# Methods and techniques of protecting information from leakage by technical channels via side electromagnetic radiation

**Pavlo Sydorkin *[1 A]; Sergey Nesterenko [2 A]; Sergey Salnyk [3 A]; Mykola Konotopets [4 A]; Oleg Kulynich [5 A]; Oleksandr Smolkov [6 B]**

*Corresponding author: [1] Senior Instructor, e-mail: pallsid@ukr.net, ORCID: 0000-0003-2374-1402
[2] Senior Instructor, e-mail: nesterenko1956@ukr.net, ORCID: 0000-0003-2097-1122
[3] Candidate of Technical Sciences, Deputy head of the special department, e-mail: s.sergey@i.ua, ORCID: 0000-0003-4463-5705
[4] Candidate of Technical Sciences, Associate Professor, Associate Professor of the department, e-mail: egorvetrovsky99@gmail.com, ORCID: 0000-0002-6963-1877
[5] Candidate of Technical Sciences, Associate Professor of the department, e-mail: oleh.nicol@gmail.com, ORCID: 0000-0002-0643-6898
[6] Candidate of Technical Sciences, Senior Instructor of the Department, e-mail: smolkoffs@ukr.net, ORCID: 0000-0001-7351-393X

[A] Institute of Special Communications and Information Protection National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute", Kyiv, Ukraine
[B] National Defence University of Ukraine named after Ivan Cherniakhovskyi, Kyiv, Ukraine

**Received:** July 20, 2021 | Revised: September 10, 2021 | Accepted: September 30, 2021

**DOI:** 10.5281/zenodo.5534847

***Abstract***

The rapid development and constant growth of the use of computer equipment, wireless radio access systems, increasing the functionality of electronic means of personal use require a timely response to threats of information leakage through technical channels.

This state of affairs has exacerbated the problem of identifying technical channels of information leakage arising from technical progress, and with it the need to ensure the required level of efficiency and cost of the process of searching and identifying technical channels of information leakage.

The next important issue is the adequacy of measures to protect information from leakage through technical channels, verification and control of their effectiveness, determining the economic feasibility of the proposed set of measures.

The use of existing means of search and detection of technical channels of information leakage, its further protection are based on the use of both active and passive methods.

The article highlights methods and tools of protecting information from leakage by technical channels via side electromagnetic radiation and guidance during their processing using technical means, when transmitting via radio and optical communication channels, channels of leakage of acoustic (speech) and visual information. Basic steps to protect information from leakage by acoustic, vibroacoustic and optoelectronic channels are defined, which centre around reducing the level of acoustic and vibroacoustic signals, voicing information, to a certain signal-to-interference ratio.

The passive and active measures analysed in the article are aimed at achieving the required signal-to-interference ratio. Passive information protection measures and their focus on improving the sound insulation of enclosing structures of information activity objects are highlighted. Active information protection measures and their impact on reducing the signal-to-interference ratio to normal by creating acoustic and vibroacoustic interference at the border of enclosing structures of information activity objects are analysed.

The conceptual foundations of technical information protection, its basic principles are given, with the principal methods and means of ensuring information security for each of the possible leakage channels defined.

***Key words:*** technical channels of information leakage, information protection systems, indirect electromagnetic radiation and guidance, bugging devices, shielding.

## Introduction

The rapid growth of information, caused by scientific and technological progress, requires institutions and organizations of all forms of ownership to have the appropriate technical means and systems designed to receive, transmit, process and store information. The physical processes that occur in such devices during their operation contribute to the emergence and propagation in the environment of electromagnetic, acoustic and other radiation.

One of the main threats to information security is the leakage of information through technical channels, which is understood as the uncontrolled propagation of an informative signal from its source through the physical environment to a technical device that receives information (Yarochkin, 1994; Xorev, 1998; Lastivka & Shpatar, 2018; Xorev, 2010; Karpov & Lepeshkin, 2018). Information interception is the illegal receipt of information using a technical means that detects, receives and processes informative signals. As a result of interception, illegal familiarization with the information or illegal recording of information on the media may occur. Features of technical channels of information leakage are determined by the physical nature of information signals and the characteristics of the distribution environment. Therefore, measures to protect the information circulating in the technical means, aimed primarily at reducing the levels of such radiation (Yarutich, 2019; Xorev, 2008; Khoroshko, Cherednychenko & Shelest, 2008; Buzov, Kalinin & Kondrat`ev, 2005; Zajcev, Shelupanov, & Meshheryakov, 2009).

