of signal danger.

Knowing the fundamental frequency of the signal, the program calculates the frequencies of harmonics, multiplying the fundamental frequency by 2 (2nd harmonic) and 3 (3rd harmonic). After that, WFM modulation is installed on the receiver, it is tuned to the harmonic frequencies, and the level is read at these frequencies. If the signal level at these frequencies exceeds the threshold, the frequency is considered to have harmonics.

If the frequency has both harmonics, the total danger level of the signal increases by 1. If there is no harmonic or there is one of the two, the danger level does not increase.

If you tune to the harmonic frequency in manual mode, you can hear the same sound as the fundamental frequency, only with some distortion.

For completeness of the analysis it is recommended to establish always check of harmonics. If the test range starts at a frequency above 1000 MHz, then the 3rd harmonic test does not make sense, because the 3rd harmonic frequency will be higher than the upper range of the receiver. When accumulating a database of friendly signals, it is recommended to disable the harmonic check.

Amplitude correlation.

In this mode, the program measures the relationship between the acoustics, the room being tested and the signal at the audio output of the receiver, which is called correlation (K). At amplitude correlation there is a comparison of amplitude of a signal in time. An active reference microphone included in the set is used to analyze the acoustics of the room. The correlation (correlation coefficient) can be in the range from -1 to +1. If there is a connection between the room acoustics and the signal at the output of the receiver, the correlation will be close to +1. This correlation indicates that the receiver is configured on the embedded device.

In the search mode, the amplitude correlation is performed with several types of modulation - WFM, NFM and AM (set before turning on the search mode).

The results of the correlation measurement are displayed in the lower right part of the main window DigiScan -2000 on the page «Protocol». The amplitude correlation is denoted by K 1. The database gets the maximum correlation value when modulating WFM, NFM and AM and is stored in the field K 1.

In accordance with the value of K1, the level of danger of the tested signal is calculated:

- when K1 = 0-0.33, the level of danger does not change;
- when K1 = 0.33-0.66, the level of danger increases by 1;
- when K1 = 0.66-1.0, the level of danger increases by 2.

Depending on the conditions in which the test is performed, *you can use one of the types of amplitude correlation:*

- passive
- passive with sounding
- active

Passive correlation. Passive correlation is performed silently and does not unmask the search event. There must be some sound in the room for successful passive correlation. This can be music from a CD or MIDI computer player, recording an English course on a tape or a radio. If a radio is used, the frequency to which it is tuned can be entered by the program in the «Dangerous» section. Passive correlation gives less accurate results than active. For example, if in active mode the correlation of a bug is equal to 0.76, in passive it can be 0.45, and sometimes less. If the number of passes in the range is more than one, the probability of passing a dangerous signal is reduced. To increase the accuracy of passive correlation measurement, it is necessary to set the correlation time longer than when conducting active. For passive correlation, it is recommended to set the time to at least 10 seconds.

You can use a computer CD or MIDI player to sound the room. These settings are set on the «Sound» page of the «Settings» command in the «Mode» menu.

Passive correlation with sounding. The same test as passive correlation, except that the program periodically changes the volume of the CD - or MIDI player during correlation measurement. First, the volume becomes maximum, then minimum, etc. This allows you to significantly increase the accuracy of the correlation and not unmask the search process. The listener may think that the volume is just being adjusted. This type of correlation requires the use of sound with a CD - or MIDI -player computer. The time of passive correlation with sounding can be 5-10 s.

Active amplitude correlation. During active amplitude correlation DigiScan - 2000 also compares the amplitude of the room acoustics and the signal from the audio output of the receiver. The difference is that during active correlation, computer speakers reproduce sound pulses, which significantly increase the accuracy and reliability of the search. Sound pulses are reproduced with a random period from 0.2 to 1 s. When using active correlation, the time may be less (3-5 s), although you can set more to increase reliability.

Spectral correlation. In this mode, the program compares the spectrum of room acoustics and the signal from the audio output of the receiver. For successful spectral correlation, it is necessary that a signal with a changing frequency is heard in the room. This is achieved by playing the default.wav sound file with such a signal. The correlation time depends on the length of this file.

Spectral correlation is also performed with several types of modulation - WFM, NFM and AM. The results of spectral correlation are displayed in the «Analysis» tab of the main window in column K 2. The same name has a database field in which the maximum correlation result is stored (with different modulation).

When the spectral correlation is close to -1, it means that there is an inverse relationship between the sound spectrum in the room and the signal spectrum. This is possible when using radio transmitters with spectrum inversion.

In accordance with the value of K2, the level of danger of the tested signal is calculated:

- when K2 = 0-0.33, the level of danger does not change;
- when K2 0,33-0.66, the level of danger increases by 1;
- when K2 0,66-1.0, the level of danger increases by 2.

The general level of signal danger is calculated by the presence of harmonics and by the amplitude and spectral correlation coefficients. If the danger level of the threshold value is exceeded (recommended value 2), the signal is classified as dangerous and is entered into the database of dangerous signals.

Analysis of search results. After several passes and scanning the specified frequency range, you can print the entire database or database of dangerous signals, which records the following signal parameters:

- frequency, modulation, band;
- presence of harmonics;
- values of K1 and K2;
- general level of danger;
- time, date of entering the signal into the database;
- counter value (how many times the signal was encountered during the search);

- comment.

The database has the following sections: «New», «Dangerous», «Friendly», «Everything».

After that, *all dangerous signals are analyzed in detail in manual mode:*

- a dangerous signal is heard;
- the signal is written to the waf-file;
- the oscillogram is analyzed;
- the spectrogram is analyzed;
- the 2nd and 3rd harmonics are listened;
- the amplitude correlation coefficient is calculated;
- the spectral correlation coefficient is calculated.

On the basis of the detailed analysis of dangerous signals *the conclusion* on existence in the checked room of radio radiating embedded device and its characteristics is made.

All work results are automatically entered into the protocol file, which is a reporting document. A printout of the protocol is attached to the inspection report (Addition 6). In addition, the reporting documents include a database of dangerous signals, oscillograms, spectrograms of signals of detected embedded devices.

Localization and search for the location of the detected radio transmission EDs is performed using additional search tools:

- ST 031 «Piranha»;
- PROTECT 2103;
- RFM -32.

6.1.2. Localization of the location of radio-emitting ED using the search device ST 031 «Piranha».

Multifunctional search device ST 031 «Piranha» is designed to carry out activities to detect and localize special technical means of covert information retrieval, to detect natural and artificial channels of information leakage, as well as to control the quality of information protection. It provides the solution of control and search tasks only within the premises (object) or in close proximity to it.

A detailed description of the device ST 031 «Piranha», its preparation for operation, health check and recommendations for its use are given in Addition 3.

Detection of the fact of operation (detection) and localization of the location of radio emitting ED, creating potentially dangerous, in terms of information leakage, radio radiation is carried out in the mode of high-frequency detector-frequency meter (RADIO FRECUENCY CHANNEL).

The effectiveness of the device ST 031 «Piranha» for control and search work is determined by: the degree of readiness of the operator to use the device; completeness and quality of preparatory activities; compliance with the order of the operator's general rules and proven in practice techniques.

The operator must have strong skills of preparation, inspection and control of the device in the provided modes, as well as skills of analysis of the results of auditory and

visual (by oscillograms and spectrograms) control of the parameters of potentially dangerous signals.

Features of the high-frequency detector-frequency meter mode.

In this mode, the device provides reception of radio signals in the range from 30 to 2500 M Hz in the near area (within the object of special work), their detection and output for auditory control and analysis in the form of alternating tonal parcels (clicks), or in the form of explicit phonograms when listening to them both on the built-in loudspeaker and on headphones.

At any given time against the background of a real noise situation, the most powerful of all radio signals in the operating range is received and detected. Its level relative to the set threshold of the detector is displayed on a two-line indicator with a 40-segment scale at the top of the liquid crystal display.

The difference in the use of the two scales is as follows: the upper scale reflects the average value of the detected signal, and the lower its peak values. Accordingly, the upper line will be dominated by signals with a constant frequency (without modulation, frequency modulated), and the lower close to the pulse types of signals (e.g. signals with amplitude and pulse modulation). The presence of an indication on two scales indicates a mixed type of signal at the input of the detector (e.g., television signal).

In the case of reliable signal reception with consciously known parameters, the inscription of the signal identification is displayed under the digital scale of the signal level.

Indication of detection of signals of the following standards is possible: GSM (inscription «GSM»), DECT (inscription «DECT»).

Depending on conditions and the purposes of carrying out control and search works there is a possibility of a choice and installation of necessary (most rational) threshold of the detector.

At the same time, the current values of the frequency of the received radio signal are measured and its most stable value is determined (for signals with a constant frequency). Both values are explicitly displayed on the display screen.

To qualitatively assess the degree of variability of the radio signal frequency, a special computational procedure is used, the results of which are displayed on the display screen in the form of a thin horizontal line that dynamically changes in length directly above the digital symbols of current frequency values. The line length is proportional to the derivative of the frequency of the received signal.

Preparation of the controlled room.

Close doors and windows, as well as curtains or blinds. To reduce the background of the electric field, you need to turn off office equipment, network adapters, transformers, cordless phones, fluorescent lamps and other electronic devices and appliances - potential sources of background increase. These devices should be tested separately, including them in turn. If the premises or adjacent rooms equipped

with active radio masking systems (radio frequency noise generators, etc.) are inspected, they must be switched off during the inspection.

It is recommended that you remove the handsets to activate the phone radio bugs.

To activate radio bugs with acoustic start and ensure the classification of detected radio signals, you need to include an identification sound source, which can be used as a tape recorder or CD player in the mode of music or speech phonogram. It is not recommended to use a radio or a TV for this purpose, as the sound signal generated by them may correlate with the corresponding radio signal on which the transmission is made, received by the device ST 031.

Visually identify potentially dangerous places from which it is advisable to start the inspection (negotiating table, desk and other places of the most probable placement of radio bugs).

The inclusion of the device ST 031 in the mode of high-frequency detector-frequency meter is carried out in the following order:

- make sure that the appliance is switched off («POWER» - «OFF»);
- release the connectors of the main control unit, processing and indication «RF ANT» and «PROBES» from additional external devices;
- connect a telescopic antenna (via an adapter) or a high-frequency antenna to the «RF ANT» socket;
- turn on the power of the device: switch «POWER» - «ON»;
- the LCD backlight will turn on at the same time as the melody signal display and it will appear the inscription «RADIO - FREQUENCY», «CHAN NEL», «30 ... 2500 MHz».

Note. Simultaneous operation of ST 031 «Piranha» with a nonlinear locator is not allowed.

The order of control of the device in the mode of the high-frequency detector-frequency meter.

The «zero» threshold of the detector is set when turned on automatically. If necessary, press the «<» or «>» buttons to set the detector threshold manually, guided by the readings of the additional scale «min - - - | - - -max». If necessary, press the «□» button to return to the automatic threshold setting.

Visually assess the signal level by the number of fully colored elements of the signal level indicators and «by ear» by the frequency of clicks in the built-in speaker or headphones.

If necessary, press the «SET» button to set the required values of the dynamic range: (8 - 16) dB; (8 - 32) dB; (8 - 48) dB.

Press the «RUN / STOP» button and stop (if necessary) dynamic measurements of the radio signal level and frequency. Press this button again to resume dynamic measurements.

Press the «ENTER» button (translation of the sound indication into the «A U D» mode), listen to the presence and content of potentially dangerous modulated radio emissions.

Press the «+» and «-» buttons to set the desired volume output either to the built-in speaker or to the headphones of the audio signal (tone or demodulated).

Press the «OSC» button and go (if necessary) to the Oscillographic control of signal parameters.

Press the «SA» button and go (if necessary) to the analysis of the spectrum of the demodulated signal.

In case of malfunction, press the «RESET» button and restart the device.

Setting the sensitivity threshold of the device ST 031.

Preparation of the device ST 031 «Piranha» (after checking its operability in this mode) is to set the "zero" threshold of the detector, which is, in fact, crucial for successful work. Lowering the threshold will inevitably lead to frequent false alarms, and its overestimation - to the probable omission of the signal ED. Both significantly complicate the work of the operator, increase time and reduce the likelihood of test results. Therefore, to set the «zero» threshold, it is necessary to follow a few simple rules.

It is not possible to install the threshold in the room being inspected, as during the operation of the radio bug already placed in it, the level of its radio emission will be determined by the device as «zero».

It is not allowed the using of radio stations, radiotelephones and other radio emitting means in the process of setting the threshold.

Do not bring the antenna of the device closer to the switched on PC and other office equipment, as SEMI sources in the range of the device.

Do not allow the antenna of the device to come into contact with metal objects and wires as sources of re-radiation of high-frequency signals.

The device should be set up in one of the closest to the premises being inspected, in which, probably, the background level does not differ significantly, and the installation of «radio bugs» is either impossible or impractical. Such premises are usually considered premises of other purpose, but located on the same floor and with window openings facing the same side of the building.

If the object of inspection is a car or other moving object, the setting of the «zero» threshold should be no closer than 10 - 20 meters from it.

After setting the «zero» threshold, the device is moved to the controlled room (to the controlled object) WITHOUT SWITCHING OFF THE POWER SUPPLY. Because each subsequent inclusion leads to automatic installation of a threshold already according to new conditions of an electromagnetic situation.

Following the above rules and restrictions, we can assume that the room being inspected (object) and the device ST 031 «Piranha» are prepared for inspection work.

When conducting search operations, two search methods are used:

- amplitude search method;
- method of searching for «acoustic connection».

Amplitude method.

This method is based on a sharp increase in the level of the received signal and when placing the receiving antenna of the device in the near area of the source.

The magnitude of the detection radius of a local source depends on the power of the signal emitted by it, the pattern and orientation of its antenna and the background level of the electric field at the location of the receiving antenna.

Having detected a dangerous radio signal, it is necessary to move in the direction of increasing its level. The signal level is monitored according to the scale of level indication and increase of the frequency of clicks of the sound alarm system in the «TONE» mode. When painting all segments of the level indication scale, it is necessary to increase its range with the «SET» button, and also to increase the detection threshold with the «<» button.

The method of «acoustic connection».

This method is based on the occurrence of positive acoustic feedback between the microphone of the radio bug and the speaker of the device ST 031. To use this method, you must enable the «AUD» mode. Acoustic connection can occur only in the case of detection of a microphone radio bug, which uses the usual types of amplitude and frequency modulation, and the output of the amplitude detector ST 031 listens to the acoustic background of the room. When there is an acoustic connection, the speaker of the device emits a characteristic «squeak», the tone and intensity of which change when approaching the source (microphone radio bug).

The range of the acoustic effect depends on the volume of the sound emitted by the speaker of the ST 031. By reducing the volume with the «-» button and reducing the area of the acoustic connection, you can achieve the exact location of the source.

It should be noted that the occurrence of characteristic sound when using this method unmasks the work and, if there is a remote control in the radio bug, it can be turned off or tuned to another frequency.

Features of search of radio emitting ED by means of the ST 031 search device.

The radio frequency channel of the ST 031 device is a broadband direct amplification receiver with an amplitude detector, a built-in frequency meter and a wide-range remote antenna. The principle of detection of radio signals with its help is to amplify, detect and determine the frequency of the electromagnetic waves induced in the antenna, the intensity of which exceeds the threshold value (background level). Signs of radio signal detection are:

- staining of positive segments (to the right of zero) on the scale of indication of level. The higher the level of the induced signal, the more colored segments;
- relatively stable frequency value. The limits of frequency fluctuations can be from tenths to several hundredths of a kilohertz and depend on the stability of the carrier frequency of the transmitter, the type of signal modulation, the signal level given in the antenna. For the convenience of estimating the stability of the received frequency above the line Freq = ****. ** a thin horizontal line is displayed, the length of which is proportional to the modulus of the frequency derivative (the more stable the signal frequency, the shorter the line). When the values of several frequency measurements coincide, the

fact of frequency capture is recorded by the appearance on the display of the inscription Capt = ****. ** MHz, with loss of frequency this inscription disappears;
- the appearance of clicks of the audible alarm in the «TONE» mode when the signal level exceeds the threshold by more than four segments. As the level increases, the click frequency increases;
- stable listening of the demodulated signal in the «AUD» mode.

As a result of numerous reflections and re-radiations of electromagnetic waves of external and internal sources in the controlled room the difficult picture of distribution of maxima and minima of intensity of an electric field is formed. This triggers the device display not only if a radio bug signal is detected. In this regard, all detected signals must be classified to assess the degree of their danger and determine the location of the source (external, internal).

Dangerous signals:

a) radio bug signals - the source can be internal or external. Internal - the radio bug is installed in the inspected room. External - the radio transmitter is installed outside the room, but in the area of its reception by the device ST 031, for example:
   - radio microphone with remote microphone;
   - the radio transmitter of the hidden video camera is taken out;
   - radiostethoscope mounted on the outside of the wall;
   - phone radio bug, installed on the communication line outside the room, but in close proximity to it;
b) spatial high-frequency imposition signal - probing signal - external, reflected - internal;
c) SEMI signals from PCs, fax machines and other electronic devices and devices - can be quite powerful and, when used by interested persons of special receiving equipment, it is possible to intercept confidential speech, computer and information transmitted via communication channels. SEMI signals are internal.

Safe signals:

a) signals from external sources (BRS, TVI, radio means, etc.) - are classified "by ear" in the «AUD» mode. Marked with the highest level near the windows, in the corners of the room, near the internal re-radiating and reflective objects and surfaces (large metal objects and surfaces, PC cases, safes, heating batteries, pipes, wires). Frequency stability - low;
b) signals from internal sources (electrical appliances, office equipment, power supplies) - when listening in the «AUD» mode do not contain signs of modulation by the room acoustics and digital transmission. In oscilloscope mode («OSC»), the demodulated signal has a frequency of 50 Hz (or harmonics). Marked in the immediate vicinity of the source.

Features of the radio emitting different ED using the radio frequency transmission channel are described in Addition 3.

After detection and localization of the location of the implemented ED, it is necessary to start the physical search and disposal of the ED. Search results in

accounting and reporting documentation (Add 6). You can also use the PROTECT 1203 field detector or the RFM-32 frequency meter when physically searching for the EDs embedded in the interior items.

6.1.3. Search and detection of active radio emitting ED using the field detector PROTECT 2103.

The PROTECT 1203 field detector is designed to search and detect embedded devices when they are in active mode. With PROTECT 1203 you can check the premises, cars, various interior items, as well as people for the presence of portable transmitters. The search is performed in stealth mode, which uses a built-in vibrator. The device detects that the interlocutor has a working mobile phone. A detailed description of the device is given in Addition 5 to this Methodology.

Search for active ED in the premises.

It is necessary to close all windows and curtains in the room. Turn on lighting and office equipment to create normal working conditions. Before entering the room to be inspected, it is necessary to turn on the device and extend the antenna to medium length. It is necessary to make sure that the first (widest) segment of the antenna is extended. You can hide other segments of the antenna, but the first segment must be extended.

Adjust the sensitivity of the device. To do this, unscrew the adjustment knob until only one segment on the indicator light is lit or flashing. If during the search the operator does not want, or does not have the opportunity to observe the level of the radio field with the help of an indicator light, you can set the sensitivity at which all green segments are lit. In this case, if the operator approaches the radiation source, the red segments will glow and the built-in vibrator will turn on.

The algorithm for finding active ED is based on the amplitude method and includes the following operations:

1. Enter the inspected room, holding the detector upright and observing the readings of the indicator light. Turn lights, office equipment and other electrical appliances on and off. Observe changes in the readings of the device. If they change synchronously with the on / off mark of any equipment, it is a signal of possible presence in this device of the embedded device of unauthorized collection of information.
2. Go around the whole room, watching the readings of the device. As you approach / move away from the radiation source, the displayed radiation level will increase / decrease accordingly.
3. Determine the place with the highest level of radiation by moving the device in all directions and observing the readings of the indicator light.
4. Check all items that may contain embedded devices. The signal of detection of this type of transmitter is a change in the readings of the indicator light.
5. It is necessary to pinpoint the location of the source of illegal radiation. To do this, reduce the sensitivity of the device to a minimum. If the antenna is fully extended, the level of the radio field displayed on the indicator light will not depend on the relative position of the antenna and the transmitter, and a constant level of radiation near the transmitter can be observed. Sometimes the indicator light may show

an increase in the level of the radio field near wires or metal objects. This is due to the fact that metal objects act as an "extension" of the antenna and such situations do not necessarily signal the presence of a transmitter.

6. After finding the exact location of the radiation source, you must begin a physical search. Carry out a visual inspection and check with a detector of each object located in the "danger" zone. If necessary - disassemble lighting fixtures, telephone, power outlets, telephone sockets, fire alarm sensors, etc. Inspect telephone lines and 220 V power lines very carefully. Inspect all interior items, books, table contents, etc.

7. If an embedded device is detected, the further search does not stop. It is necessary to continue the search very carefully, as there is no guarantee that only one ED is implemented in the inspected premises. Professionals often "put" 2 listening devices - one is quite easy to detect, and the other is well disguised, with remote control, with non-standard modulation, etc.

Checking telephone lines.

The telephone bug can be installed on any section of the telephone line: in a telephone set, telephone socket, switch box or on a telephone cable. Most telephone bugs are activated only when the handset is picked up, so the test is performed when the handset is picked up.

You should start the test with a telephone. Place the detector antenna near the device and lift the handset. Observe changes in the level of the radio field. If the radiotelephone is checked, then, naturally, a strong increase in the level of the radio field will be detected when removing the handset from the base, due to the fact that the handset and the base are connected by radio. It should be noted that the cordless phone itself is a wonderful radio bug.

To further search for ED, it is necessary to move the detector antenna along the telephone line with the handset raised. Check all sockets and switch boxes. In the process of checking telephone lines, sockets should be picked up several times and hang up the phone. If it is noticed that the level of the radio field changes synchronously with the raising / lowering of the handset, it can be concluded that there is a telephone embedded device on the line. Then it is necessary to determine the area of the line with the maximum level of radiation and conduct a thorough physical search.

Checking people for the presence of radio emitting ED.

There are a large number of transmitters built into the clothes, personal belongings of the visitor, etc. These devices can broadcast conversations or (and) video information. To check, you need to adjust the sensitivity so that all the green segments of the indicator light. Hide the PROTECT 12 03 field detector in your pocket or under your clothes by first extending the first (widest) antenna segment and turning on the power of the device. When approaching an attacker who has a ED, the built-in vibrator of the detector will be activated, which signals the presence of a radio signal in the device.

An alternative method of checking visitors is to place the PROTECT 1203 detector under a table with an extended antenna as close as possible to the interlocutor. It is necessary to observe changes in the readings of the indicator light when the visitor sits down at the table or gets up from the table.

The results of the instrumental control and search of the ED by the field detector PROTECT 1203 are entered in the accounting and reporting documentation (Add 6).

6.2. Search for embedded devices that use wired communications

For search of ED, using wired communications, the multipurpose search device SWT 031 «Piranha» in the mode of the scanning analyzer of leading lines (WIRE LINES ANALYSIS) is applied.

This mode is intended for search and localization of embedded devices that unauthorizedly transmit information on wired lines (220V, 50Hz network, telephone line cables, local area networks, fire and burglar alarms, etc.). Such embedded devices include:

- embedded devices that use 220V AC lines to transmit intercepted information and are capable of operating at frequencies up to 15MHz;
- PC and other technical means of production, reproduction and transmission of information;
- technical means of systems of linear high-frequency imposing working at frequencies over 150 kHz;
- embedded devices that use subscriber telephone lines, lines of fire and security alarm systems with a frequency of more than 20 kHz for the transmission of intercepted information.

Preparation of the device for work.

Connect the AC adapter to the "PROBES" jack.

Switch on the appliance. "WIRE LINES ANALYSIS" should appear on the display, confirming that the lead line analyzer mode is enabled.

Make sure the device is working using a test network sensor. In the absence of a test network sensor, a sign of serviceability of the analyzer is the reception and detection of signals in the 220V mains (guidance from speech radio stations SW and MW bands).

Use the appropriate adapter cable lugs for easy connection to the line being tested.

In the "PANORAMA" mode, the following functions are available via the "SET" button:

"4" - setting the start and end frequencies of the scan range;

"2" - enable / disable the mode of subtraction of the spectrum shown on the display before the inclusion of this mode, from the newly measured spectrum;

"3" - enable / disable manual adjustment of the lower threshold of the level meter indication;

"5" - select the scale of the amplitude scale "0.1-10mV" or "0.1-1mV".

Check of an electric network of 220B, 50Hz.

When connecting the ST 031 to the mains and checking the connected electrical appliances, be sure to follow the rules and safety precautions, the voltage of 220V is

life-threatening. For the safety of the appliance, do not connect it to a voltage higher than 600 V.

The test must start with the mains sockets. To reduce the noise level in the mains, disconnect from the mains (with visible disconnection of power cords from sockets) all consumers of electricity and equipment located in the controlled room. Connect the tips of the appliance to the mains using one of the sockets. The glow of the two LEDs on the adapter indicates the presence of alternating voltage.

Scan in detail the entire range from 0 to 15MHz, breaking it into intervals. The interval limits are set with the "SET", "4" buttons. The width of the intervals is determined by the load of the range of signals. Start and stop scanning with the "RUN / STOP" button. After passing one or more scan cycles, evaluate the signal levels that exceed the noise level. Manually set the required threshold to automatically stop scanning on the signal. To do this, press the "SET" button, use the "3" button to select the "SQELCH LEVEL" mode, then "ENTER". The threshold level is set with the «Δ», «∇» buttons. For convenience, the threshold level is displayed on the right side of the display with a short horizontal line.

When stopping at the signal, make a precise adjustment with the «<», «>» buttons. Analyze the signal "by ear", including alternate amplitude and frequency detectors with the "ENTER" button.

