Methods for Protection against Dangerous Electromagnetic Emissions

The problem of studying linear and other electric circuits of the cryptographic equipment is called forth by available principle possibility to restore keys or non-ciphered (clear) information as a result of intercept of its microtrace generated at the time of processing the above mentioned information in the components of the equipment. The subject of special examination also includes electromagnetic fields, channel circuits and outcoming wiring of the equipment in which researchers can find trace of key and clear information caused by the functioning of the internal components of the cryptographic equipment.

For example, let's consider the output signal of the electronic cryptographic equipment – sequence of pulses representing abstract zeros and ones. In any electronic equipment such pulses are to comply with some standards so that they can be identified by the other parts of the system. In cryptography there are some additional requirements: pulses representing identical values must be identical as much as possible.

Cryptographic equipment, like any other devices, is typical of electromagnetic emission caused by short pulses use. As any emission of a cryptographic device can be intercepted by adversaries and analyzed for obtaining useful information, there must be provided a protection against such attack, for example, by way of shielding units and blocks of the equipment. The first stage of shielding is intended to divide strictly the device into "red" (restricted) zone within which there is a plain text, and "black" (unrestricted) zone, within which there is only a ciphertext. The device must be designed so that all traffic lines between "red" and "black" zones be protected to provide passage of only designated information via them.

The adversary can organize an active attack, directing emission of high energy at a communication terminal and monitoring the reaction, expecting to obtain any information on its internal state.

The general attitude to estimating an extent of cryptographic equipment protection consists in selecting (on the basis of the analysis of proposed circuit designs) sources of dangerous signals, discovering, by experimental methods, among them the most informative ones and measuring the levels of dangerous signals from the selected sources through the leakage paths. Then a degree of informativeness is determined by calculating the signal-to-noise ratio at the output of the receiver under the conditions of operating masking noise and comparing the obtained data with the accepted values.

Basic Notions and Definitions

Dangerous Signals

A signal is considered as dangerous if processing it can result in developing effective algorithms of decryption (for example, ones reducing the key strength or restoring codes of special software) or restoring the information transmitted without identifying the key itself (sometimes even without knowing the algorithm of the equipment operation).

The following is of interest of the ill-minded person:

- encryption (decryption) key;
- signals of intermediate information being individual for each key;
- key of digital signature creation;
- signals of clear information.

Leakage Paths

The term "leakage paths" imply possible circuits and environments though which dangerous signals due to electromagnetic emissions, back and forth transfer or pickups can leave the controlled zone which prevents any uncontrolled presence (appearance) of persons and

vehicles having no permanent or time-limited pass. The subject of the examination is output channel circuits of transmission and reception as well as outcoming wires (electric circuits leaving the controlled zone) and space surrounding the equipment:

Dangerous signals can be spread in the following way:

- via wires of power supply, grounding, input/output in so called additive form – depending on the state and functioning of all the components of the cryptographic equipment during its operation;
- through modulation of output signals, synchronizing clock signals and supply voltage.

The characteristics of sources of dangerous signals and channels of their spread can be experimentally estimated.

Informativeness of Dangerous Signals

Informativeness of dangerous signals in the leakage paths under examination is estimated by calculation method in the form of signal-to-noise ratio, taking into account the model of the interception receiver, level of masking noise and category of the facility of ciphered communication link which is supposed to use samples of cryptographic equipment under examination.

Sources of Dangerous Signals

A source of a dangerous signal implies an element or unit of the cryptographic equipment generating, transforming and transmitting a dangerous signal.

Analysis of Schematic and Design Realization of Cryptographic Equipment

The analysis of schematic and design realization of the equipment is intended to discover sources of dangerous signals and possible paths of their spread. In the course of this analysis analysts examine schemes and designs used in the samples of cryptographic equipment being under examination and capable of influencing the general or local power supply, generating spurious output signals and modulation of output and input signals. For example, such influence can be caused by mutual arrangement of components on printed-circuit boards, their thermal mode, length of printed connectors, absence of intermediate buffer elements, which can result in excessive or irregular load on individual signal circuits (bus-bars).

Methods and Means of Signal Protection

The information can be protected by passive and active methods.