## Material and methods

Analysis of research by both domestic and foreign researchers (Yarutich, 2019; Xorev, 2010; Karpov & Lepeshkin, 2018; Infowatch, 2020; Macy Bayern, 2019) showed that the protection of information with limited access is given very much attention. At the same time, the results of the analysis reflected a steady trend of increasing cases of leakage of information with limited access (Infowatch, 2020, 2021) and the emergence of new channels of its leakage (Infowatch, 2020;2021; Macy Bayern, 2019]. The constant growth of the use of electronic means, the further development of radio frequency resources, the development of intelligence tools and methods of their use require constant monitoring of the security of information and the objects on which it circulates (Karpov & Lepeshkin, 2018; Infowatch, 2020, 2021; Macy Bayern, 2019). That, in turn, requires timely analysis and consideration of possible threats in the overall system of protection of information and the objects on which it circulates.

Purpose of the article is systematization of technical channels of information leakage through side electromagnetic radiation and methods of their protection against unauthorized influence.

## Results and discussion

The general classification of technical information leakage channels contains the following types(Fig.1) (Yarochkin, 1994; Xorev, 1998):

- leakage channels processed by technical means of receiving, processing, storing and transmitting information by technical means of transmitting information (hereinafter referred to as TMTI);
- technical channels of speech information leakage (hereinafter referred to as TCSIL);
- channels of information leakage during its transmission by communication channels;
- technical channels of visual information leakage.

During the operation of TMTI, the following technical channels of information leakage are created:

1. Electromagnetic channels:

- side electromagnetic radiation and guidance (SEMRG) of the TMTI;
- electromagnetic radiation at the operating frequencies of HF generators of the TMTI;
- radiation at the self-excitation frequencies of low-frequency amplifiers (LFA) of TMTI;
- radiation at the operating frequencies of high-frequency (HF) TMTI generators and auxiliary technical means and systems (ATMS).

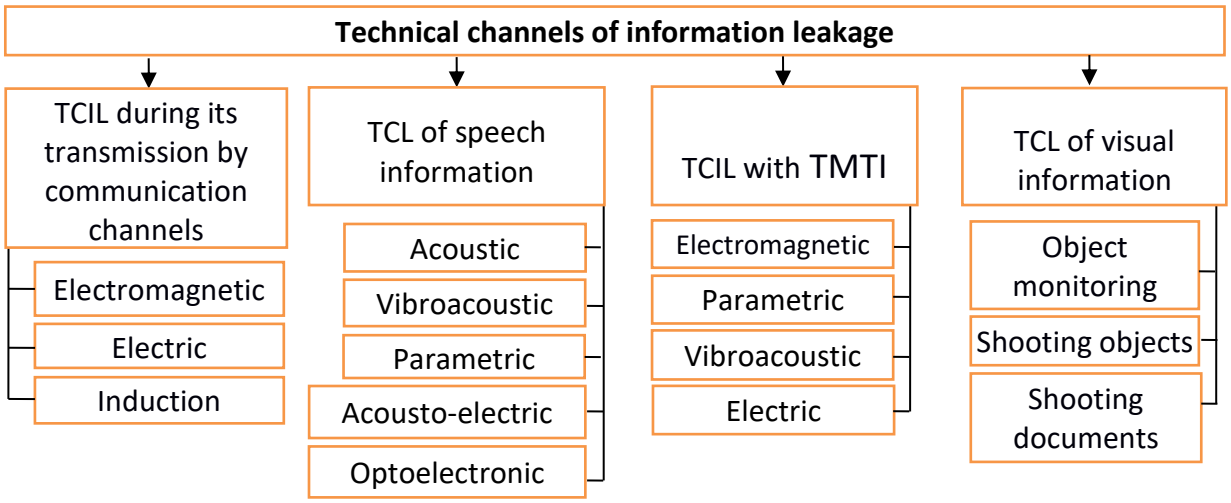


Figure1 – General classification of technical channels of information leakage

2. Electric channels:
- guidance of electromagnetic radiation of TMTI elements on foreign conductors;
- leakage of information signals in the power supply line;
- leakage of information signals in the ground circuit;
- shooting information using bugging devices (BD).