To analyze weak signals, change the amplitude scale with the "SET", "5" ("0.1-10mV" or "0.1-1mV" buttons). If the signal has signs of modulation by acoustics of the room, for localization of a source it is necessary to use a method of acoustic connection, in turn connecting to all sockets of the checked room. In order to ensure safety, to physically search for a source of dangerous signal in the sockets, they must be de-energized.

After analyzing the detected signals, save the panorama of each interval in the device memory by pressing the buttons: "SAVE", "ENTER".

Check tees, extension cords and appliances, alternately connecting them to the mains.

Check in turn the means of computer and other equipment.

To accelerate the detection of newly recorded signals when turning on the next test hardware, it is advisable to use the mode of subtraction of spectra:

a) call from memory the panorama saved earlier at check of the socket to which the checking device is connected, the "LOAD" button;
b) set the subtraction mode with the "SET", "2" buttons;
c) start scanning with the parameters read from memory by the "ENTER" button;
d) analyze new signals;
e) scan the entire frequency range, calling alternately panoramas of saved intervals, as described above.

Check the lighting network.

It should be noted that with the help of the device ST 031 it is possible to determine only the fact of the presence of interference from the means of computer and other equipment. To determine the degree of their informativeness (danger) and to

draw a conclusion about the need to take additional protection measures is possible only after conducting special studies of specific technical means using special measuring equipment.

Checking telephone lines.

The conductor line analyzer mode can be used to detect telephone bugs transmitting room acoustic information at a carrier frequency of more than 20 kHz over telephone line wires, high-frequency linear interference signals, and unauthorized connection of a telephone microphone (or additional special microphone). to the line when the handset is off.

To carry out the check, it is necessary to connect to the telephone line with needle tips or clamps. The test should be performed with the handset hung up. The analysis of signals is carried out in the same way as when checking the power grid.

Check of security, fire alarm systems and other leading lines.

All conductive lines found in the room (including of unknown origin - in the first place) must be checked in turn. The glow of only one LED on the device adapter indicates the presence of a constant voltage in the line under test.

The analysis of signals is carried out in the same way as when checking the power grid.

The results of the instrument control of the device ST 031 in this mode are entered in the accounting and reporting documentation (Add 6).

6.3. Search for embedded devices that use low-frequency magnetic radiation.

To search for ED using low-frequency magnetic radiation, the multifunctional search device SWT 031 «Piranha» in the mode of the detector of low-frequency magnetic fields (MAGNETIC CHANNEL) is used.

This mode is designed to find and localize the location of sources of electromagnetic fields with a predominance of the magnetic component of the field, the routes of laying hidden (unmarked) wiring, potentially suitable for the installation of ED. Such embedded devices include:

- output transformers of sound frequency amplifiers;
- dynamic speakers;
- electric motors of dictaphones and tape recorders.

Features of the low-frequency magnetic field detector mode.

In this mode, the device provides reception on an external magnetic antenna and displays the parameters of signals from sources of low-frequency electromagnetic fields with a predominant, (available) magnetic component of the field in the range from 300 to 5000Hz.

The identification of signals and their sources is carried out on the basis of the analysis of the oscillogram automatically displayed on the display screen, which reflects the shape of the received signal and the current value of its amplitude. Improving the reliability of identification of signals and their sources is provided by

the possibility of simultaneous analysis of the image on the display screen, listening to the «background» situation using the built-in speaker or headphones.

For work in the conditions of a difficult noisy situation the differential mode of the antenna which is put into action by the switch on its case is provided.

Preparation of the device.

Connect the external magnetic antenna to the connecting cable and the cable itself to the «PROBES» connector. Turn on the power of the device. Oscillographic control of parameters of the signal received on a magnetic field is included automatically.

Visually on the amplitude and nature of the signal on the oscillogram and «by ear» on its key in the built-in speaker or headphones to assess the level of the magnetic field and the presence of the background of the mains 220V, 50Hz or its harmonics. If necessary (in case of a high level of a background of a power supply network) to include a differential mode of the antenna by the switch on its case (position «to a white point»).

Search for signals and localization of sources.

For low-frequency magnetic channels of information transmission is characterized by the fact that they occur when the intended use of authorized means (PCs, intercoms, amplification systems, tape recorders, telephones, etc.). Therefore, one of the main tasks should be considered the study of such tools for the presence, intensity and range of low-frequency magnetic field. Accompanying tasks of finding hidden (unauthorized) wiring and detecting working dictaphones can be considered accompanying.

Potential sources of dangerous low-frequency magnetic fields should be checked separately, including them in the work in turn.

At research of technical means, it is necessary to estimate range of propagation of magnetic fields and features of their spectrum. To do this, first place a magnetic antenna in close proximity to the object under study. Record the relative level of the field on the oscillogram. Moving away from the device under study and changing the spatial orientation of the antenna, estimate the range of reliable reception of low-frequency signal.

When searching for audio frequency amplifiers that have an output transformer, you should evaluate the range of reliable (legible) reception of the speech (test) signal. Such an assessment can serve as a basis for the correct choice of places of installation of appropriate means in relation to the outside of the room and options for their joint location in the room. If necessary, turn on the «SA» mode, analyze the spectrogram and write it to independent memory.

To find the hidden wiring, you must consistently bypass all the walls of the room, having a magnetic antenna in close proximity to them. Fix the area of growth of the field level and by moving the antenna horizontally and vertically to determine the passage of the hidden wiring route.

The ability to detect working dictaphones is determined by both the level of the magnetic field generated by their motors and the level of the magnetic background of the room. Detection of such means is possible at a distance of not more than 30 cm.

The results of the instrument control of the device ST 031 in this mode are entered in the accounting and reporting documentation (Add 6).

6.4. Search for embedded devices that use infrared radiation.

The multifunctional search device SWT 031 «Piranha» in the mode of the infrared radiation detector (INFRARED CHANNEL) is used for search of ED using infrared radiation.

This mode is designed to search for devices for unauthorized transmission of information in the infrared frequency range. Such embedded devices include:

- ED extraction of acoustic information with its subsequent transmission to the IR range;
- technical means of spatial tracking in the IR range;
- laser systems for recording acoustic information.

Preparation for work.

Connect the IR sensor to the «PROBES» socket.

Switch on the appliance. "INFRARED CHANNEL" should appear briefly on the instrument display.

Check the operation of the device in this mode. Any infrared remote control from household audio and video equipment can be used as a test sensor for infrared radiation.

When setting the threshold, do not point the IR sensor towards powerful sources of IR radiation (electric heaters, incandescent lamps, direct sunlight).

Search for signals and localization of sources.

Features of IR transmitters:

a) a direct optically transparent channel between the IR transmitter and the receiving device is required;
b) there may be a narrow pattern of the IR transmitter.

Given these features, the search for dangerous signals should start from the windows of the room, moving into the depths of the room, and changing the spatial orientation of the IR sensor.

The analysis of the detected signals is performed "by ear" in the "AUD" mode, as well as visually, using the "OSC", "SA" modes. The localization of such devices can be carried out both by the amplitude method and by the acoustic method.

The results of the instrument control of the device ST 031 in this mode are entered in the accounting and reporting documentation (Add 6).

6.5. Search for passive embedded devices.

A nonlinear locator ED 900 EM is used to search for passive EDs (which are in the off state), as well as EDs with a low level of unmasking features.

The principle of operation of this device is based on the method of nonlinear location. Its essence is that all nonlinear components of electronic devices (semiconductor devices) have the physical property to emit into the air, when irradiated

with UHF signals, harmonic components, multiples of the irradiation frequency. Thus, it is possible to detect any embedded devices that contain semiconductors. Such embedded devices include:

- passive ED;
- ED with hidden transmission channels;
- ED with a low level of DMP;
- ED of ultrasonic and infrared ranges;
- means of sound recording: dictaphones, tape recorders.

Features of nonlinear locator operation.

The nonlinear locator consists of one transmitter and two receivers tuned to the 2nd and 3rd harmonics. After switching on the NR 900 EM, the underlying surface is irradiated with a UHF signal. Semiconductor devices located in the irradiation zone, the signal is re-emitted and received by receiving antennas. Receivers allow the operator to represent the level of harmonic components of the reflected signal in visual and audio form. Determination of nonlinear components is possible at a distance of about 0.7 m from the transmitting antenna. The energy potential of the locator provides an effective search for embedded EDs in interior elements and in enclosing building structures. However, a significant disadvantage of the locator is the difficulty of identifying artificial semiconductors from natural (corrosive) nonlinear reflectors. In addition, using a nonlinear locator does not detect:

- ED, located in the cavities of metal objects;
- ED, located in structurally complex electrical products (refrigerator, air conditioner, etc.);
- ED, located in radio and electronic devices of general purpose;
- ED, which do not have semiconductor devices, operate in the microwave frequency range, have a high degree of shielding.

Despite these shortcomings, this locator is the most effective means for detecting and locating passive ED.

Addition 4 provides a detailed description of the nonlinear locator and the procedure for working with it.

Preparing the locator for work.

Secure the antenna system to the boom using the mounting assembly. Connect the antenna system to the transceiver following the color coding. Switching on the locator without the connected antenna system is not allowed.

Connect the headphones to the «PHONE» jack of the receiver. Install the battery or connect the power adapter connector to the DC 15 V jack. Connect the control cable to the CONTROL jack of the receiver. The LCD screen should read: "RADAR TURNED OFF". The device is ready to turn on.

The order of detection and search of embedded devices.

Before switching on the device, make sure that the antenna system is connected.

Press the ON / OFF button of the control panel only once - the mode in which the transmitter is installed, receivers are switched on, receiver attenuators are set to minus 10 dB, headphones are connected to the output of the receiver of the second harmonic, volume - in the middle position.

Using the ATT button to set the maximum sensitivity of the receivers, the LCD screen in the left part of the 1st and 2nd line should play the characters 00. Aiming the antenna system in different directions and connecting the OUT 2/3 headphones to the outputs of the receivers of the second and third harmonics, make sure that there are no interferences at the reception frequencies at the maximum sensitivity of the receivers. Otherwise, evaluate the possibility of working with the locator by setting the attenuators of the receivers so that the interference signal is below the sensitivity threshold.

Press the ON / OFF button on the control panel a second time - the «300» mode must be switched on - the transmitter output power is maximum.

Note. The third press of the ON / OFF button turns off the unit, and "RADAR TURNED OFF" appears on the LCD.

Switching headphones from one harmonic to another is done with the OUT 2/3 button. In case of overload of receivers in this line the inscription appears: "OVER".

The power is changed with the MAX / MIN button.

Use a standard simulator to make sure that the device works. To do this, place the simulator in a free place in the absence of electronic equipment nearby. Set the maximum level of the probing signal with the MAX / MIN button and the maximum sensitivity with the ATT button. Use the OUT 2/3 button to switch the headphones to the output of the 2nd harmonic receiver. Aim the antenna system towards the simulator from a distance of 0.7-0.8 m. The headphones should listen to a tone with a frequency of 300 Hz medium volume, and the LCD screen in the 1st and 2nd line should reproduce the level of the received signal of the 2nd and 3rd harmonics, respectively. And the level, on the display in the right part, should be not less than 10-15 and 5-10 dB accordingly, and the difference of levels which is specified in the 3rd line, should be not less than 5 dB. Removing the simulator from the sounding zone at a constant position of the antenna system should lead to the disappearance of the response signal.

Search for semiconductor elements, working depending on the noise situation as much as possible with maximum power and maximum possible sensitivity. To do this, move the antenna system along the surface to be inspected. When a tone signal with a frequency of 300 Hz appears in the headphones, it is rough to determine the location of the reflective object. As the antenna system approaches it, the intensity of the tone in the headphones will increase.

Monitor the ratio of response signals of the 2nd and 3rd harmonics on the LCD screen. In the case of a significant excess of the signal level of the 3rd harmonic over the 2nd, it is most likely that the source of the response signal is corrosion nonlinearity.

To more accurately identify the response, without changing the orientation and location of the antenna system, switch the analyzer to "20K". To do this, press the "300/20 K" button.

Set the maximum transmitter power, maximum receiver sensitivity and maximum signal volume in the headphones. Make sure that the modulation signals of the second harmonic of the probing signal are listened to.

Bring the antenna system as close as possible to the surface being inspected at the point of detection of the reflective object. Move the antenna parallel to the

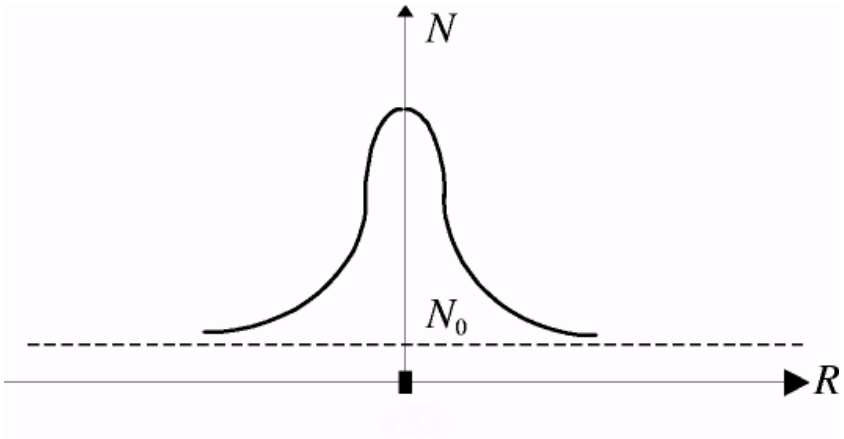
examined surface from the point of detection to the periphery by 30 ... 40 cm and back, monitor the noise level in the headphones.

Depending on the nature of the reflective object - a corrosion diode or an artificial semiconductor element (radio electronic device), there may be two fundamentally different dependences of the noise level in the headphones on the movement of the antenna system along the examined surface. Their typical appearance is presented in Pic. 5, 6.

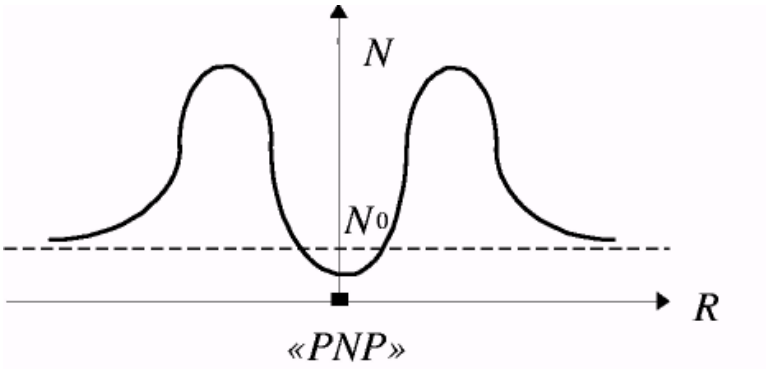
To increase reliability, it is recommended to listen to the noise response in the analyzer headphones in the «20K» mode when tapping the location of the reflective object, any non-metallic object. The corrosion diode is usually characterized by a hoarse irregular crunch.

When switching to the mode of listening to the modulation of the third harmonic of the probing signal, depending on the noise in the headphones, the opposite (curves shown in Pic. 5 and 6, change places).

A significant excess of the 2nd harmonic of the probing signal over the 3rd harmonic (20 dB or more) with a high degree of probability indicates the artificial nature of the reflection of the p - n junction.



Pic. 5. The dependence of the level of modulation noise of the 2nd harmonic of the corrosion p-n junction on the distance from the object to the axis of the antenna of the locator system: K is the location of the corrosion p-n junction; N - noise level in the headphones; N_0 - noise level in the headphones in the absence of a nonlinear reflective object; R is the distance from the location of the reflective object to the axis of the antenna system of the device.



Pic. 6. The dependence of the level of modulation noise of the 2nd harmonic of the semiconductor p-n junction from the distance from the object to the axis of the antenna system of the locator: «PNP» - the location of the semiconductor element; N - noise level in the

headphones; N0 - noise level in the headphones in the absence of a nonlinear reflective object; R is the distance from the location of the reflective object to the axis of the antenna system of the device.

The results of the instrument control of the device NR 900 EM are entered in the accounting and reporting documentation (Add 6).

6.6. Research of premises for the presence of acoustic and vibroacoustic channel of information leakage.

Unauthorized removal of acoustic information from the inspected premises can be carried out not only with the help of embedded devices, but also from other technical channels of information leakage (TCIL) from adjacent premises. Such channels include:

- soundproof building enclosing structures of the premises (walls, floors, ceilings, windows, doors, etc.);
- sound-conducting building constructions and systems of engineering and technical communications (heating, water supply, etc.);
- soundproof cavities and channels in building structures (ventilation ducts, cable shafts, niches, through holes, etc.).

To identify the most vulnerable places, in terms of vibroacoustic and acoustic channels of information leakage, as well as to assess the effectiveness of vibroacoustic protection systems and their sound insulation, the search device ST 031 «Piranha» is used in the modes: vibroacoustic receiver (VIBRO - ACOUSTIC) receiver (ACOUSTIC CHANNEL).

Features of the vibroacoustic receiver mode.

In this mode, the device provides reception from an external vibroacoustic sensor and displays the parameters of low-frequency signals in the range from 300 to 6000 Hz.

The state of vibroacoustic protection of premises is assessed both quantitatively and qualitatively.

Quantitative assessment of the security status is based on the analysis of the oscillogram, which is automatically displayed on the display screen, which displays the shape of the received signal and the current value of its amplitude.

Qualitative assessment of the security status is based on direct listening to the received low-frequency signal and analysis of its volume and timbre characteristics. To do this, use either a built-in speaker or headphones.

Features of the acoustic receiver mode.

In this mode, the device provides reception to an external remote microphone and display the parameters of acoustic signals in the range from 300 to 6000 Hz.

The state of sound insulation of premises and the presence of vulnerable, in terms of information leakage, places are determined both quantitatively and qualitatively.

Quantitative assessment of the sound insulation of the premises and detection of possible channels of information leakage is based on the analysis of the oscillogram,

which is automatically displayed on the display screen, which reflects the shape of the received signal and the current value of its amplitude.

Qualitative assessment is based on direct listening to the received acoustic signal and analysis of its volume and timbre characteristics. To do this, use either a built-in speaker or headphones.

Preparation of the device.

To switch the device to the vibroacoustic receiver mode, it is necessary to connect an external vibroacoustic sensor to the «PROBES» socket. Turn on the power of the device. Oscillographic control of parameters of the signal received on the vibroacoustic channel is included automatically.

To switch the device to the acoustic receiver mode, it is necessary to connect a remote microphone to the «PROBES» jack. Turn on the power of the device. Oscillographic control of the parameters of the received acoustic signal is turned on automatically.

Evaluation of the effectiveness of vibroacoustic protection and sound insulation of premises.

The combination of these uses of the device is determined by the common sources of information leakage channels (speech signal in the acoustic range), the similarity of control techniques and the practical identity of the capabilities of ST 031 «Piranha».

First, in both cases, when preparing the room, you must turn off devices and tools that create an additional acoustic background.

Second, in both cases, test, and preferably calibrated, audio sources should be used.

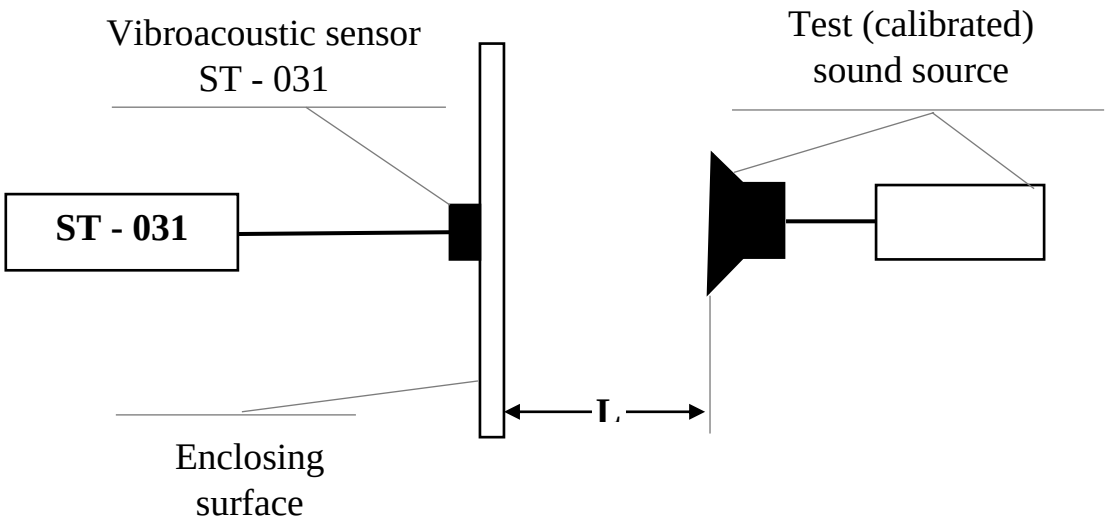
Thirdly, in adjacent, in relation to the premises being inspected, the minimum possible level of acoustic background must be provided.

Fourth, use almost the same methods of signal analysis ("by ear", on oscillograms and spectrograms).

Evaluation of the effectiveness of vibroacoustic protection of the premises is usually carried out in two stages. At the first stage, protection, if any, should be excluded and the actual vibroacoustic properties of the enclosing surfaces of the surfaces should be checked. For this purpose, it is necessary to attach the vibroacoustic sensor in various places of surfaces which are checked (walls, doors, windows, if possible a floor and a ceiling) from the external, in relation to the controlled room, parties.

Turn on the test audio source. It can be placed either in the usual place of confidential conversations, or at a certain distance from the surveyed surface (for example, as shown in Pic. 7).

The sound level is usually set to the appropriate volume (74 dB). For calibrated sound sources, the distance «L» is chosen within 1-2 m. First, the vibroacoustic properties of the examined surfaces are evaluated at a qualitative level (by direct listening), and then, by switching to «SA» mode, the amplitudes of the frequency components of the test signal are quantified.



Pic. 7. Scheme for assessing the vibroacoustic properties and vibroacoustic protection of premises

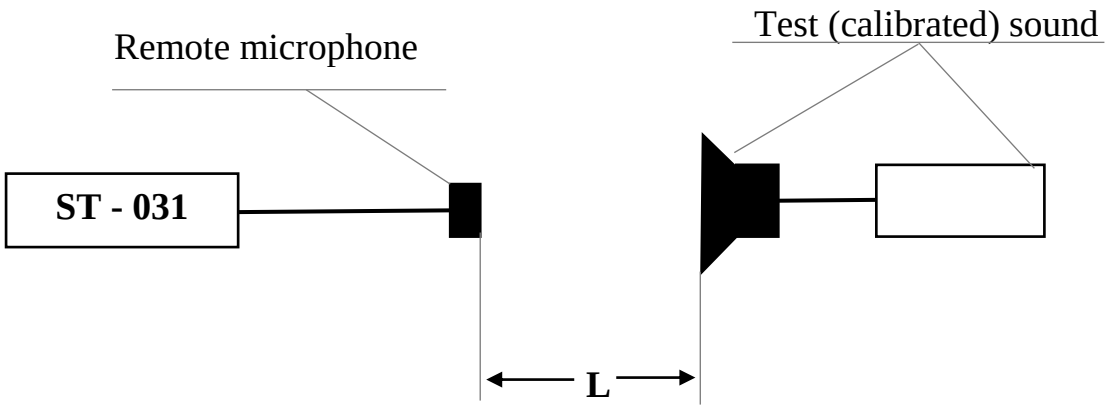
In the second stage, if provided, the effectiveness of the vibroacoustic protection system is evaluated. To do this, on each surface, both qualitatively "by ear" and quantitatively on the spectrogram, the ratio of the levels of the test and masking signal is determined, and the «undisguised» components of the spectrum are detected. This serves as an objective basis for the correction of the amplitude-frequency characteristics of the masking signal sources.

According to the generally accepted rules, the legibility of speech signals is guaranteed not to be restored if the noise that masks (interference) is 4-5 times (16 dB) higher than their level. Complete exclusion of speech features is achieved when the signal level is exceeded 8 times by an obstacle created by the active protection system.

It is also advisable to assess the sound insulation of the premises in two stages.

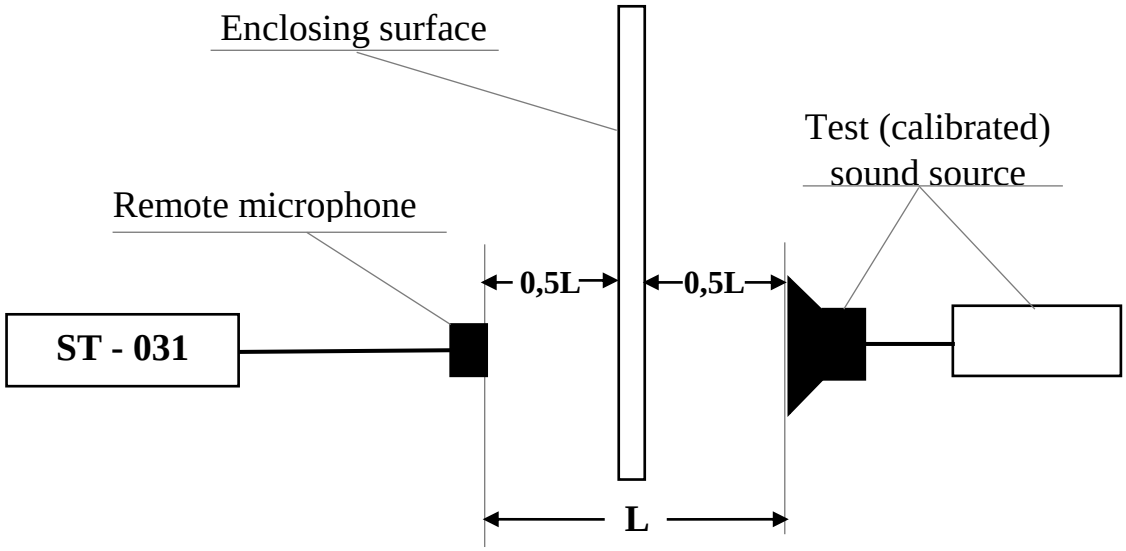
In the first stage, using a test signal source with a sound level corresponding to the loud speech, to establish a correspondence between this level and the readings of the device ST 031 in the modes of the oscilloscope and spectrum analyzer. To do this, place the acoustic emitter of the sound source and the microphone of the device ST 031 at some fixed distance. It is usually chosen within 1-2 m (Pic. 8).