The passive methods of information protection are intended:

- to reduce unwanted electromagnetic emissions at the boundary of the controlled zone to the level denying possibility to single out from them any dangerous signals by reconnaissance means against the natural noise background;
- to reduce pickups of unwanted electromagnetic emissions in outside wires and connecting lines leaving the controlled zone to the level denying the possibility to single out dangerous signals from them by reconnaissance means against the natural noise background;
- to prevent (reduce) leakage of information signals into power supply lines leaving the controlled zone to the level providing no possibility to single out dangerous signals from them by reconnaissance means against the natural noise background;

The active methods of information protection are intended:

- to establish additional masking spatial electromagnetic interference (noise) for reducing the noise-to-signal ratio at the boundary of the controlled zone to the level denying the possibility to single out from them any dangerous information signals by reconnaissance means;

- to establish masking electromagnetic interference with outside conductors and connecting lines for reducing the noise-to-signal ratio at the boundary of the controlled zone to the level providing no possibility to single out from them any dangerous information signals by reconnaissance means;

Unwanted electromagnetic emissions and their pickups in outside conductors are reduced by shielding and grounding cryptographic equipment and devices as well as their connecting lines.

Leakage of information signals into power supply lines is prevented (reduced) by filtering of information signals.

For establishing masking electromagnetic noise there are used systems for making spatial and line noise.

The protection method can be divided into the following basic groups:

- algorithmic;
- design-technological;
- schematic.

Algorithmic Methods of Protection

For preventing any leakage of microtrace of the key and clear information into the channel circuits or outcoming wires the modern cryptographic equipment uses special cryptographic algorithms reducing informativeness of unwanted signals.

The algorithmic methods of protection are based on introducing uncertainty when performing cryptographic transformations. Conditionally the algorithms for reducing informativeness of unwanted signals can be divided into two classes:

- algorithms reducing the content of information in signals when calculating operational keys;
- algorithms reducing informativeness of signals in the process of cryptographic transformations.

Protection can be provided by introducing redundancy into the algorithm of transformation which consists in calculating, during every cycle of the encryption device operation, a set of operations of the same type from which only a part corresponds to the transformation of the crypto-algorithm. Provided that the adversary does not know cryptographic algorithms of encryption and algorithmic protection, he will observe only a set of operations of the same type and not be able to determine their attribution.

The algorithmic methods of protection are very promising because in some cases they make it possible obstaing from using expensive passive and active methods of protection (or significantly simplify them) without prejudice to the information security.

Technical Measures, Design-Technological and Schematic Methods of Protection

Technical measures for protecting information provide use of special technical means as well as realization of engineering solutions. Technical measures are intended to close information leakage paths by reducing the level of information signals or reducing the signal-to-noise ratio in the locations of possible placement of portative means of reconnaissance or their sensors to the level ensuring impossibility to single out information signals by reconnaissance means, and are performed, using passive and active protection means.

The design-technological methods of protection used in the promising cryptographic equipment consist in realization of modularity principle, that is complete function units of the equipment are placed in separate shielded sections. The devices processing information of different classified ranks and placed in separate shielded sections are recommended to be fed from independent secondary power sources. As a version it is permitted to supply power from one secondary power source with using independent rectifiers which are not galvanicly

interconnected. For mounting purposes, multilayer printed circuit boards with layer - separation of signals of different categories of classification and buffer shielding between the layers are used. The communication between the sections is provided through in-line filters. Special secure connectors are used for some types of such equipment.

Information can be exchanged between individual units by non-contact methods with the use of optoelectronic isolators or planar transformers. This increases the impermeability (as to penetration of spurious pickups and modulations) of the interconnected sections.

Technical Complexes and Systems of Information Protection Efficiency Control

The efficiency of encryption means and electromagnetic emission protection methods is estimated by experimental measuring of unwanted signals with use of various measuring devices and complexes which include scanning receivers, various types of digital analyzers of spectrum, selective microvoltmeters and radiotesters.

One of the most effective and convenient devices for making special tests is the complex "Issledovatel" (Researcher) designed for measuring automatically spurious electromagnetic emissions of the technical means under test, registering, storing, processing and documenting the obtained results. This device is an automatic software-hardware testing complex of a new generation.

The software-hardware complex "Issledovatel" can provide:

- discovering spurious electromagnetic emissions of the equipment being tested and standardize the list of spurious electromagnetic emissions discovered with registering frequency, level of spurious electromagnetic emissions, pass band and antenna used the emission discovery;
- checking the list of discovered spurious electromagnetic emissions with test on or off on the equipment under examination;
- displaying spectrum of the found signals on the computer monitor;
- performing manual verification of the list of discovered spurious electromagnetic emissions, using scope mode of the analyzer for monitoring the demodulated test signal with listening simultaneously to the text at the audio frequencies range via built-in speakers;
- processing the obtained results and calculate zones of access to spurious electromagnetic emissions and coefficient of the facility protection.