3. Parametric channels – interception of information by high-frequency irradiation of TMTI.

These technical channels are potential sources of information interception using bugging devices.

**Bugging devices**

Bugging devices, according to the type of intercepted information, can be divided into (Lastivka & Shpatar, 2018; Yarutich, 2019; Karpov & Lepeshkin, 2018):
- instrument bugs for intercepting images displayed on the monitor screen;
- instrument bugs for intercepting information output from the computer keyboard;
- instrument bugs for intercepting information output to peripherals (for example, a printer);
- instrument bugs for intercepting information saved on the computer hard drive.

Information that is intercepted using bugging devices is either directly transmitted by a radio channel, or recorded on a transitory medium, and then transmitted on command to the interception checkpoint.

**Technical channels of information leakage when it transmitted by radio communication channels**

For the purpose of transmitting information, the following communication channels are mainly used: short-wave, ultra-short-wave, radio relay, tropospheric and space communication channels; various types of telephone radio communication (for example, cellular communication), as well as cable and fiber-optic communication lines. Which under certain conditions (in the absence of cryptographic protection tools) create natural and accessible for the offender information leakage channels.

**Methods and means of searching for bugging electronic devices for intercepting information**

Search and detection of bugging devices can be carried out visually, as well as using special equipment: detectors of voice recorders and video cameras, field indicators, radio frequency meters and interceptors, scanner receivers and spectrum analyzers, software and hardware

control systems, nonlinear locators, X-ray systems, conventional testers, as well as special equipment for checking conducting lines (Lastivka & Shpatar, 2018; Xorev, 2008; Buzov, Kalinin & Kondrat`ev, 2005; Zajcev, Shelupanov, & Meshheryakov, 2009).

The method of searching for bugging devices is largely determined by the use of particular monitoring equipment.

The main methods of searching for bugging devices include:

- special examination of allocated premises;
- search for radio bugs using field indicators, radio frequency meters, and interceptors;
- application of scanner receivers and spectrum analyzers, software and hardware monitoring systems;
- search for portable sound recording devices using voice recorder detectors for the presence of their indirect electromagnetic radiation, magnetization generators and electric motors;
- search for portable video recording devices using video camera detectors;
- search for bugs using non-linear locators;
- search for bugs using X-ray systems;
- verification using HF probes of power supply lines, radio broadcasting and telephone communication;
- measurement of parameters of power supply lines, and telephone communication lines;
- conducting a test “ringing out” of all telephone sets installed in the checked room, while monitoring the passage of all PBX call signals.

The simplest and cheapest means of detecting radio emissions from bugging devices are electromagnetic field indicators, which signal the presence of an electromagnetic field with a voltage higher than the threshold (background) at the antenna location point with a light or sound signal.

To detect the radiation of bugging devices in a closer area, special devices called interceptors can also be used. The interceptor automatically adjusts to the frequency of the most powerful signal and detects it. The sensitivity of field detection devices is low, so they allow to detect the radiation of radio bugs in close proximity to them. Special radios with automated scanning of the radio band (scanners) have significantly better sensitivity. They provide search in the frequency range from tens of kHz to units of GHz. Spectrum analyzers have the best capabilities for searching radio bugs. In addition to intercepting the radiation of bugging devices, they also allow to analyze their characteristics, which is important when detecting radio bugs that use complex types of signals to transmit information. A large group is created by means of detecting or localizing bugging devices based on the physical properties of elements of an electrical circuit or structure – semiconductor devices, and electrically conductive metal parts of the structure. Of these tools, the most reliable results are provided by nonlinear radars that receive the 2nd and 3rd harmonics of the reflected signal due to the nonlinearity of the semiconductors' characteristics.