The second stage evaluates the sound insulation properties of the enclosing surfaces of the room (walls, doors, windows, and if possible, floors and ceilings), the effectiveness of the active protection system (noise), as well as the possibility of leakage of acoustic information through ventilation elements, various niches, through holes, etc.



Pic. 8. Scheme of calibration of indicators of level of a sound signal of the ST 031 device

To assess the sound insulation properties of walls, doors (floors, ceilings), the test sound source can be located either in the usual place of confidential conversations, or at a distance from the inspected surface. For example, in the embodiment shown in Pic. 9.



Pic. 9. Scheme of assessment of sound insulation of premises

Placing the microphone in different places of adjacent (above and below) rooms qualitatively «by ear» and quantitatively on the spectrogram to determine the range of interception of speech information from the room and assess the reduction of the sound signal due to the properties of enclosing surfaces, as well as the least weakened components of the spectrum. The latter makes it possible to make an informed decision about the need for additional protection, including active and the choice of characteristics of protection.

If the room is located above the first floor, there are some difficulties in checking the sound insulation of window structures. In this case, the following, often used technique gives a sufficient effect for qualitative assessment. The test sound source is placed using one of the previously discussed options. The window, transom or other

part of a window opens, depending on features of window frames. The microphone is hung outside and in this position the level of the test signal received by it from the room is fixed. Then open the window carefully (so as not to damage the microphone cable), but, if possible, tightly covered. Qualitatively «by ear» and quantitatively by the oscillogram or the spectrogram sound-insulating properties of window designs are estimated.

Since the air ducts of ventilation systems are considered to be the most dangerous channels of leakage of speech acoustic information, they are subject to mandatory inspection. To do this, the microphone of the device ST 031 must be inserted into the outlet (inlet) of the air duct of each of the adjacent rooms, and possibly some others. Qualitatively «by ear» to assess the passage and legibility of the signal from the test source, and the indicators of the device ST 031 in the mode of the oscilloscope or analyzer of its attenuation spectrum when passing through the air duct to the location of the microphone. Thus the correct estimation of attenuation can be received only if there is a detailed scheme of ventilation system. Its presence makes it possible to take into account the attenuation introduced by various elements of the design of air ducts. Thus, the attenuation of the speech signal is usually:

0,15 dB / m - in direct metal air ducts;

0,2 - 0,3 With dB / m - in direct non-metal air ducts;

1,0 - 3,0 dB / m - when changing the cross section of the duct;

3,0 - 7,0 dB / m - per bend of the duct.

The results of the inspection serve as an objective basis for deciding on the need for additional protection, for the choice of measures and means of ensuring it. All results of work according to inspections are entered in the accounting and reporting documentation (Add 6).

6.7. Visual inspection and physical search of embedded devices.

According to the results of instrumental control, localization of the location of embedded devices, a physical search and disposal of ED is carried out. Visual inspection of fencing structures, furniture and other interior items for the presence of embedded devices in them is a mandatory and necessary element of the search work. A thorough inspection is always associated with the movement of furniture and objects, which after the inspection of the premises must be left in the position and form in which they were before the inspection. Therefore, before the inspection is recorded, up to photography, the placement of all objects in the room.

In the process of inspection, you should look for new, previously not inherent in this room, possibly thrown objects, as well as signs of possible use of interior elements

and construction of the room for the introduction of embedded devices. Such features include:

- rearrangement of furniture and objects, the appearance of new, previously unnoticed elements and details;
- displacement of objects, coverings and furniture from their usual places;
- traces of opening of panels and other removable elements of a design of the room and subjects;
- traces of recent sealing of holes, fresh plaster or painting surfaces, etc.

At visual inspection of the room it is recommended:

- raise and inspect the bottom of the floor covering (carpets, strips, linoleum), paying attention to areas uncharacteristic of this coating: inserts, gluing, patches;
- inspect the floor surface, explore areas with traces of recent painting, repair, use of tools that violate the integrity of the surface;
- inspect plinths, carefully examine places with traces of recent repairs and possible intrusion, if necessary, carry out their temporary dismantling to inspect the space under the plinths, make sure there are no conductive and fiber-optic lines under the plinths;
- open and inspect the channels under the floor, paying special attention to the underside of removable covers, the existing grooves and cracks, traces of their recent sealing; carefully, to the maximum possible depth with the use of an endoscope to inspect the contents of the pipes that approach the underfloor ducts, to make sure that there are no foreign objects and wires in them; during the inspection, it is recommended to remove the standard wires and cables from the mortgage pipes (cable channels) to the maximum possible length in order to make sure that there are no unauthorized connections to the wires;
- carefully inspect the places of passage through the floor of water pipes, steam heating pipes and other communications, because in these places it is easiest to mask the traces of intrusion during the installation of CRI.

Visual inspection of the walls. When inspecting the walls, you need:

- free their surface from superimposed objects and coatings (paintings, mirrors, carpets, etc.);
- inspect the surface of the walls, paying special attention to places that differ in color or texture from the rest of the surface; mark suspicious places on the floor plan for further investigation with the help of special technical means;
- in case of pasting of a surface of walls by wall-paper carefully to examine places of roughnesses, joints of wall-paper, patches, cuts and tears, to be convinced of density of adjoining of wall-paper to a wall surface; if necessary, open the wallpaper, which peeled off to check the contents of the formed cavity;
- in the case of wall binding, pay special attention to the presence of traces of drilling and subsequent clogging of holes;

- if there are technological, communication and other niches in the walls, which are closed with removable covers or panels, the niches should be inspected in accordance with the recommendations for inspection of underfloor ducts.

At visual inspection of ventilating and other technological apertures and cavities it is recommended:

- check the integrity of the grille that closes the hole or lid on the special marks applied during the preliminary inspection;
- remove the grilles that cover the hole, make sure there are no traces of violation of the dust layer around the hole and on its inner surfaces;
- make sure there are no foreign objects and wires in the hole, cavities and pipes that fit into the cavity, for which use mirrors, endoscopes and lights.

At visual inspection of windows, it is necessary:

- to inspect the surfaces of the window sill, window opening and window frame, paying special attention to the existing gaps and cavities, the tightness and uniformity of the seals, traces of violation of the integrity of the surface;
- open the window and make sure that there are no foreign conductors and objects on the inner and outer surfaces of the window frame, traces of dismantling or replacement of seals, locking elements, fasteners;
- in case of double frames to carry out their dismantling, to be convinced of absence of extraneous conductors and subjects in between frame cracks;
- carefully inspect all surfaces and cavities of cornices and blinds, folds of curtains, make sure there are no foreign objects;
- by inspecting the areas of external walls adjacent to the window opening, make sure that there are no foreign objects, patches or other traces of possible intrusion on them; special attention should be paid to areas hidden from surface inspection of water-repellent visors.

In most rooms under the windows are radiators of the steam heating system. The complex configuration of radiators, often the use of decorative screens that hide the radiators and pipes of the heating system from surveillance, create favorable conditions for installation in these places embedded devices.

At visual inspection of a door it is recommended:

- to inspect cracks behind platbands of a door box, are convinced of absence of traces of dismantling of platbands; in case of suspicion of their opening to dismantle platbands, to examine the grooves and cracks hidden by them, to be convinced of absence of traces of their recent laying;
- to be convinced of absence of traces of opening of a door upholstery and a door cloth, in suspicious cases to remove and examine the reverse side of a door upholstery and the surface of a door cloth hidden by an upholstery;

- inspect the elements of the door hinge and make sure there are no traces of their dismantling; in case of suspicion to dismantle door hinges and to examine the surface of a door box or a door cloth hidden behind them;
- when inspecting metal doors, pay special attention to traces of drilling holes in the door leaf and door frame, traces of temporary dismantling of locking elements and door hinge elements; in suspicious cases to dismantle the lock and to examine internal cavities of a door cloth by means of an endoscope.

When visually inspecting the ceiling, you should pay attention to areas with traces of recent painting, repair, leakage, through the passage of pipes and other communications. The inspection of a false ceiling needs special attention. Such a ceiling consists of removable, fixed to the frame, panels and can easily be used by an attacker to install ED. Inspection of a false ceiling, as a rule, is combined with visual inspection and check of lines and the equipment of the leading communications established on a ceiling.

Before opening the ceiling panels, make sure that the marks left during the preliminary inspection are intact. In case of violation of the labels or detection of traces of possible opening of the panels, the inspection of the panel space should start from suspicious places. When opening the panels, first of all, their reverse side is inspected. Particular attention should be paid to the inspection of grooves and opaque bottom surfaces of the frame. The use of viewing mirrors is absolutely necessary. In the process of inspection of the panel space, a parallel inspection is carried out with dismantling and disassembly of lighting, signaling and other devices mounted on the ceiling.

Visual inspection of furniture is carried out in the following sequence:

- furniture surfaces (shelves, drawers, seats, etc.) are freed from objects and coatings, removable and easily removable elements are removed for separate inspection;
- surfaces of the main constructive elements for detection of the fixed foreign objects and details, openings of unclear purpose, inserts, stickers, seams, other traces of invasion are inspected; special attention is paid to the comparison of the thickness of the walls and panels, inspection of the rear and lower surfaces of the elements, grooves and gaps, as well as folds and seams of upholstered furniture;
- the surfaces of fasteners and fasteners are inspected to identify traces of possible dismantling of furniture in order to hide behind the fasteners of the CRI; to facilitate further control of the inviolability of the fasteners and fasteners, it is advisable to cover the heads of the fasteners and the joints of the elements with a thin layer of marked paint;
- the inspection of external and internal surfaces which can be taken out and easily removable elements according to recommendations from the review of the main constructive elements is carried out.

Upon completion of the inspection of furniture, and sometimes in parallel with it, a visual inspection of other interior items: which stand alone on the floor, hung on the walls, placed on windowsills or furniture surfaces.

Special care should be taken to inspect items that are constantly on the desk or in the immediate vicinity of the manager's desk. Folders with documentation, books, picture and mirror frames, trash cans, flower pots and houseplants, clocks, figurines and other items that have cavities inside them, the size of which allows you to place in them ED are subject to inspection and verification.

It is recommended to conduct a physical search and visual inspection not only in the premises indicated by the head of the enterprise who ordered the inspection, but also in adjacent ones.

Detection of a masked dictaphone, a dropped radio microphone or other CRI device should not cause superficial execution of other search operations provided for in the plan, moreover, their folding and termination.

The results of the work on the physical search of embedded devices and visual inspection of the premises are entered in the accounting and reporting documentation (Add 6).

7. METHODS OF WORK AT THE FINAL STAGE OF A COMPREHENSIVE INSPECTION OF THE PREMISES

The final stage of verification is the final of all search activities.

The purpose of the final stage is the processing of inspection results, preparation of reporting documentation, preparation of the act of inspection of the premises.

At the beginning of the final stage, the results of the inspection are processed, measurement protocols are drawn up, and the necessary engineering calculations are performed. If an embedded device is detected on the object, then, based on the results of measuring the frequency and amplitude of the radiated electromagnetic field, the maximum distance from the ED to the possible means of information registration is calculated for it.

To study the new, previously unknown means of CRI, the technical characteristics and consumer properties of the detected embedded devices are determined, the approximate time and method of their buging are determined. Based on the study of these data, the unmasking features of the detected ED are analyzed in detail and their identification is performed according to the ED classification (section 2). If necessary, additional instrumental checks should be performed for the detected unmasking signs and methods of their masking.

For drawing up of the act of check the description of the carried-out works and researches with the appendix of the used schemes and plans of rooms is carried out.

Based on the results of instrumental control and physical search, recommendations are developed to improve the security of the premises being inspected. The following works are performed to make recommendations:

- the list and schemes of the revealed TCIL is made;
- an assessment of the degree of existing protection of each room, which is checked against CRI by detected TCIL;
- additional measures and methods of protection are developed for each detected channel;
- a list of technical means and systems recommended for installation to protect information from leakage through technical channels;
- proposals for ways to use the recommended technical means and systems are developed.

On the basis of the work performed, an act of inspection of the premises is drawn up, which includes the results of the work performed and recommendations (Add 6, 7). If necessary, recommendations are also issued to the Customer on the inspection of computers and scanners for the presence of implemented EDs in organizations that provide this type of service.

CONCLUSION

Accurate execution of all operations described in this Methodology, combined with high professionalism of performers and the use of advanced search equipment, allows you to effectively conduct comprehensive special checks for the presence of embedded devices and other means of covert recording of information on business objects.

This Methodology is a set of logically interconnected procedures and operations that allow with high reliability to detect, locate and identify active embedded devices on the following unmasking features:

- *electromagnetic fields of the radio frequency transmission channel;*
- *acoustic-electrical conversion signals in wired communications;*
- *low frequency electromagnetic radiation with a predominance of the magnetic component;*
- *infrared radiation, which is modulated by speech signals.*

The search for passive embedded devices that do not show any unmasking features is proposed to be carried out by a new advanced method of nonlinear location, based on the physical properties of all nonlinear components of electronic devices to emit into the air, when irradiated with UHF signals, harmonic components, multiples of the irradiation frequency.

Particular attention in this Methodology is paid not only to the search for embedded devices, but also to the preparation of accounting and reporting documentation, the development of recommendations for improving the technical security of information at business facilities.

References

1. The law of Ukraine "On information". dated 2.10.1992 p. № 2657-XII.
2. Law of Ukraine" On information protection in automated systems " dated 5.07.1994 No. 80/94-BP.
3. Law of Ukraine "On state secrets" of 21.01.1994 No. 3855-XII.
4. Law of Ukraine" On licensing issues of commercial trade and types of economic activity " dated 1.06.2000 No. 1775-III.
5. Regulations on technical protection of information in Ukraine, approved by the resolution of the Cabinet of Ministers of Ukraine of 27.9.1999 No. 1229.
6. Regulations on the Department of special telecommunication systems and information protection of the security Service of Ukraine, approved by the Cabinet of Ministers by decree of the President of Ukraine of 6.10.2000 No. 1120.
7. License conditions for the implementation of economic activities related to the development, production, implementation, maintenance and research of the effectiveness of systems and means of technical protection of information. Provision of services In the field of technical protection of information.
8. Recommendations for conducting inspections of premises, special and general-purpose technical equipment for the presence of embedded devices intended for taking information with boundary access via acoustic and second channels. Department of special telecommunication systems and information protection of the security Service of Ukraine.
9. Technical descriptions and instructions of information security tools.
10. Laptiev O.A., Savchenko V.A., Barabash O.V. Savchenko V.V., Matsko A.I. The metod of searching for digital vtfns of illegal obtaning of information on the basis cluster analysis. Magyar Tudományos Journal. Budapest, Hungary, 2019. № 31. P. 33 – 37
11. Laptiev O., Kliukovskyi D., Barabash A., Zidan A., Analysis of Existing Signal Detection Methods, Development of a Technique for Calculating the Probability of Secret Information Capture. International Journal of Science and Engineering Investigations (IJSEI). Denmark. 2019. Vol. 8, Issue 92. P. 99 – 103.
12. Laptiev O., Sobchuk V., Barabash O., Musienko A. Analysis of the main Approaches and Stages for Providing the Properties of the Functional Stability of the Information Systems of the Enterprise. Sciences of Europe. Praha, Czech Republic. 2019. Vol. 1. No 42. P. 41 – 44.
13. Laptiev O. A., Voichenko T. A., Kudyukin P. V., Stepanenko V. I. Method for estimating signal parameters of unauthorized data acquisition tools based on correlation and regression analysis. Scientific journal "Science-intensive technologies" K: NAU, 2019. no. 3 (43). P. 313 – 320.
14. Laptiev O. A., Polovinkin I. M., Klyukovsky D. V., Barabash A. A. Model of searching for means of tacit obtaining information based on differential transformations. Sciences of Europe. Praha, Czech Republic, 2019. Vol. 1. No 43. ISSN 3162-2364. G. 59-62
15. Laptiev O. A., Sobchuk V. V., Savchenko V. A. Method for improving the noise immunity of the system for detecting, recognizing and localizing digital signals in information systems. Collection of scientific papers of the Military Institute

of the Taras Shevchenko national University of Kyiv. K: OKNU, 2019. Issue 66. Pp. 124-132.

16. Laptiev O. A. Methodology for determining the probability of secret receipt of information by a potential violator. Science and Education a New Dimension. Natural and Technical Sciences. Budapest, Hungary, VII (24), Issue: 200, 2019. ISSN 2308-5258. P. 27-31.

17. Khoroshko V. A., Chekatkov A. A., Kovtanyuk Yu. S. Methods and means of information protection. K.: Junior. 2003. 502 p.

18. Khoroshko V. A., Chekatkov A. A. Methods and means of information protection. K: 2003. 214 p.

19. Khoroshko V. A. Khokhlacheva Yu. E. Assessment of security of information systems. Modern information security. 2012. No. 4. P. 50 – 57.

20. Decree of the President of Ukraine No. 1229 of September 27, 1999 "Regulations on technical protection of information in Ukraine".

21. Silantev V. A. Application of vector analyzers in radio monitoring systems. Special equipment. 2002. No. 5. P. 25 – 37.

22. Radzievsky V. G. Sirota A. A. Theoretical foundations of electronic intelligence. Publishing House «Radiotechnics» 2004. 432 p.

23. Regulatory document of the system of technical protection of information ND TPI 1.5-001-2000 " Radio detectors. Classification. General technical requirements».

24. Regulatory document of the system of technical protection of information ND TPI 2.3-001-2001 " Measuring radio detectors. Methods and means of testing".

25. Regulatory document of the system of technical protection of information ND TPI 2.3-004-2001 " Indicator radio detectors. Methods and means of testing".

26. Regulatory document of the system of technical protection of information ND TPI 2.3-005-2001 "Panoramic radio detectors. Methods and means of testing".

27. Regulatory document of the system of technical protection of information ND TPI 2.3-006-2001 "Analyzing radio detectors. Methods and means of testing".

28. Regulatory document of the system of technical protection of information ND TPI 1.4-002-08 " Nonlinear radars. Classification. Recommended testing methods and tools".

29. Regulatory document of the system of technical protection of information ND TPI 2.7-011-2012 " Protection of information on objects of information activity. Guidelines for developing a method for detecting embedded devices»

30. Ensuring security around the world is our constant mission [Electronic resource] / / Symantec (Norton Security). 2015. Access mode to a resource: http://www.symantec.com/ EN/EN/

31. Maksimenko G. A., Khoroshko V. A. Methods for detecting, processing and identifying signals of radio-embedded devices. To: Poligraphical-ting, 2004. 317 PP.

32. Laptiev O. A., Dryagin A. B., Yudenok I. S., Blazhenny V. I., Shevchenko Yu. V. Modern trends in the development of communications and radio engineering support for flights. Theses: Scientific and technical seminar of the National Academy of defense of Ukraine. Kyiv, January 21, 2003, Pp. 9-14.

33. Krivtsun A.V. Zakharov A.V. Use of new capabilities of the complex of radio monitoring and digital analysis of signals "Cassandra-M" for detection of modern

special technical means with information transmission via radio channel [Electronic resource] access mode: http://www.inspectorsoft.ru/article.php?id=388 (24.05.2019)

34. Cyber spy attacks the special services of Ukraine [Electronic resource] ESET. 2015. Access mode: http://eset.ua/ru/news/ view/390/operation-potao.

35. Zhurilenko B. E., Khoroshko V. A. Systems and devices for information protection. K: NAU, 2004. 63 p.

36. Zhurilenko B. E., Levandovskaya L. I., Nikolaeva n. K. Protection of acoustic information in the room by a tonal signal. Information protection. K: NAU, 2007. P. 36-39.

37. Zabara S. Characteristics of model systems in environment MATLAB. K.: View. University "Ukraine", 2011. 137 p.

38. Law of Ukraine "On the State service for special communications and information protection of Ukraine".

39. Zakharov A.V. Requirements for a promising network analyzer

40. Wi-Fi [Electronic resource] access Mode: http://www.analitika.info/ (25.05.2019).

41. Anansky E. V. What are radio tabs and how to detect them? (part 2) / magazine " Security Service " [Electronic resource] access mode: http://www.kvirin.com/articles/267/

42. The law of Ukraine "On information". https://zakon.rada.gov.ua/laws/main/2657-12

43. The Law of Ukraine "On access to public information".

44. The Law of Ukraine "On information protection in information and telecommunication systems". https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80

45. For the Law of Ukraine " On basic principles of cybersecurity of Ukraine" https://zakon.rada.gov.ua/laws/main/2163-19

46. Law of Ukraine "On electronic documents and electronic document circulation". https://zakon.rada.gov.ua/laws/show/851-15

47. Resolution of the Cabinet of Ministers of Ukraine "On approval of the Rules ensuring information security in information, telecommunications, and information and telecommunication systems " from 29.03.2006 No. 373. https://zakon.rada.gov.ua/laws/main/373-2006-%D0%BF

48. Resolution of the Cabinet of Ministers of Ukraine " On approval of the Procedure connection to global data transmission networks " No. 522 dated 12.04.2002.

49. Resolution of the Cabinet of Ministers of Ukraine "On approval of the list mandatory stages of work during design, implementation and operation systems and means of automated data processing and transmission " from 04.02.1998. № 121. https://zakon.rada.gov.ua/laws/main/121-98-%D0%BF

50. Resolution of the Cabinet of Ministers of Ukraine "On approval of General requirements for cyber protection of critical infrastructure objects " from 19.06.2010. No. 518.

51. Resolution of the Cabinet of Ministers of Ukraine "On approval of the standard instructions on accounting, storage, use, and destruction of documents and other material media containing service information " dated October 19, 2016 No. 736.

52. DSTU 33960-96. The protection of information. Technical protection of information. Fundamentals. http://www.dsszzi.gov.ua/dsszzi/control/uk/publish/article?art_id=38911&cat_id=38836

53. DSTU 33961-96 Protection of information. Technical protection of information. The order of operations. http://www.dsszzi.gov.ua/dsszzi/control/uk/publish/article?art_id=38911&cat id=38836

54. ND 1.6-005-2013 Protection of information on the objects of information activities. The regulation on the categorization of objects, where information with restricted access circulates and does not constitute a state secret. https://zakon.rada.gov.ua/rada/show/v0215519-13

55. ND TPI 1.1-002-99. General terms for protecting information in computer systems from unauthorized access. http://195.78.68.84/dsszzi/control/uk/publish/article?showHidden-1&art id-302408&cat_id=89734&ctime=1547122731920

56. ND TPI 1.1-003-99. Terminology in the field of information security in computer systems from unauthorized access. http://www.dsszzi.gov.ua/dsszzi/control/uk/publish/article?showHidden=1&art id=89740&cat id=89734&ctime=1547204009788

57. ND TPI 3.6-003-2016 Order of work on creation and certification of technical information security systems.

58. ND TPI 1.4-001-00. Model Provision on the information security service in an automated system. http://www.dut.edu.ua/uploads/I 1023 75718671.pdf

59. ND TPI 1.6-003-04 Creation of technical protection complexes information on objects of information activity. Development rules, build, display, and design a threat model for information.

60. ND TPI 2.5-004-99 Criteria for evaluating the security of information in computer systems from unauthorized access. http://dstszi.kmu.gov.ua/dstszi/doccatalog/document?id=106342

61. ND TPI 2.5-005-99 Classification of automated systems and standard functional profiles of security of processed information from unauthorized access (with change # 1). http://dstszi.kmu.gov.ua/dstszi/control/uk/publishvarticle showHidden=1&art_id=101870&cat id=89734&ctime=1344501089407

62. ND TPI 2.5-008-02 Requirements for protecting confidential information from unauthorized access during processing in class "2" automated systems. http://dstszi.kmu.gov.ua/dstszi/doccatalog/document?id=106343

63. ND TPI 2.5-010-03 Requirements for protecting WEB page information from unauthorized access. http://dstszi.kmu.gov.ua/dstszi/doccatalog/document?id=106344

64. ND TPI 2.7-011-12 Information protection at objects of information security activities. Guidelines for developing a methodology for identifying embedded devices. http://www.dsszzi.gov.ua/dsszzi/doccatalog/document%3Fid=103253

65. ND TPI 3.7-001-99. Guidelines for the development of technical tasks for creating a comprehensive information security system in the AS. http://www.dsszzi.gov.ua/control/uk/publish/article?art_id-46075

66. ND TPI 3.7-003-05. Procedure for creating comprehensive information security system in the information and telecommunications system http://www.dsszzi.gov.ua/control/uk/publish/article?art_id=46074

67. ND TPI R-001-2000 Means of active protection of speech information with acoustic and vibroacoustic radiation sources. Classification and General technical requirements. Recommendations. http://dstszi.kmu.gov.ua/dstszi/control/uk/publish/articleshowHidden=l&art_id=101924&cat_id=89734&ctime=1344501363205

68. Temporary recommendations for technical protection of information from leakage by channels of side effects of electromagnetic radiation and interference. (TR TPI PEMWN-95) http://www.dsszzi.gov.ua/dsszzi/control/uk/publish/article?showHidden=1&art_id=101798&cat_id-89734&ctime=1344500065981

69. Temporary recommendations for technical protection of information in the computer technology, automated systems and networks from leakage channels of side effects of electromagnetic radiation and interference (TP EOT-95). http://www.dsszzi.gov.ua/dsszzi/control/uk/publish/article?showHidden=1&art id=120206&cat id=89769&ctime=1421836194327

70. DSTU ISO / IEC 27001: 2015 Protection methods. Management systems ofinformation security. Requirements (ISO/IEC 27001: 2013, IDT).