The special software of the complex "Issledovatel" does not require any special skills of operating PC otherwise than general procedures of using the operational system Windows. The analysis of spectrum and oscillograms of discovered signals in manual mode does not also require from operator any knowledge of designation of and procedures of using controls located on the front panel of the analyzer because all controls are manipulated through the software, using the mouse and entering data from the PC keyboard.

The basic modes include:

- setting up operation modes (setting the range of frequencies to be measured in accordance with electric and magnetic constituents of the field, list and characteristics of antennas used and pass band of the spectrum analyzer);
- registering background and electromagnetic environment;
- searching for spurious electromagnetic emissions signals by way of comparing with the background the newly measured spectrum in the given frequency range with test on-position on the equipment under examination;
- automatic verification for removing the signals not being a part of spurious electromagnetic emissions from the list of discovered signals;
- manual verification (this mode is used for observing spectrum characteristics and oscillograms of signals on PC, listening to them through the analyzer speakers to correct manually the list of spurious electromagnetic emissions);

- preparing data of and calculating zones of access to spurious electromagnetic emissions and coefficients of the facility protection;
- formating and printing measurements protocol.

The application of the complex permits to make up-to-date examination of all unwanted emissions from the cryptographic equipment which can carry dangerous signals and estimate the efficiency of the protection means used in the equipment.

List of Standard Complex Components

- Analyzer of spectrum HP ESA-L1500A or HP 8591E (HP 8593E, HP 8594E, HP 8595E HP 8596E) with built-in options and additional accessories:
- Built-in interface HPIB (standard IEEE-488.2);
- PC: desktop, not worse than PII-333/64/3,2 Gb/SVGA 8 Mb, or Notebook type, not worse than P233MMX/32/3,2 Gb/AM 12,1″/24x CD-ROM/SB16(*).
- Interface card of standard IEEE-488.2 to be mounted in computer (types AT-GPIB, PCI-GPIB, PCMCIA- GPIB of National Instruments Company or similar – at option of customer);
- Printer[1].
- Set of measuring antennas AI4-2 and AIR2-2/2 or similar at customers option[2].
- Antenna communicator[3].
- Package of application software.
- Documents:
  - technical description;
  - log book;
  - metrological certificate of compliance;
  - certificate of supplied measuring antennas;
  - certificate issued by Gostechkomissiya of the President of the Russian Federation

Characteristics	HP ESA-L1500A	HP8591E	HP 8594E	HP 8595E	HP 8596E	HP 8593E
Range of operational frequencies	9kHz …1.5 GHz	9kHz … 1.8 GHz	9kHz … 2.9 GHz	9kHz … 6.5 GHz	9kHz … 12.8 GHz	9kHz … 26.5 GHz
Accuracy of frequency determination	+/- 210 Hz	+/- 210 Hz	+/- 210 Hz	+/- 210 Hz	+/- 1.2 kHz	+/- 1.2 kHz
Frequency resolution	1kHz…3 MHz	30 Hz… 3 MHz	30 Hz… 3 MHz	30 Hz… 3 MHz	30 Hz… 3 MHz	30 Hz… 3 MHz
Noise average	-120 dBm	-130 dBm	-127 dBm	-127 dBm	-127 dBm	-129 dBm
Frequency deviation	+/-1.0 dB	+/-1.0 dB	+/-1.0 dB	+/-1.5 dB	+/-2.0 dB	+/-2.0 dB
Amplitude range	from –120 dBm to +30 dBm	from –130 dBm to +30 dBm	from –127 dBm to +30 dBm	from –127 dBm to +30 dBm	from –129 dBm to +30 dBm	from –129 dBm to +30 dBm
Dimensions, mm	373x222x409	325x163x427	325x163x427	325x163x427	325x163x427	325x163x427
Weight, kg	12.3	14.5	16.4	16.4	16.4	16.4

[1] The complete standard complex does not include it, supplied at option of customer.
[2] The concrete configuration is specified by the customer when making the order.
[3] The concrete configuration of the complete complex is specified by the customer when making the order.