Metal detectors respond to the presence of electrically conductive materials in the search area, primarily metals, and allow to detect cases or other metal elements of the bug.

Portable X-ray systems are used to show through objects whose purpose cannot be detected without disassembly, primarily when disassembly is impossible without destroying the found object.

Depending on the type of communication, technical channels intercepting information can be divided into electromagnetic, electrical, and induction ones.

1. Electromagnetic channels are electromagnetic radiation from communication transmitters modulated by an information signal (wiretapping of radiotelephones, cell phones, radio relay communication lines).

2. Electric channels are created when connected to communication lines – to the cable (wired) communication lines. The electric channel is most often used to intercept telephone conversations (telephone radio bugs). The contact method is mainly used for obtaining information from coaxial and low-frequency communication cables.

3. Induction channel, where the effect of the appearance of an electromagnetic field around a high-frequency cable during the passage of information signals is used. Induction sensors

are mainly used to intercept information from symmetrical high-frequency cables. This channel is widely used for wiretapping to telephone conversations conducted over radiotelephones, radio relay and satellite communication lines, cellular communication systems and channels based on Bluetooth technologies.

Effective interception of information in a fiber-optic communication line (hereinafter referred to as FOCL) is possible by direct physical connection to a fiber-optic line. Information losses can also be caused by the processes that occur when radiation is introduced (removed) to the optical waveguide and wave propagation in the dielectric waveguide, optical radiation from permanent and split connections of optical fibers, as well as bending and damage to these fibers.

The main causes of radiation of light energy of FOCL at the junctions of optical fibers are:

- displacement of fiber joints (axial unconnected);
- the presence of a gap between the ends of the joined fibers;
- non-parallel end surfaces of the joined fibers;
- angular mismatch of the joined fibers' axes;
- difference in the diameters of the joined fibers.

FOCL can cause acoustic information leakage, when the geometric dimensions change or the ends of the connected light guides in the detachable device shift relative to each other as a result of the influence of an external acoustic field on a fiber-optic cable. As a result, an amplitude modulation of the information signal of radiation passing through the fiber occur.

**Technical channels of speech information leakage**

1. Direct acoustic channels (propagation medium is environment). To intercept them, miniature highly sensitive microphones and special directional microphones are used. Speech information intercepted by bugging devices can be transmitted over a radio channel, or an optical channel (in the infrared wavelength range), an AC network, connecting lines of auxiliary technical means, and other conductors (water supply pipes, sewers, metal structures). Recording of acoustic information is possible using cellular communication devices and voice recorders (RD TPI 1.1-001-99; RD TPI 2.5-001-99).

2. Vibroacoustic channels (propagation medium is building structures). Contact microphones (stethoscopes) are used to intercept acoustic vibrations in such an environment. A radio channel is mainly used to transmit information, so such devices are often called radio-stethoscopes. It is possible to transmit information via an optical channel in the near-infrared range of wavelengths, as well as an ultrasonic channel (over metal structures of the building).

3. Acousto-optical (laser) channels (laser beam irradiation of vibrating surfaces). To intercept speech information, this channel uses 'laser microphones' – complex laser acoustic location systems. They operate in the near-infrared range of waves, devices for capturing information from a fiber-optic cable covered with a protective shell (RD TPI 4.7-001-2001; RD TPI P-001-2000).

4. Acousto-electric channels (channels for converting acoustic signals into electric ones). Electronic bugging devices (parallel or serial connection to a communication line) and recording with sound recording devices (voice recorders) are used to capture information (RD TPI 4.7-001-2001; RD TPI P-001-2000).

5. Acousto-electromagnetic channels (conversion of acoustic channels into electromagnetic waves) (RD TPI 4.7-001-2001; RD TPI P-001-2000).