71. DSTU ISO/IEC 27002: 2015 Information technologies. Method of protection.Code of practice on information security measures (ISO/IEC 27003: 2013, IDT).

72. DSTU ISO / IEC 27005: 2019 Information technologies. Method of protection. Information security risk management (ISO/IEC 27005: 2018, IDT).

73. Decree of the President of Ukraine " On Regulations on technical protection of information in Ukraine " from 27.09.1999 № 1229.

74. Buryachok V. L., Tolyupa S. V., Semko V. V., Buryachok L. V., Skladny P. M., lukova-Chuiko N. V. Information and cyberspace: Security issues, methods and means of struggle. Manual. - K.: DUT. - KNU, 2016. - 178 p.

75. Buryachok V. L., Gulak G. M., Tolubko V. B. Information and cyberspace: security issues, methods and means of struggle. Textbook. - Co.: SIC group Ukraine LLC, 2015. - 449 P.

76. Kobozeva A. A., Machalin I. A., Khoroshko V. A. Security analysis of information systems: textbook. K. GUIKT, 2010. - 316 p.

77. Grebennikov V. Comprehensive information security systems. Design, implementation, maintenance / V. Grebennikov "Publishing solutions", 2018. - 249 p.

78. Technical channels of information leakage. Procedure for creating complexes technical protection of information. Textbook / S. A. Ivanchenko, Gavrilenko A.V., Lipsky A. A., Shevtsov A. S.-K.: IC33I NTUU KPI, 2016. 104 p.

79. Khoroshko V. A., Azarov A.D., Maksimenko G. A., Yaremchuk Yu. E. Search and localization of embedded radio devices. Textbook. - Vinnytsia: VNTU, 2007. - 333 p.

80. Technical protection of information in information and telecommunication systems: textbook . / G. I. Lastovka, P. M. Shpatar / / - Chernivtsi, CHNU, 2018. 252 PP.

ADDITIONS

Kyiv – 2020

CONTENT

Addition 1. A variant of the plan of conducting a comprehensive special inspection of the premises…….59

Addition 2. Methods of searching for embedded devices using the search software and hardware complex SHC DigiScan……....64

Addition 3. Methods of searching for embedded devices using the search device ST 031 «Piranha»……..75

Addition 4. Methods of searching for embedded devices using the nonlinear locator NR-900EM……101

Addition 5. Method of searching for embedded devices using the PROTECT 1203 field indicator……109

Addition 6. A variant of the act of complex special inspection of premises……113

Addition 7. A variant of recommendations for improving the security of inspected premises and facilities……117

Addition 8. The list of normative-legal documents on the basis of which activity on rendering of services on TPI is embodied……...122

Addition 1

A variant of the plan of conducting a comprehensive special inspection of the premises

Ex.№_

Total_ex.

Agreed	**Approve**
Head of the enterprise security service	Head of the enterprise
_____/_____/	_____/_____/
"____"_____20__ye.	"____"_____20__ye.

PLAN

conducting a comprehensive special inspection of the premises

1. Conclusions of the enemy's assessment.

The visitor (client) who had access to the office of the head of the enterprise and to the adjacent premises is considered as the subject chosen by the probable opponent for installation of embedded devices (ED) and other means of covert receipt of information (CRI). To establish the means of the CRI, it is possible for the enemy to use one of the employees who carried out cosmetic repairs of the manager's office in the period from _ to _ (date, time). The visitor (client) or outsiders outside the controlled area were considered as the subject of information retrieval.

The entity that installed the CRI is a specialist in the secret removal of information, has information about the location of the premises it needs, the placement of equipment and interior items.

Given the possibility of installing CRI during the repair of the head's office, we can expect the use of the enemy, both radio-emitting ED and transmitting information over wired communications. In adjacent premises, it is possible for the enemy to install means of taking information from telephone lines and electronic stethoscopes. The expected technical and technological level of ED and other CRI tools used corresponds to the average part of the price range of these tools.

The most probable installation of CRI means during the repair of the manager's office by tossing, connecting to the telephone line, replacement of electrical and telephone switching products. It is possible to toss the radio microphone while visiting the office by the visitor (client). Probable time of installation of CRI means - in the period from _ to _ (date, time). Expected methods of recording information are

connection to wired lines in adjacent premises and interception of radio transmissions by means of a radio control point located outside the controlled territory.

If the enemy discovers intentions to conduct a special inspection of the premises, temporary withdrawal of ED is possible. Establishing the fact of such a check may temporarily disable the remotely controlled ED. When establishing the fact of detection of the installed ED the most probable attempt to install a new similar device.

2. The purpose of conducting a comprehensive special inspection of the premises.

The purpose of the inspection is to prevent damage from the leakage of acoustic and video information from the premises due to potentially installed ED.

The following are subject to inspection:

1. Office of the head of the enterprise.

Room area –_ sq. m., volume - _cub. m. Enclosing structures - reinforced concrete panels (thickness of the outer wall panels –_cm), adjacent to the accounting wall - brick, thickness –_cm. The ceiling is suspended, the walls are plastered and covered with wooden panels. Two passive ventilation ducts.

Office equipment: TV, PC, telephone. Standard office furniture: desks and coffee tables, two armchairs, built-in wardrobe, two shelves, three armchairs, safe, refrigerator occupy _ percent of the total area of the room.

Wired communications of power and lighting power grid, telephone line, fire and burglar alarm lines. Steam heating main.

2. Premises of accounting.

(the characteristics of the second room are given)

List of planned works:

1. In the office of the head of the enterprise:

1. Visual inspection of fencing structures, furniture and other interior items (expected labor intensity –_human hours).
2. Checking the elements of building structures, furniture and other interior items using special search equipment (_human hours).
3. Checking the lines and equipment of the power and lighting network (_human hours).
4. Checking the lines and equipment of the subscriber telephone network (_human hours).

5. Check of lines and the equipment of the fire and security alarm system (_human hours).

6. Checking the radio for the presence of signals of radio emitting means of implicit recording of information (radio monitoring of the premises) (_human hours).

7. Check for unauthorized transfers of information in the infrared range (_human hours).

8. Search for embedded devices that use low-frequency magnetic radiation (_human hours).

9. Search for passive embedded devices (_human hours).

10. Examination of the premises for the presence of devices and other means of CRI (_human hours).

11. Physical search of embedded devices and other CRI tools (_human hours).

2. On the outer surface of the wall facing the street, the head's office:

Visual inspection of fencing structures (_human hours).

3. In the secretary's office (adjacent to the head's office):

(the list of the planned works is resulted)

4. In the accounting office:

(The following is a list of premises, including those adjacent to the one being inspected, and a list of works planned for them).

Time of special inspection:

From (date, time) to (date, time). The total duration of the direct inspection is _ hours.

Option to cover the preliminary inspection of the premises:

Inspection of premises for drawing up an estimate for the installation of a forced ventilation system (from (date, time) to (date, time)). It is reported to the secretary and the person responsible for the operation of the building three days before the inspection (date).

The document confirming the legend is a copy of the contract for installation work.

Option to cover search works:

1. Check by specialists of the telephone exchange, the state of telephone lines and equipment (from (date, time) to (date, time)). It must be recorded by the secretary two days before the inspection (date).

Documents confirming the legend - an order for work and permission to work on the equipment.

2. Search for sparking contacts, hidden wiring to eliminate PC interference (from (date, time) to (date, time)). It is reported to the secretary and the person in charge of electricity before the inspection (date).

The document confirming the cover - a copy of the contract for the search work.

Measures to activate the installed embedded devices:

Bringing to the secretary and persons of the management of the enterprise information on holding on the day of the inspection a meeting of the management of the enterprise on accelerating the development of new product samples and promoting them on the market of goods and services. Method of proof - distribution of the agenda of the meeting and the order on preparation of reports among the persons of the leading staff. Date: __ (one week before the inspection).

Actions in case of detection of means of implicit removal of information:

Without touching the detected tool, report the fact of detection to the head and head of the security service of the enterprise to decide on further action.

3. Means and forces involved, their distribution by objects and types of work.

The composition of the search team:

1. _____ - manager;
2. _____.
3. _____.

The list of special equipment and technical means involved in the inspection:

1. Complex of inspection mirrors (used only when the doors and rooms are closed and there are no outsiders in it).
2. Search software and hardware complex SHC DigiScan (used only when the door is closed and there are no outsiders).
3. Non-linear radar device NR 900E (in the process of radio monitoring do not turn on, use only when the door is closed and there are no outsiders).

(The list of equipment and technical means with the indication of the main features of their application within the limits of the chosen variants of cover and other restrictions established by conditions of check proceeds further).

Additional measures to activate the installed ED:

In the office of the head of the enterprise for activation of ED with acoustic start by means of a radio tape recorder of the reports made at the scientific conference are reproduced. Pre-recorded records of non-confidential business matters are reproduced in the accounting office. Start of reproduction of records - with the beginning of a visual inspection of enclosing structures, furniture and other interior items.

When checking the presence of signals in the wired lines, all the equipment connected to them is put into operation (switched on in the operating mode), the handsets of the telephones are removed to switch the telephone lines to the "busy" mode.

4. The list of reporting documents based on the results of the inspection and the deadline for their submission for approval.

1. Comprehensive special inspection of premises.
2. Description of work and research.
3. Recommendations for improving the reliability of information protection against its possible leakage through technical channels.
4. Journal of registration of factory and inventory numbers of equipment, furniture and items.
5. Logbook of seals and hidden labels.

The act of inspection of the premises - in two copies (one - to the contractors). Other documents in one copy.

All documents are marked «confidential».

Deadline for approval – _.

Agreed
Head of the organization conducting the inspection
_____/_____/

"_____"_____20__ye.

Head of the search team

_____/_____/

Members of the search team

_____/_____/
_____/_____/
"_____"_____20__ye.

Addition 2

Methods of searching for embedded devices using the search software and hardware complex SHC DigiScan

1. Purpose and components of the complex.

Automated search software and hardware complex SHC DigiScan, consisting of a laptop with special software DigiScan-2000 and scanning receiver AR-3000A, designed to detect radio signals from embedded devices, determine their frequency, bandwidth, study of signals by correlation functions, amplitude and spectral characteristics, detection of signal harmonics, classification of the detected signal (friendly or dangerous) and entering the result in the database.

The DigiScan complex detects the following types of radio emitting embedded devices both with an open channel and with spectrum inversion masking:

- room radio transmitters with autonomous power supply;
- room radio transmitters powered by a network, telephone line or other source;
- portable radio transmitters;
- telephone transmitters.

DigiScan allows you to search both in secret mode and in active mode. In secret mode, no beeps are issued, which unmasks the work. The program controls the sound of the room, which is required for the activation of embedded devices with "voice-on" and for the successful measurement of correlation. A CD or MIDI player is used as a subsonic.

In the active mode the maximum speed and reliability of detection is provided. The DigiScan-2000 software controls the sound card to output sound pulses or tones.

When measuring correlation, the program compares the signal from the audio output of the receiver and the reference signal. If these signals are similar, the correlation is 1 and the signal is considered dangerous. As a source of reference signal, an active microphone is used, which is equipped with a cable, 10 m long, which also allows you to check the adjacent rooms without moving the computer.

DigiScan summarizes the results of all tests in a single level of danger (DANGER), which is the conclusion about the type of signal. The DANGER value can be from 1 to 5. The DANGER level is set by the operator.

The composition of the software and search complex DigiScan:

1) Portable computer;

2) Specialized software DigiScan-2000;

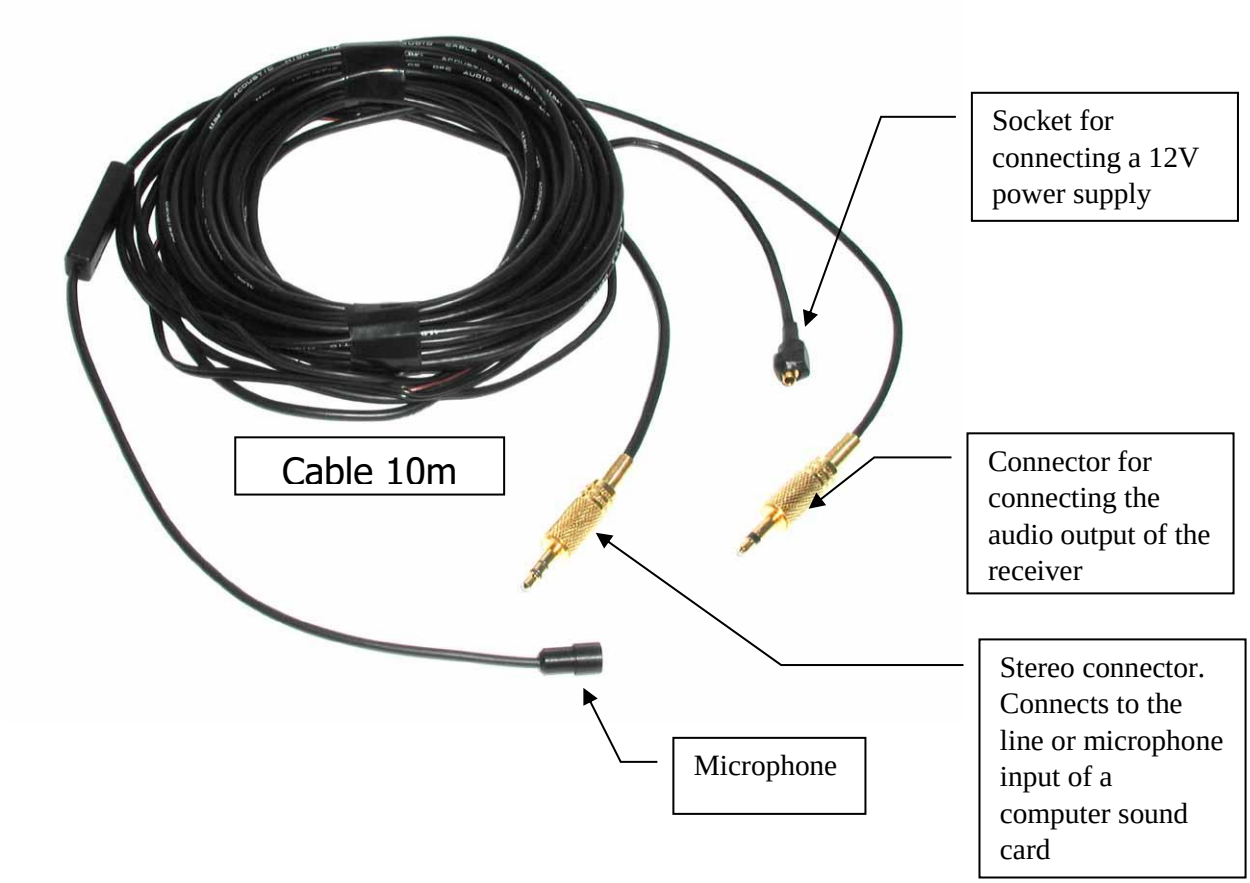
3) Active speakers to your computer;

4) Scanning radio AR 3000A;

5) External antenna of the DA 3000 receiver;

6) Cable with remote microphone and 12 V power supply (Pic. 1);

7) RS 232 connection cable from the AR 3000A receiver to the computer's COM port.



Pic. 1. Cable with remote microphone.

2. Preparation of the room to be inspected.

In preparation for the search, it is necessary to carry out in accordance with the plan (Addition 1) measures to prepare the premises to be inspected and to activate the installed ED, such that are included remotely or on the principle of acoustic start. Such measures may include:

- organizing a "false" meeting or negotiation;
- reproduction on a tape recorder of the reports recorded at open meeting;
- switching on all computers, office equipment, lighting to create a working environment;
- removal of telephone handsets from devices, disconnection of radiotelephones and other authorized radio transmitters;
- disabling the means of technical protection of information.

3. Preparation of the complex for work.

Preparation of a complex for work consists in connection of all cables, connection of all devices and installation of initial settings. The sequence of works is as follows:

1) install a laptop and AR-3000A receiver at the workplace;
2) connect speakers to the output "SPK" of the computer sound card;
3) connect the microphone cable connector to the "LINE" socket of the computer;
4) connect a 12 V power supply to the microphone power socket;
5) connect the microphone cable connector to the "EXT.SP" audio output of the AR-3000A receiver;
6) connect the connecting cable to the "REMOTE" connector of the AR-3000A receiver and to the COM port of the computer;
7) connect the external antenna DA 3000 to the connector "ANT" of the receiver AR - 3000A;
8) connect the 12 V power supply to the "DC 12 V" connector of the AR-3000A receiver;
9) connect the HASP key to the LPT1 port of the computer;
10) connect to the network 220V, 50 Hz power supply of the receiver AR - 3000A, the power supply of the microphone and the plug of the power cord of the computer;
11) set the AR-3000A switch of the built-in remote control to the "ON" position (on the rear panel of the device);
12) set on the receiver AR - 3000A volume control "VOLUME" in the position "10 o'clock", sensitivity regulator "SQUELSH" in the position "12 o'clock";
13) turn on the power of the computer "POWER";
14) turn on the power of the receiver AR - 3000A ("POWER" - ON), on the LCD (liquid crystal display) of the receiver will appear the symbol "RMT".

4. Launch the DigiScan-2000 program, set the threshold and scan settings.

After making all the connections and connections (step 3), starting the computer's operating system, you need to start the DigiScan-2000 software (hereinafter referred to as the program). Execute the command "DigiScan-2000" in the "Programs" menu of the "Start" button.

After launching the program, the "Receiver search" window opens, the connected receiver is automatically tested and the connection parameters are set: exchange speed, port, etc. (see table.1). After that, the main program window opens, consisting of:

1) command menu: File, Mode, Tests, Signals;
2) toolbars;

3) main panorama (in the upper left corner of the screen);
4) auxiliary panorama;
5) signal database windows;
6) oscillogram and spectrogram windows;
7) protocol windows;
8) volume control.

After that it is necessary to set the sensitivity threshold and scan parameters.

Setting the threshold.

The threshold setting window is opened using the «Threshold» command from the «Mode» menu.

The threshold is the level above which the current frequency is entered into the database and the program enters the mode of analysis of this signal. The threshold level is selected by the operator, taking into account the local radio situation, depending on the background noise level in the areas of the tested range. The higher the threshold, the higher the search speed and the higher the probability of signal transmission. The lower the threshold, the higher the search reliability, but the lower the speed.

For each section of the frequency range it is necessary to set:

- the initial frequency of the range «Beginning F1»;
- the final frequency of the range «End of F2»;
- threshold level (from 0 to 15);
- attenuator value (0, - 10 or - 20 dB).

All information about the range sections and the exposed threshold and attenuator levels is stored in the ar3000.thr file.

Setting parameters.

All parameters and algorithm of program operation are set in the parameters window. The settings window opens with the «Settings» command from the «Mode» menu and has 5 pages: «Receiver», «Search», «Analysis», «Sound», «Notifications». The set parameters and recommended values are summarized in table 1.

DigiScan operation parameters are set

Table 1

Customizable settings	***Recommended values***
«Receiver» page	
Receiver	AR-3000A
Address CI-V	52
Port	COM2
Exchange speed	9600
Survey interval	25 ms

Customizable settings	*Recommended values*
Number of requests	2
The receiver is connected to the sound card	Linear
«Search» page	
Range: Begin, MHz Final, MHz	20 2000
The standard step is equal to the WFM band, kHz	180
Threshold of danger (1… 5)	2
Detect: Suspicious signals	
«Analysis» page	
Additionally in the modulation of AM	select
Check harmonics	2 and 3
Correlation: None, Passive, Passive with sounding, Active	select Active
Amplitude or Spectral	select both
Correlation time, s	5
«Sound» page	
Automatic gain control	select
Sound: No (listen to the receiver), Use CD player, Use MIDI player	No
Record a sound sample	install
Recording time, s	3
«Notifications» page	
Report about bug: None, When detected, When detected with user confirmation	select «When detected»
Sound signal	select waf-file

5. Scan the radio frequency range for dangerous signals.

The complex works under the control of the universal search software DigiScan - 2000, which implements the following advanced detection methods:

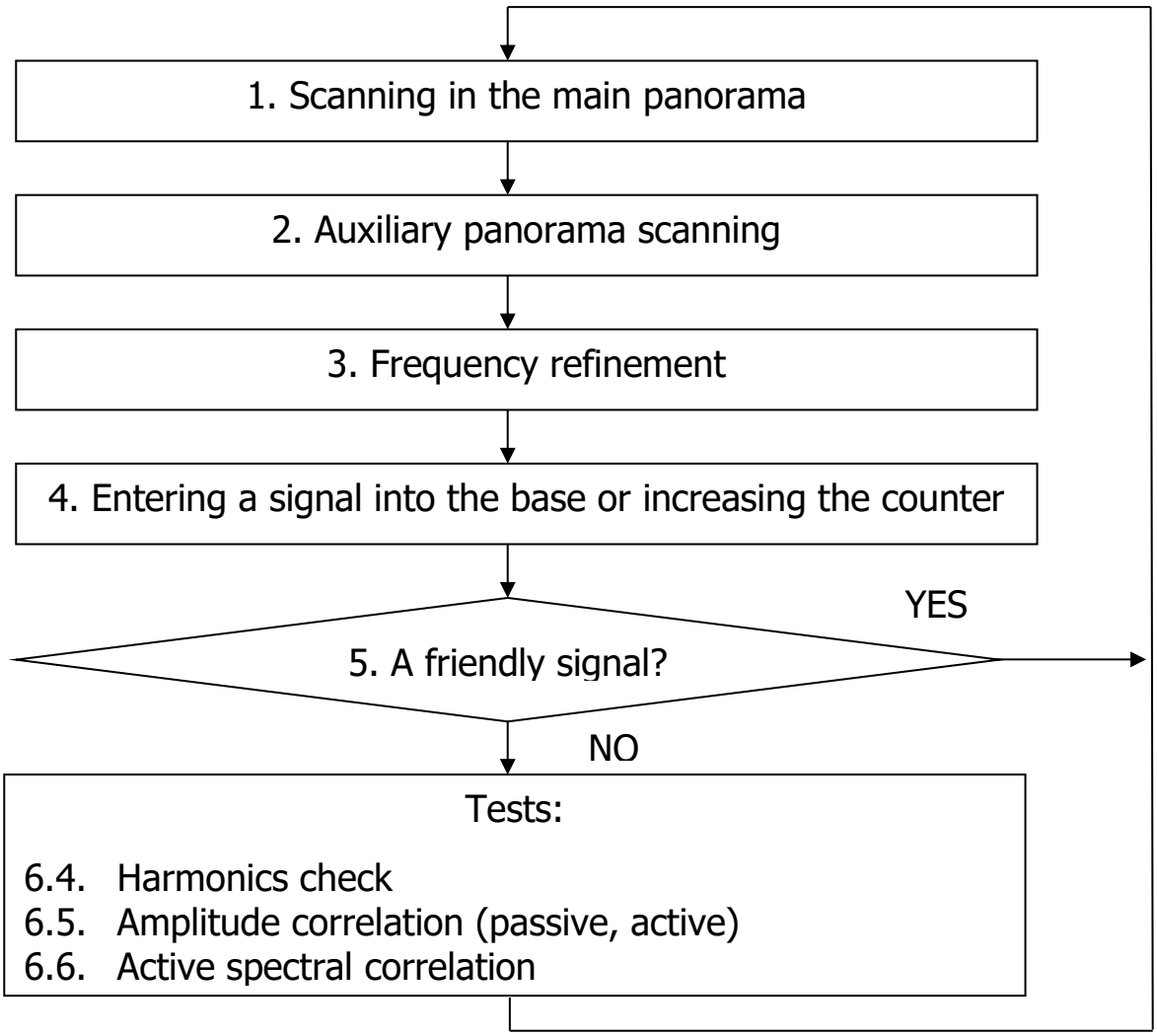
- dynamic threshold;
- signal band measurement;
- checking the presence of signal harmonics;
- passive correlation;
- passive correlation with sounding;
- active amplitude correlation;
- active spectral correlation;
- selection of signals on the total level of danger.

DigiScan - 2000 works in two modes - Search and Manual mode.

After setting the parameters, *the operator turns on the automatic scanning mode in the specified range* (command «Search» in the menu «Mode»).

In *search mode*, the program automatically scans the specified range, finds signals that exceed the specified threshold, and performs tests set by the operator. If a dangerous signal is detected, the program beeps or displays a message on the screen and includes a recording of the sound sample. The signal is entered in the «Dangerous»

section of the database. All other signals are entered in the «New» section of the database. The «All» section includes all signals, regardless of the danger. After several scans of the entire range, the operator stops the search and switches to manual mode.



Pic. 2. Block diagram of the search algorithm

In *manual mode*, the operator can analyze the search results or try to find new signals. To do this, the operator steps on the range and performs tests on the detected signals. In manual mode, the threshold set by the operator is also used. In manual mode, the operator can view the waveform and the range of signals on the displays «Amplitude» and «Spectrum».

Algorithm for searching dangerous signals.

The algorithm for finding dangerous signals is shown in the block diagram presented in Pic. 2. The current operation is displayed in the status bar at the bottom of the program.

Scanning in the main panorama.

In search mode, DigiScan - 2000 starts scanning in the main panorama. Receiver modulation - WFM, the scanning step is equal to the band of this modulation. For AR3000A, this value is 180 kHz. The blue vertical line on the main panorama is a marker that shows the current frequency. On the main panorama, a red line shows the threshold. When the threshold is exceeded, the program remembers the frequency at which the excess began (F1) and continues scanning to the frequency at which the excess ends (F2). The program remembers these frequencies and proceeds to a detailed scan in the auxiliary panorama.

The main panorama allows you to display from 0.1% to 100% of the range being checked. The zoom in the lower left part of the main panorama is used for scaling. Before starting the search, when the threshold is set, it is recommended to set the scale to 50-100% to view the entire range.

The threshold is edited before the start of the search using the «Threshold» command of the «Mode» menu item.

Scanning in the auxiliary panorama.

Receiver modulation - NFM, the scanning step is equal to the band of this modulation. For AR3000A, this value is 12 kHz. The current frequency marker is displayed with a blue vertical line. The scanning range in the auxiliary panorama (f1, f2) is automatically calculated from the values of frequencies F1 and F2:

- the beginning of the range f1 = F1 - 90 kHz;
- the end of the band f2 = F2 + 90 kHz.

After the program finishes scanning in the range from f1 to f2, it proceeds to search for threshold exceedances. The program enters the detected signals in the list, selects the first signal from this list and enters the mode of refining the frequency of this signal.

Auxiliary panorama allows you to display from 0.1% to 100 of the range being checked. The zoom in the lower left part of the main panorama is used for scaling.

Frequency refinement.

In this mode, DigiScan - 2000 specifies the frequency of the signal from the list obtained during the detailed scan. Scanning in the auxiliary panorama was performed with a step equal to the NFM band - 12 kHz. The bug may have a frequency offset relative to the 12kHz grid and the program may be inaccurately tuned and skip it. To avoid this, the program checks the signal level at a frequency less than half the NFM step and more than half the NFM step. If at any of these adjacent frequencies the level is higher than at the center frequency, then this adjacent frequency will be considered the signal frequency. Thus, the accuracy of frequency measurement is increased to 6 kHz.

Entering a signal into the base or increasing the counter.

Detected signals are automatically entered by the program into the database, regardless of the level of danger. If the signal is already in the database, its counter is incremented by 1.

Skip friendly signals.

If the signal is already in the database and marked as friendly, the search process skips this signal and continues to check other signals or scan. Friendly signals are marked «FR» near the danger level. When working in manual mode, the mark «FR» must be set manually.

Note. Marking signals as "friendly" excludes them from testing during the search. You need to make sure that all signals are safe, otherwise you can skip the bug.

Harmonics check.

In this mode, DigiScan - 2000 checks for the 2nd and 3rd harmonics of the signal. Due to limitations in the volume and power of the bug, as well as the proximity to its antenna, the signal may have harmonics multiples of the fundamental frequency. The presence of harmonics increases the level of signal danger.

Knowing the fundamental frequency of the signal, the program calculates the frequencies of harmonics, multiplying the fundamental frequency by 2 (2nd harmonic) and 3 (3rd harmonic). After that, WFM modulation is installed on the receiver, it is tuned to the harmonic frequencies, and the level is read at these frequencies. If the signal level at these frequencies exceeds the threshold, the frequency is considered to have harmonics.

If the frequency has both harmonics, the total danger level of the signal increases by 1. If there is no harmonic or there is one of the two, the danger level does not increase.

If you tune to the harmonic frequency in manual mode, you can hear the same sound as the fundamental frequency, only with some distortion.

For completeness of the analysis it is recommended to establish always check of harmonics. If the band being tested starts at a frequency above 1000 MHz, the 3rd harmonic check does not make sense, as the 3rd harmonic frequency will be higher than the upper range of the receiver. When accumulating the base of these friendly signals, it is recommended to disable the harmonic check.

Amplitude correlation.

In this mode, the program measures the relationship between the acoustics of the room being tested and the signal at the audio output of the receiver, which is called correlation (K). At amplitude correlation there is a comparison of amplitude of a signal in time. An active reference microphone included in the complex is used to analyze the acoustics of the room. The correlation (correlation coefficient) can be in the range

from - 1 to +1. If there is a connection between the room acoustics and the signal at the output of the receiver, the correlation will be close to +1. This correlation indicates that the receiver is configured on the embedded device.

In the search mode, the amplitude correlation is done with several types of modulation - WFM, NFM and AM (set before turning on the search mode).

The results of the correlation measurement are displayed in the lower right part of the main window DigiScan - 2000 on the page «Protocol». The amplitude correlation is denoted by K1. The database gets the maximum correlation value when modulating WFM, NFM and AM and is stored in the field K1.

According to the value of K1, the level of danger of the tested signal is calculated:

- when K1 = 0-0.33, the level of danger does not change;
- when K1 = 0.33-0.66, the level of danger increases by 1;
- when K1 = 0.66-1.0, the level of danger increases by 2.

Depending on the conditions in which the test is performed, *you can use one of the types of amplitude correlation*:

- passive;
- passive with sounding;
- active;

Passive correlation.

Passive correlation is done silently and does not unmask the search measure. There must be some sound in the room for successful passive correlation. This can be music from a computer's CD or MIDI player, recording an English course on a tape, or a radio. If a radio is used, the frequency to which it is tuned can be entered by the program in the «Dangerous» section. Passive correlation gives less accurate results than active. For example, if in active mode the correlation of a bug is equal to 0.76, in passive it can be 0.45, and sometimes less. If the number of passes in the range is more than one, the probability of passing a dangerous signal decreases. To increase the accuracy of passive correlation measurement, it is necessary to set a correlation time greater than when conducting active. For passive correlation, it is recommended to set the time to at least 10 seconds.

You can use a computer CD or MIDI player to sound the room. These settings are set on the «Sound» page of the «Settings» command in the «Mode» menu.

Passive correlation with sounding.

The same test as for passive correlation, except that the program periodically changes the volume of the CD or MIDI player during the correlation measurement. First, the volume becomes maximum, then minimum, and so on. This allows you to significantly increase the accuracy of the correlation and not unmask the search

process. The subject listening to the bug may think that the volume is just being adjusted. This type of correlation requires the use of sound with a CD or MIDI player on the computer. The time of passive correlation with sounding can be 5-10 seconds.

Active amplitude correlation.

During active amplitude correlation, the DigiScan-2000 also compares the amplitude of the room acoustics and the signal from the receiver's audio output. The difference is that during active correlation, computer speakers reproduce sound pulses, which significantly increase the accuracy and reliability of the search. Sound pulses are reproduced with a random period from 0.2 to 1 s. When using active correlation, the time may be shorter (3-5 s), although you can set more to increase reliability.

Spectral correlation.

In this mode, the program compares the spectrum of room acoustics and the signal from the audio output of the receiver. For successful spectral correlation, it is necessary that a tone with a changing frequency sound in the room. This is achieved by playing the default.wav sound file with such a signal. The correlation time depends on the length of this file.

Spectral correlation is also done with several types of modulation - WFM, NFM and AM. The results of the spectral correlation are displayed in the «Analysis» tab of the main window in column K2. The same name has a database field, which stores the maximum correlation result (with different modulation).

When the spectral correlation is close to k-1, it means that there is an inverse relationship between the sound spectrum in the room and the spectrum of the received signal. This is possible when using radio transmitters with spectrum inversion.

According to the value of K2, the level of danger of the tested signal is calculated:

- when K2 = 0-0.33, the level of danger does not change;
- when K2 0,33-0.66, the level of danger increases by 1;
- when K2 0.66-1,0, the level of danger increases by 2;

The total signal danger level is calculated by the presence of harmonics and by the amplitude and spectral correlation coefficients. If the danger level of the threshold value is exceeded (recommended value 2), the signal is classified as dangerous and is entered into the database of dangerous signals.

Analysis of search results.

After several passes and scanning of the set frequency range it is possible to print out all base or base of dangerous signals in which the following parameters of signals are written down:

- frequency, modulation, band;
- presence of harmonics;

- values of K1 and K2;
- general level of danger;
- time, date of entering the signal into the database;
- counter value (how many times the signal was encountered during the search);
- comment.

The database has the following sections: «New», «Dangerous», «Friendly», «All».

After that, all dangerous signals are analyzed in detail in manual mode:

- a dangerous signal is heard;
- the signal is written to the waf-file;
- the oscillogram is analyzed;
- the spectrogram is analyzed;
- the 2nd and 3rd harmonics are listened to;
- the amplitude correlation coefficient is calculated;
- the spectral correlation coefficient is calculated.

On the basis of the detailed analysis of dangerous signals the conclusion on existence in the checked room of the radiating embedded device and its characteristics is made.

All work results are automatically recorded in the log file, which is a reporting document. The printed protocol is attached to the inspection report (Addition 6). In addition, the reporting documents include a database of dangerous signals, oscillograms, spectrograms of signals of detected embedded devices.

Localization and search for the location of the detected radio transmission EDs is performed using additional search tools:

- ST 031 «Piranha»;
- PROTECT 2103;
- RFM-32.

Addition 3

Methods of searching for embedded devices using the search device ST 031 «Piranha»

1. Appointment.

Multifunctional search device ST 031 «Piranha» is designed to detect and localize special technical means of implicit information retrieval (embedded devices), to detect natural and artificial channels of information leakage, as well as to control the quality of information protection. It provides the solution of control and search tasks within the premises (object) or in the immediate vicinity of it.

The device can operate in the following modes:

1) high-frequency detector-frequency meter (RADIO - FREQUENCY CHANNEL) - to search for radio emitting ED;

2) scanning wire line analyzers (WIRE LINES ANALYSIS) - to search for ED using wire lines;

3) infrared detectors (INFRARED CHANNEL) - to search for ED using infrared radiation;

4) low-frequency magnetic field detectors (MAGNETIC CHANNEL) - to search for ED using low-frequency radiation;

5) vibroacoustic receiver (VIBRO - ACOUSTIC CHANNEL) - to study the premises for the presence of vibroacoustic information leakage channel;

6) acoustic receiver (ACOUSTIC CHANNEL) - to study the premises for the presence of an acoustic channel for information leakage.

Switching the ST 031 «Piranha» to any of the modes is carried out automatically when connecting additional external devices (antennas, adapter, sensors, microphone) to the high-frequency connector «RF ANT» or «PROBES». At the same time the device can work only in one of the listed basic modes.

2. The composition of the set of search device ST 031 «Piranha».

The device includes the following components (Pic. 1):

1. The main control, processing and indication unit.

2. Wire line analyzer adapter with signal attenuation device and LED indicators for voltage in the line being tested.

3. Nozzles to the adapter (type «Needle»).

4. Nozzles to the adapter (type «220 V»).

5. Nozzles to the adapter (type «Crocodile»).

6. Headphones.

7. Magnetic antenna of the low-frequency magnetic field detector with a device to provide a differential mode of operation.

8. High frequency antenna of the detector-frequency meter.

9. Connecting cable for connecting a magnetic antenna and an infrared sensor.

10. Remote microphone of the acoustic receiver.

11. Infrared sensor of the infrared radiation detector.

12. Remote sensor of the vibroacoustic receiver.

13. Telescopic antenna of the detector-frequency meter.

14. Adapter to telescopic antenna.

15. Shoulder strap of the main unit.

16. Stand for the main unit.

17. Power Supply.

Pic. 1. Appearance of accessories of the ST 031 «Piranha» device

3. Construction and controls of ST 031.

The main control unit, processing and indication of the device ST 031 «Piranha» is structurally made in the form of a small portable monoblock. On the front panel there is a liquid crystal display screen, controls and a 16-button keyboard that provides control of the device in all modes. All control keyboard buttons are multifunctional.

The order of their use and the functions which are realized thus are defined by features of work of the device in each of the provided modes.

At the same time, most of the control buttons provide the implementation of primary functions common to all modes of operation. In particular:

- the «MUTE» button turns on (off) the built-in speaker;
- the «HELP» button allows you to get contextual on-screen help when working in any mode with the ability to move the text by pressing the «Δ» and «∇» buttons;

- the «OSC» button enables oscillographic control of signal parameters in the current mode;
- the «SA» button turns on the spectral control of the signal parameters in the current mode;
- the «SAVE» button provides recording in the non-volatile memory of the displayed oscillogram or spectrogram with the accompanying parameters of the analyzed signal;
- the «LOAD» button makes a call to the screen from the non-volatile memory of the previously saved oscillogram or spectrogram;
- the «RUN/STOP» button starts (stops) the current dynamic measurements of the parameters of the controlled signal;
- the «SET» button allows to carry out a choice of various options of carrying out the analysis of the controlled signal;
- the «ENTER» button provides output for auditory control of a tonal signal, or that is demodulated;
- the «RESET» button restarts the device.

The second, and in some cases further, functions of control buttons are in direct dependence on features of application of the device in various modes.

At the bottom of the front panel there is a power switch «OFF POWER ON», a line output jack «LINE» and a headphone jack «PHONE».

There are three connectors on the upper surface of the unit. The «RF ANT» connector is used to connect a telescopic (through an adapter) or high-frequency antenna of the detector-frequency meter. All other additional external devices included in the device are connected via the «PROBES» connector. The «OSC2» connector is designed to ensure the operation of the built-in oscilloscope and spectrum analyzer in two-channel mode, as well as to realize the possibility of the device as a conventional low-frequency single-channel oscilloscope and spectrum analyzer.

On the back of the device there is a built-in speaker and battery compartment for 4 batteries or AA accumulators. On the lower surface of the main unit there is a connector of the power supply unit and a threaded hole for connecting the stand for the main unit. On the side walls, in the upper part there are threaded holes for connecting the shoulder strap.

4. Preparation of the ST 031 device for work.

Preparation of the ST 031 «Piranha» device for work, especially after a long break, it is expedient to begin with external inspection - to be convinced of integrity of a bag - packing, to check up completeness of a product and absence of visible mechanical damages.

Prepare power supplies. To do this, check the external condition of the batteries or accumulators for the absence of oxidation on the contact surface of the poles. Measure the voltage of each battery with a voltmeter (should be 1.45… 1.55 V). Make sure of the mechanical integrity of fixed and spring contacts, as well as the absence of traces of oxidation on them. Insert batteries or accumulators with the correct polarity. The device is ready for inclusion and check of serviceability.

After a long break in operation of the device it is necessary to carry out the following checks of serviceability of tracts:

- systems of inclusion of the device and indication of a condition of a power supply;
- liquid crystal display and backlight of its screen;
- systems of automatic transfer of the device to the main modes;
- private tracts that correspond to the main modes of the device;
- sound tract;
- built-in low-frequency oscilloscope;
- built-in low-frequency spectrum analyzer;
- non-volatile memory.

The test procedure and technology are described in the ST 031 Operating Instructions.

5. Search for radio emitting ED using the device ST 031 in the mode of high-frequency detector-frequency meter (RADIO-FREQUENCY CHANNEL).

5.1. The order of control of the device in the mode of the high-frequency detector-frequency meter.

Connect a telescopic antenna using an adapter or a high-frequency antenna to the «RF ANT» connector. Turn on the power of the device.

The «zero» threshold of the device is set when it is switched on automatically. If necessary, set the detector threshold manually by pressing the «<» or «>» buttons, following the readings of the additional scale «min - - - | - - - max». If necessary, press the «Δ» button to return to the automatic threshold setting. Lowering the threshold will inevitably lead to frequent false alarms, and its overestimation - to the probable omission of the signal «radio bug». Both significantly complicate the work of the operator, increase the time and reduce the reliability of the test results. Therefore, to set the «zero» threshold, it is necessary to follow a few simple rules:

- it is impossible to carry out installation of a threshold in the checked room as at functioning of the «radio bug» already placed in it, the level of its radio emission will be defined by the device as «zero»;
- the use of radio stations, radiotelephones and other radio emitting means is not allowed during the threshold setting;

- do not bring the antenna of the device closer to the included PC and other means of office equipment, as sources of SEMI in the range of the device;
- prevent contact of the antenna of the device with metal objects and wires as sources of overexposed high-frequency signals;
- the device should be set up in one of the nearest rooms, where the background level is probably not significantly different, and the installation of «radio bugs» is either impossible or impractical. Such premises are usually considered premises of other purpose, but located on the same floor and with window openings facing the same side of the building;
- if the object of inspection is a car or other vehicle, then, ensuring the correct choice of the place of work, the setting of the «zero» threshold should be carried out not closer than 10 - 20 m from it.

After setting the «zero» threshold, the device is moved to a controlled room (to the controlled object) WITHOUT SWITCHING OFF THE POWER SUPPLY. Because each subsequent inclusion leads to the automatic setting of the threshold in relation to the new conditions of the electromagnetic environment.

Visually evaluate the received signal level by the number of fully colored elements of the signal level indicators and «by ear» by the frequency of clicks in the built-in speaker or headphones.

If necessary, press the «SET» button to set the required limits of the dynamic range: (-8… -16) dB; (- 8 ...- 32) dB; (- 8… -48) dB.

Use the «RUN/STOP» button to start and stop dynamic measurements of the radio signal level and frequency.

Press the «ENTER» button (switch the audio indication to «AUD» mode) to listen to the presence and content of potentially dangerous modulated radio emissions.

Press the «+» and «-» buttons to set the desired volume of the audio signal (tone or demodulated) output to the built-in speaker or headphones.

Press the «OSC» button to go to the oscillographic control of the signal parameters.

Press the «SA» button to go to the analysis of the spectrum of the demodulated signal.

In case of malfunctions, press the «RESET» button and restart the device.

5.2. Methods of search and localization of radio signal sources are used.

Information leakage channels in the radio frequency range can be created artificially (intentionally), due to the use of attackers by special technical means (radio microphones, telephone repeaters, unauthorized radio stations, beacons, etc.). They

can occur naturally, due to side electromagnetic radiation (SEMR) of technical means of information processing (PCs, telexes, faxes and the like).

In any case, there is a need to classify signals in the radio frequency range on a set of criteria for dangerous and safe, internal and external.

Dangerous radio signals can be generated by both internal and external sources. Moreover, in practice there is a fairly large number of their various combinations. Usually to purely internal dangerous radio signals include:

- radio bugs signals (radio microphones, telephone broadcasters, etc.);
- radio beacon signals;
- signals of radio stations and radiotelephones switched on in the premises without authorization;
- incidental electromagnetic radiation from a PC and other technical means of information processing.

To the category of dangerous, in combination internal and external, it is accepted to carry radio signals which sources can be:

- radio microphones with a portable acoustic microphone;
- telephone repeaters installed on the communication line outside the premises (but near it);
- radiostethoscopes installed on the outside of the surfaces that protect the premises;
- hidden transmitters of hidden video cameras;
- external high-frequency irradiation device.

When working with the device ST 031 «Piranha» use separately or in combination two main methods of search and localization of sources of dangerous radio signals. These are the so-called «Amplitude method» and the method of «Acoustic connection».

The ***«amplitude method»*** is based on a sharp increase in the level of the received signal when the receiving antenna of the device approaches the location of its source. The radius of the source detection zone depends on the power of the signal emitted by it, the direction of its antenna and the background level of the electric field at the location of the receiving antenna of the device.

After fixing the fact of detection of a potentially dangerous radio signal, you should move in the direction of increasing its level. The level of the received signal should be monitored according to the indications of the level indicators on the screen of the device and the frequency of clicks of the audible alarm in the «TONE» mode.

The method of «Acoustic connection» is based on the emergence of positive acoustic feedback between the microphone «radio bug» and the speaker of the device ST 031 «Piranha». Mandatory activation of the audible alarm of the device in the «AUD» mode for output to the speaker of the demodulated signal. The effect of

«acoustic connection» occurs only in relation to the «radio bug», which uses the usual types of modulation - amplitude and frequency (narrowband or broadband). Moreover, in the case of frequency modulation, the effect is based on the presence of «parasitic» amplitude modulation in the frequency-modulated signal (in the case of a qualitatively performed «radio bug» the effect of «acoustic communication» will be quite weak, up to complete absence).

A sign of «acoustic connection» is the appearance of a characteristic «squeak», the tone and intensity of which change when the speaker approaches the microphone «radio bug». It should be borne in mind that the presence of a characteristic sound when using this method unmasks the work. Therefore, in the case of the use of «radio bugs» with remote control, they can be turned off during the test.

The rational choice of this or that method in many respects depends on features inherent in potentially dangerous radio signals and their sources.

5.3. Features of search of radio-emitting ED.

Work begins on the preparation of the controlled room (object) and the device ST 031 «Piranha».

Preparing the room is to create conditions under which the minimum possible background level of the electric field is provided. This is achieved by disabling office equipment, PCs, converters and power supplies, base stations for cordless phones, fluorescent lighting lamps and other electronic devices and electrical appliances. It is also advisable to close windows and doors, lower curtains or blinds.

Particular attention should be paid to switching off radiotelephones and other radio transmitting devices, as well as active radio-technical protection devices, if they are equipped or adjacent to the premises under inspection. Simultaneous operation of the ST 031 «Piranha» device with nonlinear locators is not allowed.

To create an acoustic background and to activate radio bugs with an acoustic trigger, a test sound source should be prepared and placed in a controlled room - a tape recorder with music or speech phonogram. It is not recommended to use a radio or TV for this purpose.

If the object of inspection is a car, it is necessary to choose correctly, from the point of view of reduction of level of an electromagnetic background, a place of carrying out works. Thus, high-voltage power lines, transformer substations, radiating means of communication, TV and radio broadcasting, as well as large reflecting surfaces - metal fences, walls of houses, garages, and other cars - should not be located near it.

Preparation of the device ST 031 «Piranha» (after checking its operability in this mode) is to set the «zero» threshold of the device (paragraph 5.1), which is, in fact, crucial for successful work.

Following the above rules and restrictions, you can consider the room (object) being inspected, and the device ST 031 «Piranha» prepared for inspection work.

The sequence of searching for potentially dangerous radio signals and their sources is to check for:

- stand-alone radio microphones and telephone repeaters;
- camouflage radio microphones are powered by the mains;
- radiostethoscopes;
- hidden video cameras with a radio channel;
- spatial high-frequency radiation.

It is advisable to search for stand-alone radio microphones and telephone repeaters by disconnecting the power cords of all authorized consumers from the mains sockets and switching off the lighting fixtures with incandescent lamps.

Given the fact that the radio frequency path of the device ST 031 «Piranha» is made according to the combined scheme of the detector-frequency meter, the same techniques and methods are suitable for its application as for autonomous field detectors, interceptors and radio frequency meters. In general, they are as follows.

If there are no restrictions on the secrecy of the work, the best effect is given by a combination of the amplitude method and the method of "acoustic connection". When conducting a secret search, it is necessary to focus on the amplitude method with listening to the detected signals through headphones.

Particular attention is paid to radio emission in the range of 60 - 640 MHz, the most typical for use with radio microphones and telephone repeaters.

The search is carried out by a systematic tour of the room with movement along the walls and inspection of furniture and other items. Due to the rather high sensitivity of the high-frequency antenna, it is advisable to start the search with the use of a telescopic antenna. When bypassing the antenna, it is necessary to orient in different planes, making smooth, slow turns of the main unit and achieving the maximum signal level. It is advisable to keep the antenna of the device at a distance of not more than 20 - 25 cm from the inspected surfaces and objects. If there are no restrictions on the use of the «acoustic connection» method, the speaker of the built-in speaker of the device should be oriented towards the inspected surfaces and objects (the volume value should be set to at least 3/4 of the maximum).

As the antenna approaches the location of the «radio bug», the intensity of the electromagnetic field increases, and the signal level at its input increases accordingly. With exceeding the level of the signal set to «zero» threshold, depending on the type of signal, the number of colored sectors of one of the lines of level indicators increases and, starting from the fourth (countdown from zero), the frequency of clicks in the «TONE» mode increases «acoustic connection».

If a source with a frequency modulated signal is found, the number of colored sectors of the upper signal level indicator will increase. When sufficiently close to the source, the radio frequency meter «captures» the frequency and shows in the last line of the screen its value according to the results of several measurements. By reducing the volume with the «-» button, changing the limits of the dynamic range with the «SET» button, manually increasing the threshold of the detector, constant monitoring of the frequency meter readings narrows the survey area and, thus localizes the location of the «radio bug» with an accuracy of 10 - 15 cm. Additional ability to classify radio emissions gives the periodic inclusion of the «AUD» mode and listening to the demodulated signal.

However, the effect of «acoustic connection» and clear listening to the demodulated signal are not always observed. For example, if bugs have a masked radio channel. Therefore, the basis of their search is the use of the amplitude method in its pure form. Complementary here can be a simple reception. If you turn off the source of the test phonogram and create a short sharp sound in the room under test (loud clap, a blow on the table cover or a metal object), you can record the characteristic changes of the demodulated signal «by ear» in the «AUD» mode, changes oscillograms in the «OSC» mode and spectrograms in the «SA» mode.

If a «radio bug» with digital modulation methods is used, the level indication will appear on the lower indicator. The indication of the frequency of the received signal in this case will be random.

If DECT or GSM phones are used as a «radio bug», in addition to the signal level increase indicator in the bottom line, DECT or GSM will appear on the indicator.

The search for telephone repeaters is similar to the search for radio microphones. Thus for their activation it is necessary to remove handsets of all telephones. Actually the search is carried out in two stages.

First, the telephones themselves are checked for the presence of embedded devices. The radio repeater installed in the device is manifested in the same way as the radio microphone. When the antenna of the device approaches such a telephone, the means of sound (in the «TONE» mode) indication, the signal level indicator and the frequency meter react. When switching to «AUD» mode, either a continuous or intermittent tone of the telephone exchange is heard in the speakers or in the headphones. In some cases, an acoustic effect may occur when the handset microphone approaches the speaker of the ST 031. It is not recommended to test telephones in speakerphone mode (if provided), as this may cause a false «acoustic connection» between the microphone and the speaker of the device.

Next, the search for telephone repeaters is carried out by bypassing the room along the subscriber telephone line and identifying places on it with increasing (maximum) level of the radio signal. When bypassing the antenna of the device must be oriented in different planes at the minimum possible distance from the line. There

is almost always a need to check the line up to the main switchboard. Particular attention should be paid to junction boxes and places where the line is laid with hidden wiring. On-line telephone repeaters are localized mainly by the amplitude method, supplemented by an «acoustic connection» check.