**Channels of visual information leakage**

Depending on the nature of the information, it can be classified according to the following methods of its obtaining:

1. Observation of objects using optical devices (monoculars, optical tubes, binoculars, telescopes, eyepieces with built-in video cameras), television cameras. For long-distance surveillance, aerial and space cinema and photo shooting tools, long-focus optical systems are used, and for close-range surveillance, camouflaged secretly installed television cameras are applied. At the same time, the image from television cameras can be

transmitted to monitors both via cable and by radio signal.

2. Objects' shooting is performed to document the results of observation and study objects in more detail. Television and photo equipment is used to capture objects. Miniature or portable camouflage cameras and video cameras, including aerospace cameras, are used to capture objects during the day at close range.

3. Shooting (making copies) of documents is made using special portable cameras for shooting documents. If necessary, one can also use a regular camera or smartphone, but in order to get high-quality result, the photographer needs to have the appropriate knowledge and skills.

**Protection of information from leakage through technical channels**

Engineering and technical protection of information provides for a set of measures to protect information from unauthorized access through various channels, as well as neutralize special effects – destruction, distortion or blocking of access. The concept of engineering and technical information protection defines the basic principles, methods and means of ensuring information security of objects. It is a general idea and principles of ensuring information security of an object in the face of threats, and it contains an assessment of threats and resources to be protected, an information protection system, principles of its organization and functioning, principles of building an information protection system, and legal framework.

Efficient technical protection of information resources is an integral part of a comprehensive information security system and helps cut the costs of organizing information protection. Information protection is aimed at preventing an attacker from entering information sources for the purpose of destruction, theft or modification, protecting information carriers from destruction as a result of various natural and man-made impacts, and preventing information leakage through various technical channels.

There are the following principles for designing technical information security systems (Yarutich, 2019; Karpov & Lepeshkin, 2018; Regulations on technical information, 1999; Temporary recommendations, 1995)

- continuity of information protection in space and time;
- permanent readiness and high degree of efficiency to eliminate information security threats;
- multi-zone nature and the presence of many boundaries in protection, which determines the placement of information of different values in zones with a controlled level of security;
- selectivity contained in the prevention of threats primarily for the most important information;
- integration (interaction) of various information security systems in order to increase the efficiency of a multicomponent security system, create a centralized security service in integrated systems.

According to their functional purpose, engineering and technical protection equipment is divided into the following groups:

- engineering tools that represent various devices and structures that counteract the physical penetration of intruders into security objects,
- hardware tools (measuring devices and appliances, software and hardware packages) designed to detect information leakage channels, assess their characteristics and protect information;
- software tools, software packages and information security systems in information systems for various purposes and in the main data processing tools;
- cryptographic means, special mathematical and algometric means of protecting computer information transmitted over open data transmission systems and communication networks.

The principles of engineering and technical protection of information include (Yarutich, 2019; Karpov & Lepeshkin, 2018; Regulations on technical information,1999; Temporary recommendations, 1995) reliability of information protection, continuity of protection, secrecy of information protection, expediency of protection, variety of protection methods, comprehensive application of various

methods and means of protection, cost-effectiveness of protection.

**Methods for protecting information from leakage by the SEMRG channel**

The effectiveness of the system for protecting the main and auxiliary technical means from information leakage through technical channels is assessed according to various criteria, which are determined by the physical nature of the information signal, but most often according to the signal-to-noise ratio. Protection of information from leakage through SEMRG is carried out using passive and active methods and tools (Fig. 2). The purpose of passive and active protection methods is to reduce the signal-to-noise ratio at the border of the controlled zone to values that make it impossible for enemy intelligence to allocate a dangerous information signal. In passive protection methods, reducing the signal-to-noise ratio is achieved by reducing the level of the dangerous signal, in active methods it is achieved by increasing the noise level.

Passive methods of information protection are aimed at weakening the indirect electromagnetic radiation of the main technical means and systems (MTMS) at the border of the controlled zone, weakening the interference of side electromagnetic radiation in foreign conductors, connecting lines, power supply and grounding circuits that go beyond the controlled zone, excluding or weakening the leakage of information signals in the power supply and grounding circuits that go beyond the controlled zone.