Search for masked radio microphones powered by the mains, and the location of their installation is carried out by the same methods as described above. To activate them, you must turn on the test audio source. Alternately turn on existing lighting fixtures with incandescent lamps and connect the power cords of authorized consumers to electrical outlets. Consistently inspect each of the newly connected tools.

The search for radiostethoscopes has certain features due to the methods of their use (installation outside the controlled room). Therefore, to detect the signals of radiostethoscopes, it is necessary to inspect all available external surfaces of structures that protect the premises. Since the medium of propagation of vibroacoustic oscillations can be heating and water supply pipes, these communications are also subject to verification.

The vast majority of radiostethoscopes use an open radio channel. This makes it possible to analyze the received signal «by ear» in the «AUD» mode. When inspecting structures that protect the premises, the antenna of the device should be located at the minimum possible distance from the inspected surfaces, as the radius of the detection zone of the signal from the radio stethoscope is usually smaller than from the radio microphones. When checking the pipeline communications, it is necessary to follow the same recommendations, but do not allow the antenna to come into contact with metal surfaces.

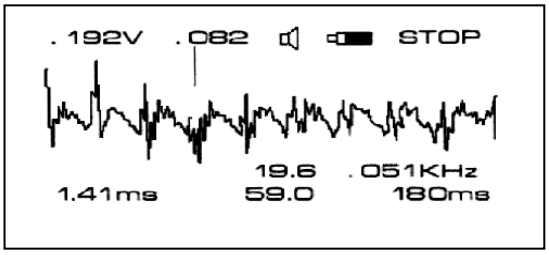
Localization of radiostethoscopes is carried out by the amplitude method in adjacent rooms, which is supplemented, if necessary, by the use of «OSC» and «SA» modes.

Finding hidden video cameras with a radio image channel (often audio) is associated with some difficulties, which are determined by the similarity of the video transmitter signal with the brightness signal of television transmitters and the operation of a significant number of these devices in the range (60 to 500 MHz).

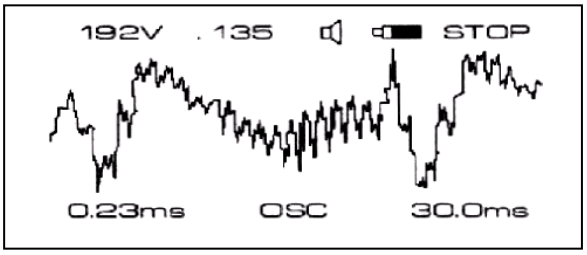
Therefore, in the course of work when detecting such a signal, the first task is to recognize it by the criterion of «external-internal». To recognize it is necessary to close the windows with curtains or blinds, leaving the interior lighting on. Make artificial lighting on and off several times. When the «AUD» mode is on, clear changes in the tone of the detected signal must be heard. To increase the reliability of recognition, turn on the «OSC» mode and make sure to change the signal structure on the oscillogram when turning on and off the lights. The type of oscillogram of the radio signal of video information transmission at different values of the horizontal scan parameters is shown in Pic. 2 and 3.

If the results of such a test are positive, the signal can be safely classified as internal, created by the transmitter of the video camera, because the change in lighting of the room does not affect the parameters of the television signal.

In principle, video camera transmitters can operate at frequencies up to 2300 MHz. The detection of a signal (similar to the brightness signal) on frequencies outside the range of television broadcasting almost clearly indicates the operation of the transmitter of the hidden video camera. Localization of such means is carried out by an amplitude method.



Pic.2. Radio signal for video transmission, scanning period 180 ms



Pic.3. Radio signal for video transmission, scanning period 30 ms

To detect spatial high-frequency irradiation, the main task is to detect the fact of creating this artificial channel for information retrieval. It is usually solved in two stages. At the first stage, the fact of irradiating the room with a high-frequency signal is revealed. In the second stage, the response to the probing high-frequency signal is monitored. It is necessary to focus on the following points.

Sharply directed beam of electromagnetic energy can be formed only at very high frequencies (800… 900 MHz and above). Peculiarities of radio wave propagation in this range (the need for «direct visibility» between the radiation source and the irradiated objects) determine as the main ways of their penetration into the controlled room, first of all, window openings. Objects that re-emit can be common for this room technical means that have a so-called microphone effect (parasitic acoustoelectric transducers). These usually include the speakers of household speakers, acoustic systems, even turned off audio equipment, telephones with electric bells and the like. The signal re-emitted at higher frequencies (usually the second or third) is localized in the immediate vicinity of the irradiated objects and is modulated by the acoustic background of the room.

Based on this, the following procedure can be used.

To identify the fact of high-frequency radiation, alternately inspect potentially dangerous window openings. To do this, raise the antenna to the inner glass at a distance of 5-10 cm, record the level and frequency of the most powerful signal. Turn on the «AUD» and «by ear» mode to determine the presence and features of the demodulated signal. Use a graphical indicator to evaluate the stability of the radiation frequency. Go to any of the adjacent rooms (oriented windows in the same direction)

and repeat the inspection in the area of each of its window openings. High frequency irradiation is quite probable if:

- the frequency of the received signal is (or very close) within the specified range;
- frequency stability is high;
- no signal modulation;
- in the adjacent premises, in relation to the inspected premises, the level of the received signal is much lower.

To identify sources of re-radiation, it is necessary to carefully inspect each of the potentially dangerous objects, placing the antenna of the device in close proximity to it. The basis for the final decision on irradiation and the presence in the room of objects that re-emit, is the evidence of the level indicator of the device ST 031 «Piranha» and its frequency meter, as well as the results of listening in the «AUD» mode. In this case, the main features are usually considered to be the fixation of the nominal frequency, a multiple of the third harmonic of the irradiating signal and the identification of the sound signal in the «AUD» mode with the acoustic background of the room.

The method of search and localization of unauthorized ***radio stations, radio telephones, telephones with extension cords and radio beacons*** is completely similar to the method of search and localization of radio microphones. Moreover, in the vast majority of cases should focus on the amplitude method with periodic listening to the demodulated signal in the «AUD» mode.

6. Search for EDs that using wire lines using the ST 031 device in the mode of the scanning analyzer of wire lines (WIRE LINES ANALYSIS).

6.1. The order of control of the device in the mode of the scanning analyzer of wire lines.

Connect the mains adapter to the «PROBES» connector and its probes to the wired line (mains line with voltage up to 600 V). Turn on the power of the device. The scanning mode of the wire line analyzer will turn on and the inscription «WIRE LINES ANALYSIS» will appear on the LCD.

Wait for 2, 3 times the «pass» of the scanning range of the marker within the automatically set range of 0.1 ... 10.450 MHz. If necessary, set the most rational limits of the scan frequency range:

- press the «SET» button, then the «4» button. Press the numbered buttons to dial a number that corresponds to the lower limit of the range. Press the «ENTER» button and confirm the completion of the lower limit value setting;
- Press the numbered buttons to dial the number corresponding to the upper limit of the range, press the «ENTER» button to confirm the setting of the upper limit of the range.

Press the «<» or «>» button and select the desired scanning direction and speed.

Press the «SET» button, then the «3» button until «3 - > ↑↓ THRESHOLD level» appears on the screen in the fourth line.

Press the «ENTER» button and return to the panorama image screen.

Press the «Δ» and «∇» buttons to set the most convenient limit of the signal level meter display (inscription under the horizontal axis «level threshold = XX%»).

Press the «RUN / STOP» button to stop the auto scan at the desired point on the frequency axis. Press the «<» or «>» buttons to make a precise manual tuning to the frequency of interest. Listen to the demodulated signal. Press the «ENTER (AM/FM)» button and select the type of demodulation («by ear», according to the quality of its playback). Press the «RUN / STOP» button and return to auto scan.

Enable the system to automatically stop scanning on the most pronounced (in amplitude) frequency components of the panorama.

Press the «SET» button, then use the «3» button to set «3 - > ↑↓ SQUELCH level» in the fourth line of the menu. Press the «ENTER» button. Use the «Δ» and «∇» buttons to select the desired level of auto stop auto scan (according to the position of the short horizontal line on the right side of the screen). After stopping the scan, use the «<» and «>» buttons to adjust the setting according to the quality of the demodulated signal.

To continue scanning, press the «RUN/STOP» button.

Enable spectrum subtraction mode:

- press the «SET» button, then the «2» button and set the inscription «2 –> Difference ON D2 – 1»;
- press the «ENTER» button to start the subtraction procedure;
- exit the spectrum subtraction mode - press the «SET» button, then the «2» button and set the inscription «Difference OFF», press the «ENTER» button.

To record a panorama image in non-volatile memory: press the «SAVE» button, then «ENTER».

View in memory and display a previously saved panorama image:

- press the «LOAD» button;
- press the «RUN/STOP» button and return the dynamically displayed panorama to the screen.

Deleting an image of any panorama is performed by pressing the «LOAD» buttons, then «SAVE» and «ENTER».

The transition to oscilloscope control of parameters is carried out by pressing the «OSC» button.

The transition to the analysis of the signal spectrum is performed by pressing the «SA» button.

Restart the device in case of malfunction by pressing the «RESET» button.

6.2. Features of ED search that use wired communications.

The search for such ED is to identify artificially created channels of information leakage along wired lines, which are based on the use of special technical means. The main types of wired lines, for the analysis of which the device ST 031 «Piranha» is intended, are power lines, as well as subscriber telephone lines and lines of fire and burglar alarm systems.

In general, the techniques and methods used to check the wire lines of these types are the same. Connection to them is carried out using a single, universal adapter. The general frequency range from 0 to 15 MHz is analyzed by scanning. The output of scan results is made in the form of a panorama image with the same display of measured parameters. The functions of the device controls are the same (regardless of the type of line being tested).

The general (for all lines) provisions of the method of work are as follows.

Preparation of the controlled room consists in check of conformity of quantity and purpose of actually existing in it wire lines earlier made (presented) in schemes of their laying.

The preparation of the ST 031 device (after checking its operability in this mode) actually consists only in choosing the most convenient tips for the probes, in relation to the type of wire lines being tested.

Most attention should be paid to the frequency range of 40 - 2500 kHz, as the most typical for use with bugs that are powered by the voltage of the wire lines and transmitting intercepted information on their wires. Embedded devices with frequencies of about 7 MHz and above are much less common. To ensure the guaranteed reliability of the transmission of bug signals by frequency, the upper limit of the scanning range in the device ST 031 «Piranha» is set at 15 MHz.

The procedure for the operator to detect ED.

Switch on the appliance. Wait for the start of scanning in the range up to 10.450 MHz and after the completion of 2, 3 cycles set the upper limit of the range at 15 MHz. Having carefully studied the most characteristic features of the panorama image to determine the presence of frequency components that exceed the level of the general background.

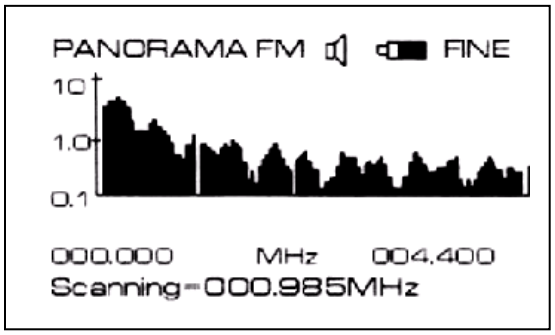
If necessary, divide the range into separate intervals and scan them in detail, focusing primarily on the frequencies of the most intense components. The interval limits are set by pressing the «SET», «4» buttons, the numbered buttons and the

«ENTER» button (or an alternative with the setting of the center frequency and bandwidth).

Set the lower threshold of the signal level indication to about 10-15%. To do this, press the «SET» button, use the «3» button to display «3 - > ↑↓ THRESHOLD level», press the «ENTER» button and use the «Δ» and «∇» buttons to set this display threshold. In the future, depending on the nature of the image of the panorama, choose the most convenient for analysis level threshold. Start and stop scanning by pressing the «RUN/STOP» button.

After several scanning cycles, you can reasonably set the threshold of «auto stop» for which press the «SET» button, select the «3» button mode «SQUELCH LEVEL», confirm the selection with the «ENTER» button and, manipulating the buttons «Δ» and «∇», put cursor to the required level. After stopping at the frequency of a signal, you should make a precise adjustment with the «<» and «>» buttons, while analyzing the signal «by ear» by alternately turning on the detectors «AM» and «FM» with the «ENTER» button. For the analysis of weak signals, it is possible to choose buttons «SET», «5» and «ENTER» more convenient amplitude range (0,1 - 1,0 mV).

If additional analysis of signals in wire lines is required, switch the device to «OSC» or «SA» modes, as the images of oscillograms and spectrograms of signals displayed on the display screen give a more detailed description of the parameters. This can be seen by comparing the image of the panorama and the waveform of the same digital signal for the transmission of speech information (Pic. 4 and Pic. 5).



Pic.4. Panorama of digital signal for voice information transmission in a wired line.

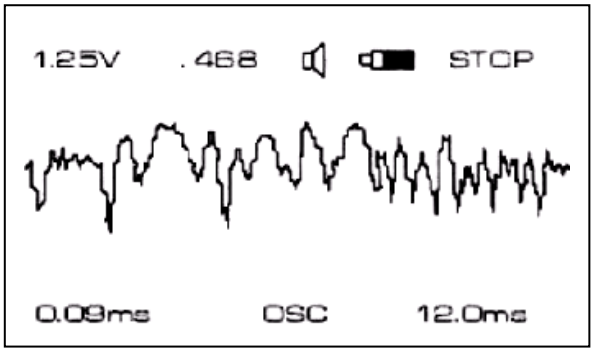


Рис.5. Oscillogram of digital signal of voice information transmission in a wired line (same signal)

If the room is regularly inspected, it is advisable to save in non-volatile memory panorama (oscillogram, spectrogram) of the required frequency intervals.

When searching for ED in wire lines, it is necessary to take into account the specifics of the lines of each type.

It is advisable to start checking the presence of ED in the mains, which receive acoustic signals from the room, are fed from the network and transmit information at high frequency on its wires from the mains sockets. To reduce the background level,

all electrical appliances and equipment located in the controlled room should be switched off (with visible disconnection from sockets).

Connect the appliance to the mains using any of the sockets.

Analyze the image of the panorama.

If a signal is detected that contains signs of modulation by the acoustics of the room, then the method of «acoustic connection» can be used to localize its source, with alternate connection to all sockets in the room being tested.

Carry out a similar test on the elements of the lines supplying electric lighting fixtures.

After checking the power lines and power lines of lighting fixtures, it is necessary to check tees, extension cords and other power consuming devices by alternately connecting them to the mains.

Checking the wired lines of fire and burglar alarm systems, as well as lines of unknown purpose is similar to checking the power lines, because they are similar to the technical means used in these communications.

When checking subscriber telephone lines, in addition to searching for the special technical means described above, it is necessary to solve the problem of identifying the fact of using the line to extract acoustic information from the premises due to linear high-frequency imposition. A sign of the fact of linear high-frequency imposition is the presence in the line of an unmodulated stable probing signal at frequencies not lower than 150 kHz. In this case, the order of connection of the device and the analysis procedure does not differ from that set out in relation to the inspection of power lines.

Checking the wire lines of fire and burglar alarm systems, as well as lines of unknown purpose is similar to checking power lines, as similar to the technical means used on these communications.

When checking subscriber telephone lines, in addition to searching for the special technical means described above, it is necessary to solve the problem of identifying the fact of using the line to obtain acoustic information from the premises due to linear high-frequency imposition. A sign of the fact of linear high-frequency imposition is the presence in the line of an unmodulated stable probing signal at frequencies not lower than 150 kHz. In this case, the order of connection of the device and the analysis procedure does not differ from that set out in relation to the inspection of lines.

7. Search for EDs that using low-frequency magnetic radiation using the ST 031 device in the mode of low-frequency magnetic field detector (MAGNETIC CHANNEL).

7.1. The order of control of the device in the mode of the detector of low-frequency magnetic fields.

Connect the external magnetic antenna to the connecting cable and the cable itself to the «PROBES» connector. Turn on the power of the device. The low-frequency magnetic field detector mode will turn on automatically and «MAGNETIC CHANNEL» will appear on the monitor. Oscillographic control of the parameters of the signal received by the magnetic field is turned on automatically.

Visually on the amplitude and nature of the signal on the oscillogram and «by ear» on its key in the built-in speaker or headphones to assess the level of the magnetic field and the presence of the background of the mains 220V, 50Hz or its harmonics. If necessary, in the case of a high level of the mains background, turn on the differential mode of the antenna with a switch on its body (position «to the white dot»).

Press the «RUN/STOP» button to start and stop dynamic measurements.

Press the «MUTE» button and the «+» and «-» buttons to set the desired volume of the signal output to the built-in speaker or headphones.

Press the «SA» button to go to the analysis of the spectrum of the received signal.

In case of malfunctions, press the «RESET» button and restart the device.

7.2. Features of ED search that use low-frequency magnetic fields.

In the mode of the low-frequency magnetic field detector, the ST 031 device receives on the external magnetic antenna and displays the parameters of signals from low-frequency electromagnetic field sources with a predominant (available) magnetic component of the field in the range from 300 to 5000 Hz.

The identification of signals and their sources is based on the analysis so that the oscillogram is automatically displayed on the screen, which reflects the shape of the received signal and the current value of its amplitude. Improving the reliability of identification of signals and their sources is provided by the possibility of simultaneous analysis of the image on the display screen, listening to the «background» situation using the built-in speaker or headphones.

The peculiarity of low-frequency magnetic channels of information leakage is that they occur when used for the intended purpose of authorized means - PCs, intercoms, sound amplification systems, tape recorders, telephones and so on. Therefore, one of the main tasks should be the study of such tools for the presence, intensity and range of low-frequency magnetic field. Accompanying tasks of searching

for hidden (unauthorized) wiring and detecting working dictaphones can be considered accompanying.

Before carrying out works it is expedient to switch off luminescent lamps indoors, and to include the antenna of the device, if necessary, in the differential mode.

Potential sources of dangerous low-frequency magnetic fields should be checked separately, including them in the work in turn.

At research of *technical means,* it is necessary to estimate range of propagation of magnetic fields and features of their spectrum. To do this, first place a magnetic antenna in close proximity to the object under study. Record the relative level of the field on the oscillogram. Moving away from the test tool and changing the spatial orientation of the antenna, estimate the range of reliable reception of the low-frequency signal.

With respect to *audio frequency amplifiers* having an output transformer, the range of reliable (legible) reception of the speech (test) signal should be assessed. Such an assessment can serve as a basis for the correct choice of places of installation of appropriate means in relation to the outside of the room and the option of their joint location in the room. If necessary, turn on the «SA» mode, analyze the spectrogram and write it to non-volatile memory.

To find the *hidden wiring*, it is necessary to bypass all the walls of the room, placing the magnetic antenna in close proximity to them. Fix the area of growth of the field level and by moving the antenna horizontally and vertically to determine the passage of the hidden wiring route.

The ability to detect *working dictaphones* is determined by both the level of the magnetic field generated by their motors and the level of the magnetic background of the room. To solve this problem usually use specialized tools with careful preparation of the premises. Therefore, a positive result can`t always be achieved only when using the device ST 031 «Piranha», especially at a distance between the recorder and the magnetic antenna of 30 cm or more.

8. Search for EDs that use infrared radiation using the ST 031 in the INFRARED CHANNEL mode.

8.1. The order of control of the device in the mode of the detector of infrared radiation

Connect the infrared sensor to the connecting cable and the cable itself to the «PROBES» connector. Turn on the power of the device. The infrared detector mode will turn on automatically and «INFRARED CHANNEL» will appear on the monitor.

The «zero» threshold of the detector is set when turned on automatically. If necessary, set the detector threshold manually by pressing the «<» or «>» buttons,

following the readings of the additional scale «min - - - | - - - max». If necessary, press the «Δ» button to return to the automatic threshold setting.

Visually evaluate the level of infrared radiation by the number of fully colored elements of the 21-segment scale and «by ear» by the frequency of clicks in the built-in speaker or headphones.

Press the «RUN/STOP» button to start and stop the dynamic measurements of the infrared radiation level. Press this button again to resume dynamic measurements.

Press the «ENTER» button (switch the audio indication to «AUD» mode), listen to the presence and content of potentially dangerous modulated infrared radiation.

By pressing the «MUTE» button and the «+» and «-» buttons, set the required volume output either to the built-in speaker or to the headphones of the audio signal (tone or demodulated).

Press the «OSC» button to go to the oscilloscope control of the parameters of the demodulated signal.

Press the «SA» button to go to the analysis of the spectrum of the demodulated signal.

In case of malfunctions, press the «RESET» button and restart the device.

8.2. Features of ED search that use infrared radiation.

In the mode of the infrared radiation detector, the ST 031 device provides, using a remote sensor, the reception of infrared sources in the near area, their detection and output for auditory control and analysis in the form of alternating tonal parcels (clicks) or in the form of explicit phonograms. listening. At any time against the background of the real situation of interference is received and is the most powerful of all signals in the operating range.

When studying sources of infrared radiation, two types of such channels of information infiltration should be considered. One of them is created through the use of special technical means with the transmission of intercepted information in the infrared range. Another channel is based on irradiating the glass of window openings with a directed beam of an infrared radiation source and receiving a reflected signal modulated by the room acoustics.

The same preparatory measures must be taken to identify both leakage channels. First of all, you should choose the right time for the inspection, namely when the windows of the controlled room do not get direct sunlight. Incandescent lamps and sources of intense heat radiation must be switched off in the room. It is also advisable to turn off the color TV, as the sensor of the device can respond to «warm» tones of the image.

The specificity of infrared bookmarks necessitates the provision of «direct visibility» between the transmitter of the bookmark and the receiver of infrared radiation. Therefore, in the room, the path of the transmitter radiation to the outside can pass only through the window openings. Given these features, the search for dangerous signals should start from the windows of the room, moving to its middle. Since the transmitter can have a rather narrow pattern, and the point of view of the sensor of the device is 30°, it is necessary to smoothly change the spatial orientation of the sensor. A sign of the presence of infrared radiation is the appearance of colored segments of the scale of the level indicator and clicks of the sound indication in the «TONE» mode after the coloring of the 4th element of the scale. The analysis of the detected signals can be performed «by ear» in the «AUD» mode, as well as visually using the built-in oscilloscope and spectrum analyzer. The localization of infrared radiation sources is most accurately performed by a combination of the amplitude method and the «acoustic connection» method. The procedure is the same as when operating in the mode of a high-frequency detector-frequency meter.

Each window opening must be inspected to detect external potentially dangerous infrared radiation. The sensor is oriented towards the window. Gradually changing its spatial position, to survey the entire area of the window opening. Since the probe signal is not modulated, its presence can be assessed only by the indications of the level indicator and tone indication in the «TONE» mode.

9. Use of the device to evaluate the effectiveness of vibroacoustic protection and sound insulation of premises

9.1. The order of control of the device in the mode of the vibroacoustic receiver (in the mode of the acoustic receiver).

Connect an external vibroacoustic sensor (remote microphone) to the «PROBES» connector. Turn on the power of the device. The vibroacoustic receiver (acoustic receiver) mode will turn on automatically and «VIBRO - ACOUSTIC CHANNEL» («ACOUSTIC CHANNEL») will appear on the monitor.

Oscillographic control of the parameters of the signal received on the vibroacoustic (acoustic) channel is turned on automatically.

Visually on the amplitude and nature of the signal on the oscillogram and «by ear» on its legibility and quality in the built-in speaker or headphones to assess the level and timbre characteristics of the converted audio signal.

Press the «RUN / STOP» button to start and stop dynamic measurements.

Press the «MUTE» button and the «+» and «-» buttons to set the desired volume of the signal output to either the built-in speaker or the headphones.

Press the «SA» button to go to the analysis of the spectrum of the received signal.

In case of malfunctions, press the «RESET» button and restart the device.

9.2. Evaluation of the effectiveness of vibroacoustic protection and sound insulation of premises.

In the mode of the vibroacoustic receiver (acoustic receiver) the ST 031 device provides reception from the remote vibroacoustic sensor (from the remote microphone) and display of parameters of low-frequency acoustic signals in the range of 800-6000 Hz.

The state of vibroacoustic protection and sound insulation of the room is assessed both quantitatively and qualitatively. Quantitative assessment is based on the analysis of the waveform of the received signal and its amplitude. Qualitative assessment is based on direct listening to the received low-frequency signal, analysis of its volume and timbre characteristics.

The combination of these uses of the device is determined by the common sources of information leakage channels (speech signal in the acoustic range), the similarity of control techniques and the practical identity of the use of the capabilities of ST 031 «Piranha».

First, in both cases, when preparing the room, you must turn off devices and tools that create an additional acoustic background.

Second, in both cases, test and, best of all, calibrated audio sources should be used.

Third, in adjacent rooms, in relation to what is being inspected, the minimum possible level of acoustic background must be provided.

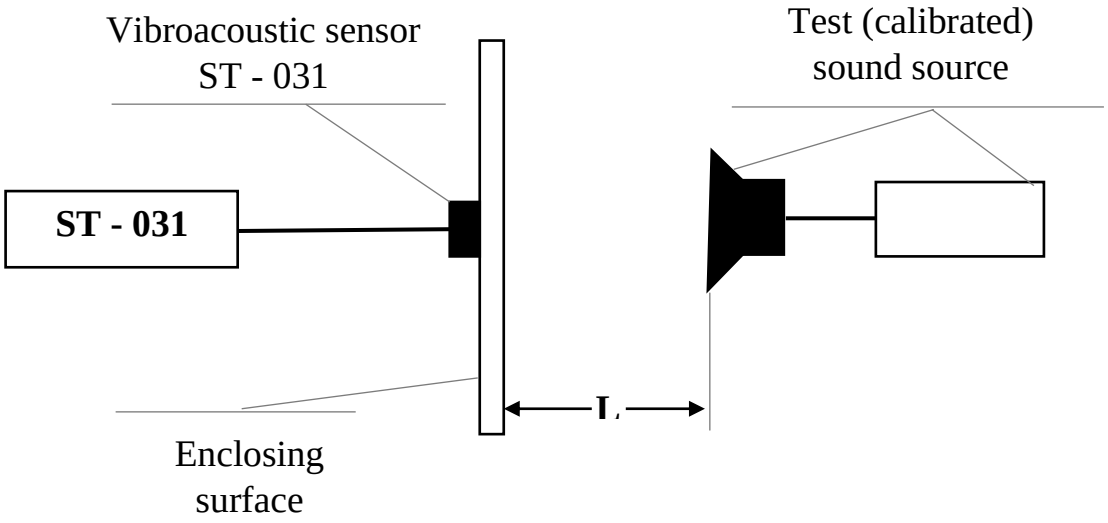
Fourth, use almost the same methods of signal analysis («by ear», on oscillograms and spectrograms).

Evaluation of the effectiveness of vibroacoustic protection of the premises is usually carried out in two stages. At the first stage, the protection, if any, should be turned off and the actual vibroacoustic properties of the surfaces protecting the room should be checked. For this purpose, it is necessary to attach the vibroacoustic sensor in various places of surfaces (walls, doors, windows, if possible floors and ceilings) which are checked, from outside, in relation to the controlled room, the party.

Turn on the test audio source. It can be placed either in the usual place of confidential conversations, or at a certain distance from the examined surface (for example, as shown in Pic. 6).

The sound level is usually set to correspond to the loud speech (74dB). For calibrated sound sources, the distance «L» is chosen within 1-2 m. First, the vibroacoustic properties of the examined surfaces are evaluated at a qualitative level

(by direct listening), and then, by switching to «SA» mode, the amplitudes of the frequency components of the test are quantified signal.



Pic. 6. Scheme for assessing the vibroacoustic properties and vibroacoustic protection of premises

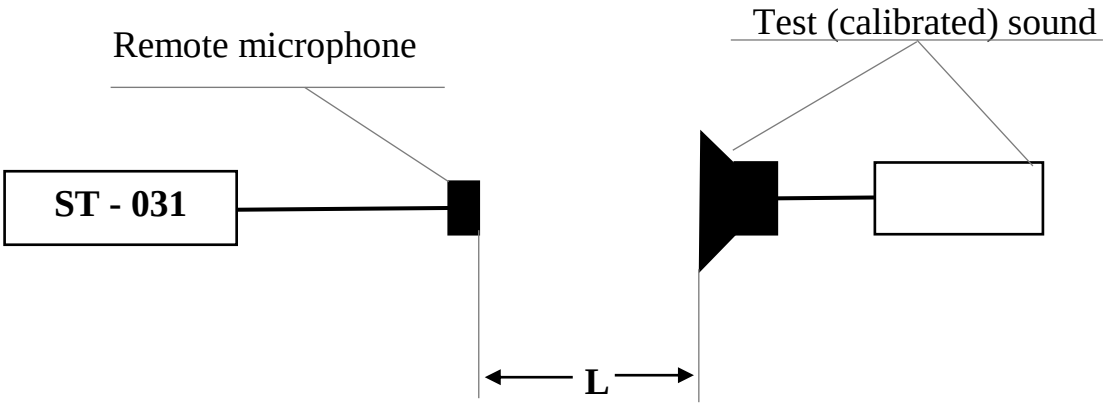
In the second stage, if provided, the effectiveness of the vibroacoustic protection system is evaluated. To do this, on each surface, both qualitatively «by ear» and quantitatively on the spectrogram, the ratio of the levels of the test and masking signal is determined, and «uncovered» components of the spectrum are detected. This serves as an objective basis for the correction of the amplitude-frequency characteristics of the masking signal sources.

According to the generally accepted rules, the legibility of speech signals is guaranteed not to be restored if the masking noise (interference) is 4-5 times (16 dB) higher than their level. Complete exclusion of speech features is achieved by 8 times exceeding the signal level by an obstacle created by the active protection system.

It is also advisable to assess the sound insulation of the premises in two stages.

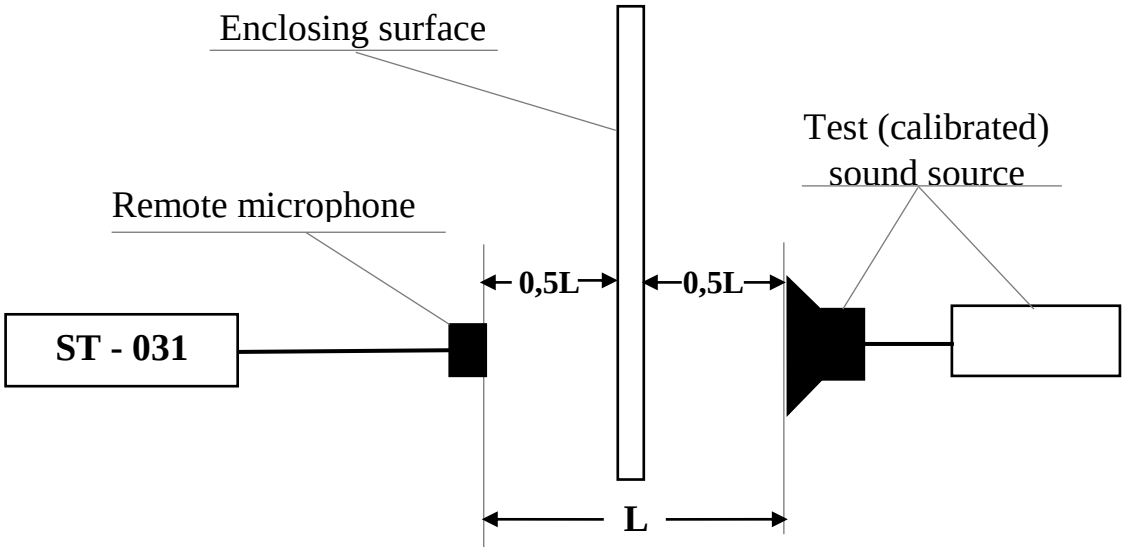
In the first stage, using a test signal source with a sound level corresponding to the loud language, to establish a correspondence between this level and the readings of the device ST 031 in the modes of the oscilloscope and spectrum analyzer. To do this, place the acoustic emitter of the sound source and the microphone of the device ST 031 at some fixed distance. It is usually chosen within 1-2 m (Pic. 7).

The second stage evaluates the sound insulation properties of surfaces (walls, doors, windows, and if possible, floors and ceilings) that protect the room, the effectiveness of the active protection system (noise), as well as the possibility of leakage of speech acoustic information through ventilation elements, various niches, through holes, etc.


Remote microphone
Test (calibrated) sound
ST - 031
L

Pic. 7. Scheme of calibration of indicators of level of a sound signal of the ST 031 device

To assess the sound insulation properties of walls, doors, floors, ceilings the test sound source can be located either in the usual place of confidential conversations, or at a distance from the inspected surface. For example, in the embodiment shown in Pic. 8.



Pic. 8. Scheme of assessment of sound insulation of premises

Placing the microphone in different places of adjacent (above and below) rooms qualitatively «by ear» and quantitatively on the spectrogram to determine the range of interception of speech information from this room and assess the reduction of the sound signal due to the properties of protective surfaces, as well as the least weakened components spectrum. The latter makes it possible to make an informed decision about the need for additional protection, including active and the choice of characteristics of protection.

If the room is located above the first floor, there are some difficulties in checking the sound insulation of window structures. In this case, the following, often used technique gives a sufficient effect for qualitative assessment. The test sound source is placed on any of the previously considered options. The window, transom or other part of a window opens, depending on features of window bindings. The microphone is hung outside and in this position the level of the test signal received by it from the room

is fixed. Then open the window carefully (so as not to damage the microphone cable), but, if possible, tightly covered. Qualitatively «by ear» and quantitatively by the oscillogram or the spectrogram sound-insulating properties of window designs are estimated.

Since the air ducts of ventilation systems are considered to be the most dangerous channels of leakage of speech acoustic information, they are subject to mandatory inspection. To do this, the microphone of the device ST 031 must be inserted into the outlet (inlet) of the air duct of each of the adjacent rooms, and possibly some others. Qualitatively «by ear» to assess the passage and legibility of the signal from the test source, and according to the device ST 031 in the mode of the oscilloscope or analyzer of its attenuation spectrum when passing through the air duct to the location of the microphone. Thus the correct estimation of attenuation can be received only if there is a detailed scheme of system of ventilation. Its presence makes it possible to take into account the attenuation introduced by various elements of the design of air ducts. Thus, the attenuation of the speech signal is usually:

0.15 dB/m - in direct metal air ducts;

0.2 - 0.3 dB/m - in direct non-metal air ducts;

1.0 - 3.0 dB/m - when changing the cross section of the duct;

3.0 - 7.0 dB/m - per bend of the duct.

The results of the inspection serve as an objective basis for deciding on the need for additional protection, for the choice of measures and means to ensure it.

Addition 4

METHOD OF SEARCHING EMBEDDED DEVICES USING NONLINEAR LOCATOR NR - 900EM

Pic. 1. Outward of nonlinear locator NR - 900EM

1. Appointment

Nonlinear locator NR900EM (hereinafter - the product) is a meter of secondary fields and is designed to search for devices containing semiconductor components, regardless of their functional state.

The product provides the ability to effectively search for any type of radio microphones, including remote control, as well as microphone amplifiers of wire microphones, means of implicit recording of information in the infrared and ultrasonic ranges, sound recording. The energy potential of the product provides an effective search in the elements of the interior and in building structures (floor, ceiling, walls).

Simultaneous reception of the second and third harmonics of the probing signal, visual indication of their levels, as well as the mode of selection of the envelope reflected signal (mode «20K»), allow the operator to distinguish signals reflected from semiconductor radio elements from signals of natural (corrosive) nonlinear. The pointed antenna system, a wide range of adjustments of the basic parameters of a product provide high accuracy of localization and facilitate carrying out search actions.

2. Technical data

The detection ranges of the standard imitator (diode 2D521A) is not less than 0.7 m. The product is powered from the built-in stand-alone AC source - battery

«Panasonic VBF – 2E» (operating time not less than 4 hours.) Or from the AC mains 220V, 50 Hz through the mains adapter.

Detection indication: visual - on a four-line monitor and audio - on headphones.

The weight of the product in the standard packaging does not exceed 12 kg. The weight of the equipped receiver unit does not exceed 3.0 kg.

The average power supplied to the antenna is not more than 0.1 W in the «300» mode and not more than 0.3 W in the «20K» mode.

Probe signal power adjustment minus 8±1 dB.

The sensitivity of the receivers at a ratio of S/N = 10 dB is not worse - 115 dB/W.

Dynamic range of receivers not less than 25 dB.

The sensitivity of the receivers is adjusted by five steps of minus 10±2 dB in each.

The gain of the receiving and transmitting antennas is not less than 8 dB.

Polarization - circular, elliptical coefficient not less than 0.75.

The width of the main petal of the pattern of transmitting and receiving antennas at the level of half power is not more than 40 degrees.

The level of the rear petals of the pattern for transmitting and receiving antennas is not more than minus 20 dB.

3. Product composition:

receiver unit	1 pc.
antenna system with a rod	1 pc.
control panel and indication	1 pc.
set of RF cables	1 pc.
headphones	1 pc.
imitator	1 pc.
mains adapter	1 pc.
accumulator	2 pc.
charger	1 pc.
suitcase	1 pc.
passport	1 pc.
technical description and operating instructions	1 pc.

4. Device and operation

The product «NR – 900EM» is a portable device consisting of an antenna system, a transmitter and two receivers, and the receivers are tuned to double and triple the frequency of the transmitter signal. Control of operating modes is carried out by means of the remote control. The probe signal of the transmitter is converted on

nonlinear (semiconductor) elements of the electronic device, re-emitted, registered by receivers and presented to the operator in visual and audio form.

5. Product construction, governing and control bodies

5.1. The product consists of three structurally independent blocks: the receiver, the antenna system, and also the control panel and indication connected by cables. The antenna system and the control panel in the working position are mounted on a sliding telescopic rod.

5.2. The receiver unit in the working position by means of a belt is located on the operator's shoulder.

On the top panel of the block there are connectors:

«OUT» - the output connector of the transmitter, marked with a red dot;

«IN» - input connector of the receiver, marked with a blue dot;

«HEADPHONES» - headphone jack;

«AC 15V» - connector for connecting the power adapter cable.

On the top panel of the unit under the shift cover there is a compartment of the autonomous power supply.

5.3. The controls of the product are located on the control panel and are made in the form of non-locking buttons, provide the following functions:

ON/OFF - power button, «LISTEN MODE» mode off and product power off;

LIGHT - button to turn on and off the backlight of the monitor;

VOLUME (+/-) - Two buttons to increase and decrease the volume of the signal in the headphones;

300/20 K - button to change the modulation mode of the probing signal of the transmitter;

MAX/MIN - button to change the output power of the transmitter;

OUT 2/3 - the signal selection button listened to in the headphones - the second or third harmonic;

ATT (+/-) - two buttons to adjust the sensitivity of the receivers - increase and decrease the attenuation.

5.4. The antenna system of the product is placed in a plastic fairing. On the back of the antenna system is the node for attaching it to the rod and two high-frequency connectors with color marking:

- red dot - transmitting antenna, connected by a cable to the «OUT» connector on the receiver unit;

- blue dot - receiving antenna, connected by a cable to the connector «IN» on the receiver unit.

5.5. Probe antennas are segments of flexible conductor 0.6 m long (2 pc.) And a segment of elastic conductor 0.6 m long (1 pc.) With connectors at one end.

5.6. The matching device is made in the form of a handle, on which are located: two connectors with colored markings (red and blue dots) for connection to the receiver unit; connector for connecting a probe antenna (unmarked); control panel mounting unit; mounting node of the standard antenna system.

6. Preparation for work

6.1. Remove the product blocks from the standard packaging.

6.2. Secure the antenna system to the boom using the mounting assembly.

6.3. Connect the antenna system to the receiver following the color coding.

Warning. Switching on the receiver without the antenna system connected is not allowed.

6.4. Connect the headphones to the **«HEADPHONES»** jack of the receiver.

6.5. Install the battery in the compartment located under the offset cover on the top panel of the receiver or connect the connector of the mains adapter to the DC 15V socket.

6.6. Connect the control panel cable to the **CONTROL** connector of the receiver. The display should show: **RADAR TURNED ON.** The product is ready to switch on.

7. The order of search for embedded devices

7.1. Before switching on the product, make sure that the antenna system is connected.

7.2. Press the ON/OFF button on the control panel once - the mode in which the transmitter is switched off, the receivers are switched on, the receiver attenuators are set to minus 10 dB, the headphones are connected to the receiver of the second harmonic, the volume is in the middle position.

Using the **ATT** button - set the maximum sensitivity of the receivers, the monitor on the left side of the 1st and 2nd line should display the characters 00. By directing the antenna system in different directions and connecting the headphones to the outputs of the receivers of the second and third harmonics with the **OUT 2/3** button, make sure that there are no interferences at the reception frequencies at the maximum sensitivity of the receivers. Otherwise, evaluate the ability to work with the product by setting the attenuators of the receivers so that the interference signal is below the sensitivity threshold.

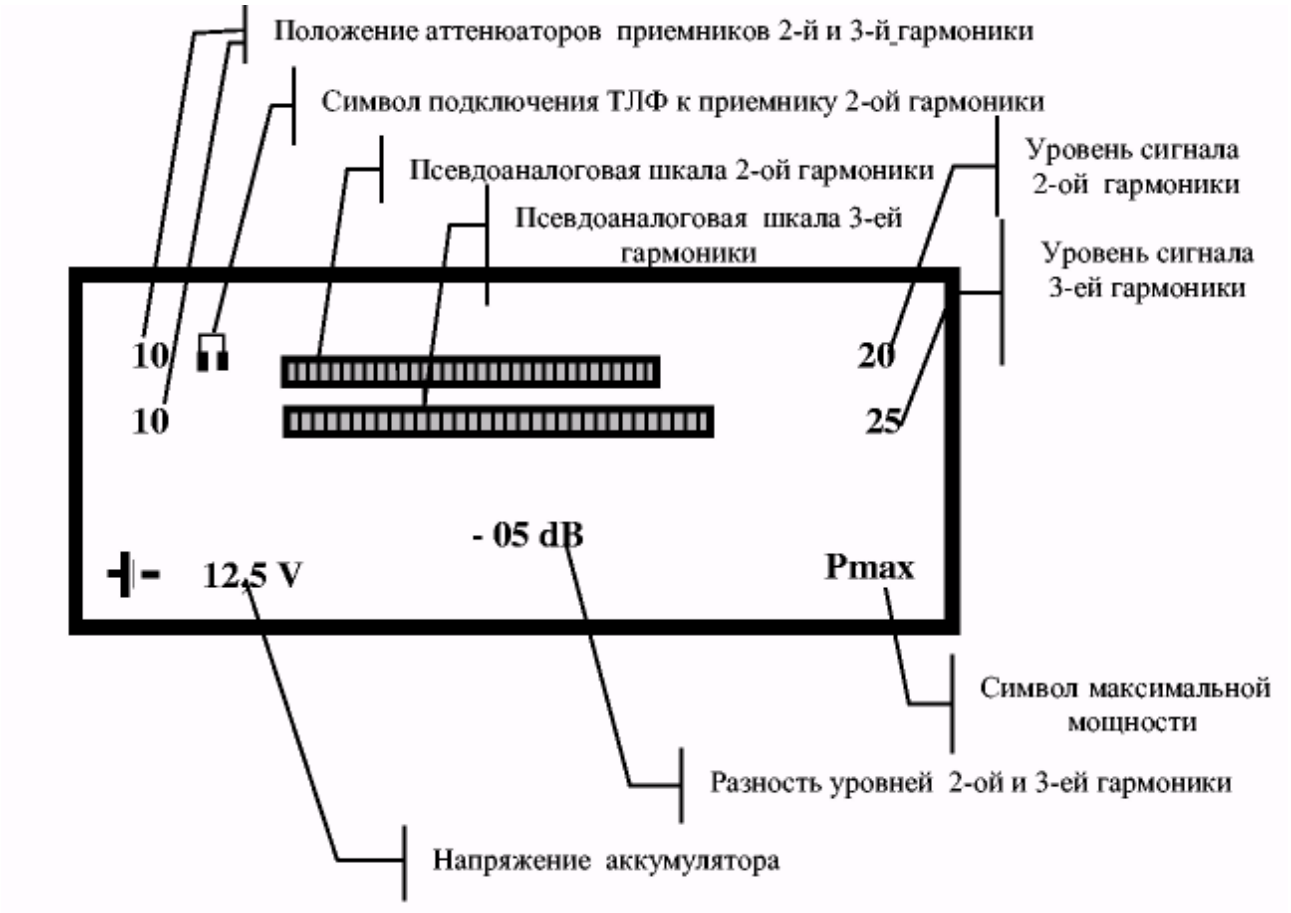
7.3. Press the **ON/OFF** button of the control panel again - the «300» mode should be switched on, the output power of the transmitter is the maximum, the attenuators of the receivers and the headphones are in the position selected in item 7.2.

Note. The third press of the ON/OFF button turns off the product, and the display shows: RADAR TURNED OFF.

When the product is switched off with the ON/OFF button, the «position» of the product controls set by the operator is memorized and restored when it is switched on again. When disconnecting or replacing the battery, the operating modes of the product after switching on are set as described in item 7.2.

The type of information displayed on the display is shown in Pic. 2.

The first and second lines display the attenuation level of the receiver attenuators, the relative signal level of the second and third harmonics in pseudo-analog and digital form and in one of these lines - a sign П, which indicates to which receiver the headphones are connected. Switching the headphones is done with the **OUT 2/3** button, while the icon moves from one line to another. The third line shows the difference between the levels of the second and third harmonics. The sign «-» means that the third harmonic exceeds the second.



Pic. 2. The type of information displayed on the display

In case of receiver overload, the word **«OVER»** appears in this line.

The left part of the fourth line shows the battery voltage, and the right - the relative level of the output power of the transmitter in the form of symbols **Pmax or Pmin.** The power is changed with the **MAX/MIN** button.

If the battery is low below 11.1 V, the fourth line will say: «**CHANGE BATTERY»**, and the headphones - intermittent sound.

Warning. Discharged batteries are not allowed.

7.4. Use a standard imitator to make sure that the product works. To do this, place the imitator in a free place in the absence of near electronic equipment. Set the maximum level of the probing signal using the MAX/MIN button (the display in the right part of the 4th line should show the symbol Pmax) and the maximum sensitivity using the ATT buttons (the display in the left part of the 1st and 2nd line should show the symbols 00). Use the OUT 2/3 button to switch the headphones to the output of the 2nd harmonic receiver. Aim the antenna system towards the imitator from a distance of 0.7-0.8 m. The headphones should listen to a tone with a frequency of 300 Hz medium volume, and the monitor in the 1st and 2nd line should display the signal level of the 2nd received and the 3rd harmonic, respectively, and the level displayed in the right part, must be at least 10-15 and 5-10 dB, respectively, and the level difference displayed in the 3rd line must be at least 5 dB. Removing the imitator from the sounding zone at a constant position of the antenna system should lead to the disappearance of the response signal.

7.5. Search for semiconductor devices, operating depending on the interference situation, if possible, with maximum power and maximum possible sensitivity. To do this, move the antenna system along the surface to be inspected. When a tone of 300 Hz appears in the headphones, it is rough to determine the location of the reflective object. As the antenna system approaches, the tone of the headphones will increase.

7.6. Monitor the ratio of response signals of the 2nd and 3rd harmonics on the display. In the case of a significant excess of the signal level of the 3rd harmonic over the 2nd, it is most likely that the source of the response signal is corrosion nonlinearity. To reliably identify the response, without changing the orientation and location of the antenna system, switch the analyzer to «20K». To do this, press the **300/20K** button.

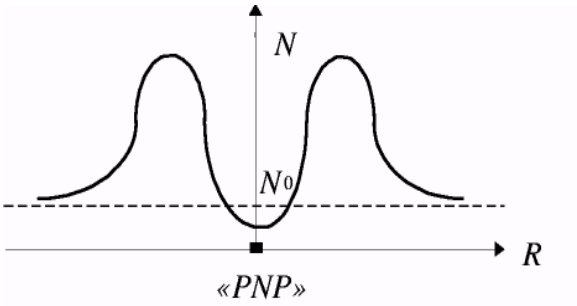
7.7. Set the maximum transmitter power, maximum receiver sensitivity and maximum signal volume in the headphones. Make sure that the modulation signals of the second harmonic of the probing signal are listened to.

7.8. Bring the antenna system as close as possible to the inspected surface at the point of detection of the reflective object. Move the antenna parallel to the examined surface from the detection point to the periphery by 30-40 cm and back, monitor the noise level in the headphones.

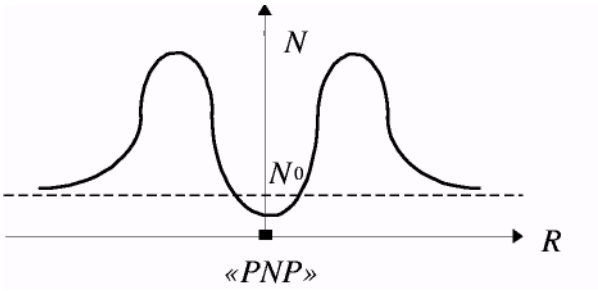
7.9. Depending on the nature of the reflective object - a corrosion diode or an artificial semiconductor element (electronic device), there are two fundamentally different

dependences of the noise level in the headphones on the movement of the antenna system along the examined surface. Their typical appearance is presented in Pic. 3, 4.

7.10. To increase the reliability, it is recommended to listen to the noise response in the headphones of the analyzer in the «20K» mode when tapping the location of the reflective object with any non-metallic object. The corrosion diode is usually characterized by a hoarse irregular crunch.



Pic. 3. Dependence of the level of modulation noise of the 2nd harmonic of the corrosion pn- junction on the distance from the object to the axis of the antenna system of the analyzer.



Pic. 4. Dependence of the level of modulation noise of the 2nd harmonic of the semiconductor pn- junction on the distance from the object to the axis of the antenna system of the analyzer.

In Pic. 3, 4 are marked:
«K» - the location of the corrosion pn- junction;
«PNP» - the location of the semiconductor element;
N - noise level in headphones;
N_0 - the noise level in the headphones in the absence of a nonlinear reflective object;
R - the distance from the location of the reflective object to the axis of the antenna system of the product.

7.11. When switching to the listening mode of the modulation of the 3rd harmonic of the probing signal, the dependences of the noise in the headphones are opposite (the curves shown in Pic. 2 and 3 change places).

7.12. A significant excess of the 2nd harmonic of the probing signal over the 3rd harmonic (20 dB or more) with a high degree of probability indicates the artificial nature of the reflective object.

7.13. After work, turn off the product, disconnect its blocks and fold into a regular layout. Recommended disconnection procedure:

- remove the battery from the power supply compartment of the receiver housing;
- disconnect the control panel connector;
- disconnect the coaxial cables from the antenna system and receiver unit.

8. Safety instructions

8.1. The average power supplied to the antenna of the product in the «300» mode does not exceed 100 mW, in the «20K» mode - 300 mW, which is approximately 4-10 times less than the power of a mobile phone.

8.2. The power flux density of the probing signal of the analyzer in the direction of maximum radiation at a distance of 1 m does not exceed the standards set by DSTU 12.1.006-84 for 8 hours of continuous operation of personnel operating the microwave installation.

However, when using the product should follow the safety rules adopted when working with devices that have open emitters of radio frequency energy:

- do not direct the antenna system towards the eyes at a distance between the antenna unit and a person less than one meter;
- avoid prolonged stay of people in the area of the main petal of the pattern of the antenna system.

Addition 5

METHOD OF SEARCH FOR EMBEDDED DEVICES USING PROTECT 1203 FIELD INDICATOR

Pic. 1. General view of the PROTECT 1203 field indicator

1. Appointment

The electromagnetic field indicator PROTECT 1203 is designed to search and detect BIS devices when they are in active mode and use as a transmission channel electromagnetic radiation. With PROTECT 1203 you can check rooms, cars, various objects, as well as people for the presence of portable transmitters. The search can be performed in stealth mode, which uses a built-in vibrator. The indicator also determines whether the interlocutor has a working mobile phone.

2. General Information

2.1. Before starting the search, it is necessary to extend the antenna, turn on the power and set the required level of sensitivity outside the test area. Then in the room where the inspection is carried out, all rooms are methodically inspected, and the availability of BIS is determined by light indication. If it is not possible to constantly monitor the indicator, you can focus on the built-in vibrator.

2.2. The PROTECT 1203 case is made of a strong duralumin alloy which protects the device from shock damages and the increased humidity, however it is not recommended to store and use the indicator in bad conditions.

2.3. PROTECT 1203 is powered by 2 AAA batteries or accumulators. Alkaline batteries provide continuous operation for 10 hours. After discharging the power supply, you can charge the batteries or replace the batteries.

2.4. Appearance of the device. On the front panel of the device (Pic. 1) there are controls for power on-off, sensitivity level control and a display indicator of the relative level of the radio field. At the bottom of the device is a battery compartment. The retractable antenna on the back of the device is used to receive radio signals. For

normal operation of PROTECT 1203 it is necessary to extend at least the first (widest) segment of the antenna.

Controls and indications.

POWER - the blue LED on the left side of the front panel shows the mode in which the device is (on/off). The button to the right of the LED is used to turn on/off the device.

SENS - sensitivity regulator of the device. The light indication to the left of the regulator is used to display the sensitivity level and the RI level.

3. A guide to conducting search activities

3.1. Preparing for the search

In preparation for the search, it is necessary, in accordance with the plan (Addition 1), to take measures to activate the embedded devices, which are turned on remotely or on the principle of acoustic start. These measures can be:

- organization of a «false» meeting or negotiation;
- reproduction on a tape recorder of the reports recorded at open meeting;
- playing musical compositions, etc.

It is desirable to search during working hours. In addition to the above measures, it is necessary to close all windows and curtains in the room. Include lighting and office supplies to create normal working conditions. Before entering the room being inspected, the appliance must be switched on and the antenna extended to the average length. It is necessary to make sure that the first (widest) segment of the antenna is extended. It is important! You can hide other antenna segments, but the first segment must be extended.

Adjust the sensitivity of the device. To do this, the adjustment knob is rotated until only one segment on the indicator light is lit or flashing. If during the search the operator does not want, or does not have the opportunity to monitor the level of RI with the help of an indicator light, you can set the sensitivity at which all green segments are lit. In this case, when approaching the radiation source, the red segments will flash, and turn on the built-in vibrator.

3.2. Search for ED indoors

1) Enter the room being inspected by holding the PROTECT 1203 upright and observing the light of the indicator light. Turn lights, office supplies and other electrical appliances on and off. Observe changes in the readings of the device. If they change synchronously with the on/off of any accessory, it is a signal of the possible presence in this device of the device of unauthorized removal of information.

2) Go around the whole room, observing the readings of the device. As you approach/remove the radiation source, the displayed radiation level will increase/decrease accordingly.

3) Determine the places with the highest level of radiation by moving the device in various directions and observing the glow of the indicator light.

4) Check all objects that may contain hidden devices for implicit information retrieval. The signal of the detection of such transmitters is again a change in the readings of the indicator light.

5) Try to pinpoint the location of the source of illegal radiation. To do this, reduce the sensitivity of the device to a minimum. If the antenna is not fully extended, the level of the RP displayed on the indicator light will not depend on the relative position of the antenna and the transmitter, and you will observe a constant level of radiation near the transmitter. Sometimes the indicator light may show an increase in the level of RI near wires or metal objects. This is due to the fact that metal objects act as an «extension» of the antenna and such situations do not necessarily signal the presence of a transmitter.

6) After determining the exact location of the radiation source, start a physical search. Make a visual inspection and check with PROTECT 1203 all objects that are in the «danger» zone. Disassemble, if possible, lighting fixtures, telephones, power outlets, telephone sockets, and the like. Examine telephone lines and 220 V lines very carefully. Browse all books, table contents, and the like.

7) If the operator has found the device of removal of the information - do not stop the further search! You should continue your search as carefully as possible, as there is no guarantee that you have been eavesdropped on by a single transmitter. Professionals often «put» 2 listening devices - one is quite easy to identify, and the other is well disguised, with remote control, with non-standard modulation and the like.

3.3. Checking telephone lines

Telephone ED can be installed on any segment of the telephone line. It can be installed in a telephone, telephone socket, switch box or on a telephone cable. Most telephone EDs are activated only when the handset is picked up, so the test is performed when the handset is picked up.

Start the test from the telephone. Place the PROTECT 1203 antenna near the unit and lift the handset. Observe changes in the level of the radio field. If you check the radiotelephone, then, naturally, you will find a strong increase in the level of the radio field when removing the handset from the base, due to the fact that the handset and the base are connected by radio. But it doesn't make much sense to check the cordless phone. The cordless phone itself is a great radio transmitter.

Move the device antenna along the telephone line with the handset raised. Check all sockets and switch boxes. If you have an assistant, ask him to pick up and hang up several times. If you notice that the level of the radio field changes synchronously with the raising/lowering of the handset, it is a signal of the presence of a bug on the line.

Try to determine the area of the line with the maximum level of radiation and conduct a thorough physical search.

3.4. Checking people

There are a large number of transmitters that are built into the clothes, personal belongings of the visitor and the like. These devices can broadcast conversations or (and) video information. To check, you need to adjust the sensitivity so that all the green segments of the indicator light up. To mask the test, hide the PROTECT 1203 in your pocket or under clothing by first extending the first (widest) antenna segment and turning on the power of the unit. Get closer to the person being tested. The activation of the vibrator signals the presence of a radio transmitting device.

Another method of verification is the location of the PROTECT 1203 under the table with the antenna extended as close as possible to the interlocutor. Observe the indicator light changes as the suspect sits down at the table or gets up from the table.

4. Detection range

The range of detection of illegal devices of information collection depends on two important factors:

1. The output power of the embedded device.

2. Radio conditions in the room - the level of radiation from TV, radio stations and legal means of communication.

The level displayed on the PROTECT-1203 indicator light increases as you approach the radio source. Increasing the level can cause not only an illegal device, but also safe TV or radio signals.

The localization of the location of the illegal transmitter is reduced to finding the area where the maximum level of radiation is observed. Direct detection of ED is carried out by physical search of embedded devices.

Addition 6

OPTION OF THE ACT OF COMPLEX SPECIAL INSPECTION OF PREMISES

Ex. №_

Total_ex.

ACT

comprehensive special inspection of the premises

on the availability of means of implicit removal of information

under the contract № ___ from _____ 20__

We, the undersigned, the representative of the Customer, represented by the General Director (name of the enterprise, surname, initials) _____, on the one hand, and the representative of the Contractor, represented by the General Director LLC "Agency _____" _____, on the other hand, have drawn up this Act that the work under the contract № ___ from _____ 20__ is performed in full and meet the requirements of the contract.

1. In the period from _____ to _____ at the enterprise (name of the enterprise) a comprehensive special inspection of the premises in which confidential information circulates, for the presence of embedded devices and other means of implicit removal of information. The works were performed on the basis of the SSSCIP License № _____ dated _____ 20___ issued by Agency _____ LLC.

2. The composition of the search team:

1) _____ - General Director;
2) _____;
3) _____.

3. The following premises were inspected:

1) Office of the head of the enterprise.

2) Premises of accounting.

4. During the inspection the following works were carried out:

1) Visual inspection of protective structures, furniture and other interior items (labor costs - __ man-hours).

2) Checking the elements of building structures, furniture and other interior items using special search equipment (__ man-hours).

3) Checking the lines and equipment of the power and lighting network (__ man-hours).

4) Checking the lines and equipment of the subscriber telephone network (__ man-hours).

5) Check of lines and the equipment of the fire and security alarm system (__ man hours).

6) Checking the radio for the presence of signals of radio emitting means of implicit recording of information (radio monitoring of the premises) (__ man-hours).

7) Audit of unauthorized transmissions of information in the range of infrared radiation (__ man-hours).

8) Search for embedded devices that use low-frequency magnetic radiation (__ man-hours).

9) Search for passive embedded devices (__ man-hours).

10) Examination of the premises for the presence of acoustic and vibroacoustic channels of information leakage (__ man-hours).

11) Physical search of embedded devices and other means of RCI (__ man-hours).

5. During the inspection the following search and research equipment was used:

1) Search software and hardware complex SHC DigiScan, consisting of a Toshiba laptop (head №__) with special software DigiScan 2000 scanning receiver AR - 3000A (head №__).

2) Multifunctional search device ST 031 «Piranha» (head №__).

3) Nonlinear locator NR900EM (head №__).

4) Portable frequency meter RFM - 32 (head №__).

5) Electromagnetic field indicator PROTECT - 1203 (head №__).

6. Audit results:

1) In the office of the head the eavesdropping device with transfer of the intercepted acoustic information on wires of a power electric network is found. The device at the time of inspection is operational, made in the form of a splitter tee and connected to an electrical outlet near the desktop of the head of the enterprise. The radius of acoustic information recording is about six meters; the transmission range of the intercepted information is to the power transformer located in the electric power booth located outside the protected territory.

The most probable places of removal of the transferred information: electric sockets in a reception, a corridor, utility rooms and a toilet room, an electric power board on a landing, an electric power box outside the enterprise.

Probable installation time - (date), during the repair of the cabinet.

The detected eavesdropping device is neutralized by acoustic isolation of the microphone and left at the detection site.

No other means of implicit removal of information were found in the manager's office.

2) Means of implicit removal of information were not found in the accounting office.

3) The office of the head of the enterprise is insufficiently protected from leakage of protected information through technical channels:

- possible leakage of acoustic information through the channel of natural ventilation of the room;

- possible leakage of acoustic information through the vibroacoustic channel formed by the steam heating main;

- unauthorized removal of information from the computer monitor by intercepting its incidental electromagnetic radiation is possible.

The accounting office is not protected from leakage of protected information through technical channels:

- possible leakage of acoustic information through a thin door and plasterboard part of the partition with the reception room;

- possible leakage of acoustic information through the channel of natural ventilation of the room;

- possible leakage of acoustic information through the vibroacoustic channel formed by the steam heating main;

- there is a possibility of remote, without connection of additional devices interception of telephone conversations conducted from the PANASONIC radiotelephone;

- unauthorized removal of information from computer monitors and other office equipment by intercepting spurious electromagnetic radiation is possible;

- possible leakage of information taken visually or with the use of photo and video equipment, through an unclosed window and a glazed part of the front door.

The inspected premises are not protected from unauthorized recording of confidential conversations on a dictaphone, recording by hidden video cameras and possible leakage of information due to leads in the wired lines laid parallel to the wires of the telephone network. The premises have many places convenient for the installation of radio microphones or quick installation of other types of implicit recording of information.

7. Recommendations for improving the security of the inspected premises and preventing the leakage of information through the identified technical channels of its leakage are set out in a separate document.

8. The contract price is _____ (_____) UAH, including 20% VAT ____ (_____) UAH.

Mutual settlements are made in full. The parties have no claims against each other.

Work submitted:	**The work was accepted by:**
General Director of LLC	General Director
« Agency_____»	_____
_____ _____	_____ _____
«____» _____ 20 __.	«____» _____ 20 __.

Addition 7

OPTION OF RECOMMENDATIONS

TO INCREASE SECURITY

TESTED PREMISES AND FACILITIES

Ex. №_

Total_ex.

RECOMMENDATIONS

to increase security

of inspected premises _____

1. The list of potential technical channels of information leakage (TCIL) found in the inspected premises:

1. Office of the head of the enterprise:

1) acoustic air TCIL through the natural ventilation channel of the room;

2) acoustic vibrating TCIL through the natural ventilation channel of the room;

3) acoustic vibrating TCIL through the main (pipeline) of steam heating of the room;

4) electromagnetic TCIL due to the interception of the SEMI computer monitor;

5) electric TCIL due to the removal of leads from the wire lines of fire and burglar alarms, laid parallel to the wires of the telephone line.

2. Accounting premises:

1) acoustic air TCIL through the natural ventilation channel of the room;

2) acoustic air TCIL through the front door of the room;

3) acoustic air TCIL through a plasterboard partition with a reception room;

4) acoustic vibrating TCIL through the natural ventilation channel of the room;

5) acoustic vibrating TCIL through a plasterboard partition with a reception room;

6) acoustic vibrating TCIL through the main (pipeline) of steam heating of the room;

7) electromagnetic TCIL due to the interception of SEMI computer monitors and other office equipment;

8) electric TCIL by removing the leads from the wire lines of fire and burglar alarms, laid parallel to the wires of the telephone line;

9) possible leakage of information due to direct interception of PANASONIC radiotelephone signals;

10) possible leakage of information taken visually or with the use of photo and video equipment, through an unclosed window and a glazed part of the front door.

Both rooms are not protected from unauthorized recording on a dictaphone, recording with hidden video cameras and dropping radio microphones. Schemes of identified potential TCIL with brief explanations - in the appendix to the document.

2. Assessment of the probability of the enemy's use of potential TCIL and the security of the premises:

1. Office of the head of the enterprise:

Due to the good audibility and legibility of speech signals and the availability of visits to neighboring premises, the probability of using acoustic air and acoustic vibration potential TCIL can be considered high.

The use of acoustic vibrating TCIL through the main (pipeline) of steam heating, due to poor signal legibility can be considered plausible.

The use of electromagnetic TCIL by intercepting a computer's SEMI monitor and electric TCIL by interfering with wire lines can be considered unlikely but possible.

Due to the lack of special means of protection of information from leakage in the office of identified potential TCIL, as well as the high probability of enemy use of acoustic air and acoustic vibration potential TCIL, the office of the head of the enterprise should be considered unprotected from leakage of protected information through technical channels.

2. Accounting premises:

(the following is an assessment of the likelihood of using potential TCILs and an assessment of the security of the premises from implicit removal of information).

3. Recommendations on measures and ways to prevent the removal of information on identified potential TCIL and increase the security of the premises:

1. Office of the head of the enterprise:

1) To protect the room from the leakage of acoustic information through the natural ventilation channel of the room, it is recommended to make noise in the channel by creating acoustic and vibrating interference with an acoustic noise generator. The most effective protection system is the complex of vibroacoustic protection BARON. A partial, cheaper alternative to the complex can be considered an acoustic noise

generator ANG - 2000. The same tools will protect the room from leakage of acoustic information through the main (pipeline) of steam heating and protective structures protecting the cabinet.

2) To protect the room from information leakage due to the interception of the SEMI of the computer monitor, it is recommended to electromagnetic noise of the room using a noise generator GRIM-ZI-4. The use of this generator will also create obstacles to the means of unauthorized removal of information from the mains, which will prevent leakage of information in the event of re-use by the enemy eavesdropping device, similar to that found during the inspection. As an alternative to the noise generator GRIM-ZI-4 on electromagnetic noise of the room the noise generator GRIM-3 or GSh-K-1000 can be considered.

3) To prevent leakage of information by removing calls from the wire lines of fire and burglar alarms, it is recommended to relocate the telephone line to eliminate its joint parallel mileage with the lines of fire and burglar alarms. An alternative to the relocation of the telephone line is the installation of fire-suppression filters FP-7 in the lines of fire and security alarm.

4) To protect the premises from unauthorized audio recording, it is recommended to use a suppressor of electronic devices of implicit audio recording STORM.

5) For timely detection of unauthorized video recording, it is recommended to install the Iris VSF - 2000 hidden video camera indicator in the office.

2. Accounting premises:

To protect the premises from leakage of acoustic information ...

(further recommendations are given to numbers and ways to prevent the removal of information on the identified TCIL and increase the security of the accounting office).

4. Summary list of technical means and information protection systems recommended to increase the security of premises.

To protect the above premises, the use of the following equipment and accessories is recommended (Table 1).

Recommended equipment and protection systems

Table 1

Rooms	№ p/p	Recommended tools	Alternative means	Appointments	The required amount
Office of the head of the enterprise	1	Vibroacoustic protection complex DNG-2300	Acoustic noise generator ANG - 2000	Protection of premises from leakage of acoustic information through natural ventilation channels, the heating pipeline protecting building designs	1
	2	Protective device BASALT - 5GESH		SEMI protection	2
	3	Confidential negotiation device dictaphone suppressor DRUID D-06		Protection of premises from unauthorized recording on a dictaphone	1
	4	Device for finding hidden camcorders WEGAi		Timely detection of unauthorized video recording indoors	1
Premises of accounting	6	The following is a list of technical means and information security systems recommended to increase the security of the accounting office			
	7				
	8				
	9				
	10				
	11				
Security service premises	12	Delta X 100/4 search engine for eavesdropping devices	Spectrum analyzer OSCOR Green (OGR-24)	Equipment of a radio control point for constant radio monitoring of office premises	1
	13	Multi-channel digital tape recorder		Ensuring public authorized control of the acoustics of office premises and restrictions imposed by management on the use of communication channels	1
	14				

5. Suggestions for the practical use of recommended means and systems of information protection:

1. The complex of vibroacoustic protection is capable to provide simultaneous protection of all checked rooms.

In the office of the head of the enterprise it is expedient to install one device for monitoring the effectiveness of vibration interference and six vibrating generators such as: one in each ventilation duct, one on the window glass, steam heating pipe, ceiling beam and floor slab between the second and third floors.

It is advisable to install four vibration generators and one device for monitoring the effectiveness of vibration interference in the accounting room. Recommended installation locations are shown in the diagram (Appendix №.)

It is recommended to install the main unit (generator) of the vibroacoustic protection complex and devices for remote activation of vibration generators in the premises of the security service.

It is recommended to turn on the interference signal in the protected premises from the premises of the security service during confidential negotiations. It is expedient to control the effectiveness of interference on the alarm signal given by the devices installed in the protected premises.

2. Noise generators are recommended to be installed one in each protected room.

Inclusion of electromagnetic noise of the room in the office of the head of the enterprise it is expedient to carry out for the time of work with the personal computer, in the bookkeeping room - with the beginning of the working day.

Activation of the mode of linear noise of the power supply network is recommended with the beginning of the working day, exclusion - after its termination.

The mode of protection of the telephone line by the noise generator in the office of the head of the enterprise is not recommended in connection with the use for this purpose of a more effective protection device PROCROST-2000.

3. Installation of FP-7 interference suppression filters in the line of fire and security alarm of the protected premises is recommended to be carried out according to schemes of appendix №.

4. It is recommended to turn on the suppressor of electronic devices of implicit audio recording by means of the remote control during meetings and confidential negotiations.

5. (hereinafter, there are proposals for the practical use of information security tools and systems recommended to increase the security of the premises).

<u>Additions</u> *(not included):*

1. Schemes identified by the results of the inspection of potential technical channels of information leakage.

2. Schemes of installation of the recommended means of information protection systems.

Agreed
The head of the organization
conducting the inspection
_____/_____/

"_____"_____20__.

Head of the search team

_____/_____/

Members of the search team
_____/_____/
_____/_____/
"_____"_____20__.

Addition 8

LIST OF REGULATORY AND LEGAL DOCUMENTS

on the basis of which the activity is carried out

on the provision of services with TPI

the language of the original

1. Закон України "Про інформацію". https://zakon.rada.gov.ua/laws/main/2657-12
2. Закон України "Про доступ до публічної інформації".
3. Закон України "Про захист інформаційно- телекомунікаційних системах". https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80
4. За Закон України "Про основні засади забезпечення кібербезпеки України" https://zakon.rada.gov.ua/laws/main/2163-19
5. Закон України "Про електронні документи та електронний документообіг". https://zakon.rada.gov.ua/laws/show/851-15
6. Постанова Кабінету Міністрів України "Про затвердження Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах" від 29.03.2006 № 373. https://zakon.rada.gov.ua/laws/main/373-2006-%D0%BF
7. Постанова Кабінету Міністрів України "Про затвердження Порядку підключення до глобальних мереж передачі даних" від 12.04.2002 р. № 522.
8. Постанова Кабінету Міністрів України "Про затвердження переліку обов'язкових етапів робіт під час проектування, впровадження та експлуатації систем і засобів автоматизованої обробки та передачі даних" від 04.02.1998 № 121. https://zakon.rada.gov.ua/laws/main/121-98-%D0%BF
9. Постанова Кабінету Міністрів України "Про затвердження Загальних вимог до кіберзахисту об'єктів критичної інфраструктури" від 19.06.2010 № 518.
10. Постанова Кабінету Міністрів України "Про затвердження Типової інструкції про порядок ведення обліку, зберігання, використання і знищення документів та інших матеріальних носіїв інформації, що містять службову інформацію" від 19 жовтня 2016 р. № 736.
11. ДСТУ 33960-96. Захист інформації. Технічний захист інформації. Основні положення. http://www.dsszzi.gov.ua/dsszzi/control/uk/publish/article?artid=38911&cat_id=38836
12. ДСТУ 33961-96 Захист інформації. Технічний захист інформації. Порядок проведення робіт. http://www.dsszzi.gov.ua/dsszzi/control/uk/publish/article?artid=38911&cat_id=38836
13. НД 1.6-005-2013 Захист інформації на об'єктах інформаційної діяльності. Положення про категоріювання об'єктів, де циркулює інформація з

обмеженим доступом, що не становить державної таємниці. https://zakon.rada.gov.ua/rada/show/v0215519-13

14. НД ТЗІ 1.1-002-99. Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу. http://195.78.68.84/dsszzi/control/uk/publish/article?showHidden-1&art id-302408&cat_id=89734&ctime=1547122731920

15. НД ТЗІ 1.1-003-99. Термінологія в області захисту інформації в комп'ютерних системах від несанкціонованого доступу. http://www.dsszzi.gov.ua/dsszzi/control/uk/publish/article?showHidden=1&art_id=89740&cat id=89734&ctime=1547204009788

16. НД ТЗІ 3.6-003-2016 Порядок проведення робіт зі створення та атестації комплексів технічного захисту інформації.

17. НД ТЗІ 1.4-001-00. Типове положення про службу захисту інформації в автоматизованій системі. http://www.dut.edu.ua/uploads/I 1023 75718671.pdf

18. НД ТЗІ 1.6-003-04 Створення комплексів технічного захисту інформації на об'єктах інформаційної діяльності. Правила розроблення, побудови, викладення та оформлення моделі загроз для інформації.

19. НД ТЗІ 2.5-004-99 Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу. http://dstszi.kmu.gov.ua/dstszi/doccatalog/document?id=106342

20. НД ТЗІ 2.5-005-99 Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу (зі зміною № 1). http://dstszi.kmu.gov.ua/dstszi/control/uk/publishvarticle?showHidden=1&art_id=101870&cat id=89734&ctime=1344501089407

21. НД ТЗІ 2.5-008-02 Вимоги із захисту конфіденційної інформації від несанкціонованого доступу під час оброблення в автоматизованих системах класу "2". http://dstszi.kmu.gov.ua/dstszi/doccatalog/document?id=106343

22. НД ТЗІ 2.5-010-03 Вимоги до захисту інформації WEB-сторінки від несанкціонованого доступу. http://dstszi.kmu.gov.ua/dstszi/doccatalog/document?id=106344

23. НД ТЗІ 2.7-011-12 Захист інформації на об'єктах інформаційної діяльності. Методичні вказівки з розробки Методики виявлення закладних пристроїв. http://www.dsszzi.gov.ua/dsszzi/doccatalog/document%3Fid=103253

24. НД ТЗІ 3.7-001-99. Методичні вказівки щодо розробки технічного завдання на створення комплексної системи захисту інформації в АС. http://www.dsszzi.gov.ua/control/uk/publish/article?art_id-46075

25. НД ТЗІ 3.7-003-05. Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі http://www.dsszzi.gov.ua/control/uk/publish/article?art_id=46074

26. НД ТЗІ Р-001-2000 Засоби активного захисту мовної інформації з акустичними та віброакустичним джерелами випромінювання. Класифікація та

загальні технічні вимоги. Рекомендації.
http://dstszi.kmu.gov.ua/dstszi/control/uk/publish/article?showHidden=l&art_id=101924&cat_id=89734&ctime=1344501363205

27. Тимчасові рекомендації з технічного захисту інформації від витоку каналами побічних електромагнітних випромінювань і наводок. (ТР ТЗІ ПЕМВН-95).
http://www.dsszzi.gov.ua/dsszzi/control/uk/publish/article?showHidden=1&art_id=101798&cat_id-89734&ctime=1344500065981

28. Тимчасові рекомендації з технічного захисту інформації у засобах обчислювальної техніки, автоматизованих системах і мережах від витоку каналами побічних електромагнітних випромінювань і наводок (ТР ЕОТ-95).
http://www.dsszzi.gov.ua/dsszzi/control/uk/publish/article?showHidden=1&art id=120206&cat id=89769&ctime=1421836194327

29. ДСТУ ISO/IEC 27001: 2015 Методи захисту. Системи управління інформаційною безпекою. Вимоги (ISO/IEC 27001: 2013, IDT).

30. ДСТУ ISO/IEC 27002: 2015 Інформаційні технології. Методи захисту. Звід практик щодо заходів інформаційної безпеки (ISO/IEC 27003: 2013, IDT).

31. ДСТУ ISO/IEC 27005: 2019 Інформаційні технології. Методи захисту. Управління ризиками інформаційної безпеки (ISO/IEC 27005: 2018, IDT).

32. Указ Президента України "Про Положення про технічний захист інформації в Україні" від 27.09.1999 № 1229.