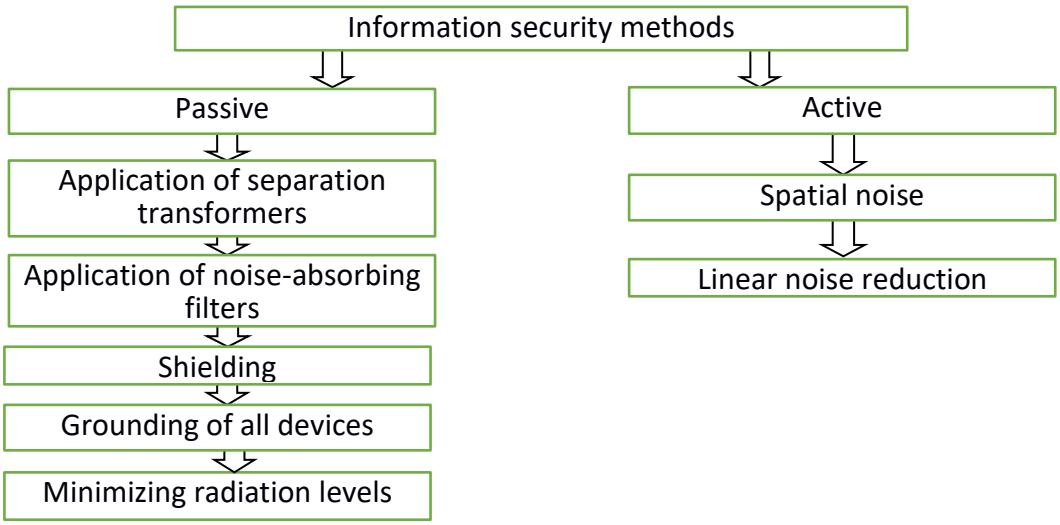


Figure 2 – Classification of information protection methods

The attenuation of a dangerous signal should be adjusted to values that make it impossible to isolate it by means of reconnaissance against the background of natural noise.

Passive protection methods include:

- use of separation transformers and filters that suppress interference;
- shielding;
- grounding of all devices as a necessary condition for effective information protection;
- upgrade of electronic devices in order to reduce the radiation level.

Active methods of information protection are aimed at creating spatial electromagnetic masking interference, creating electromagnetic masking interference in extraneous conductors, connecting lines, power supply and grounding circuits. Active protection methods include spatial and linear noise coverage.

**Shielding of electromagnetic waves**

The theoretical solution of the shielding problem and the determination of field stress indicators are generally extremely difficult. Therefore, depending on the type of problem, electric, magnetic and static, and electromagnetic shielding is analyzed:

- electrostatic shielding – suppression of capacitive parasitic bonds;
- magnetic and static shielding (suppression of inductive parasitic bonds);

- electromagnetic shielding – suppression of the electromagnetic field.

As the signal frequency increases, only electromagnetic shielding is used. Electromagnetic shielding is the most common and frequently used, since in most cases shielding has to deal with either variable or fluctuating, and less often with static fields. Electrostatic shielding is used to reduce the parasitic capacitance between electrical circuits, when a current-conducting shield is introduced, connected to a common wire. The electrostatic shielding aims to close the electrostatic field to the surface of the metal screen and remove electric charges to the ground (device's body) using a ground loop. The use of metal screens is quite effective and allows to completely reduce the influence of the electrostatic field.

Shielding of the room provides full shielding of the TMTI and communication facilities. In ordinary rooms, the shield functions are partially performed by reinforced concrete components of the building walls. Nets, metallized fabric curtains, metallized glass, current-conducting films, windows installed in metal or metallized frames are used to shield windows and doors. Shielding of electromagnetic waves of more than 100 dB can only be provided in special shielded chambers – chambers without reverberation (echoless), designed for testing and high-frequency measurements of radio and electronic equipment, antenna equipment and testing of technical means for electromagnetic compatibility. There are two main types of echoless chambers – half-echoless and fully echoless.

Upgrade of computer equipment devices is carried out by using various radio-absorbing and shielding materials and circuit, and technical solutions. It is possible to significantly reduce the radiation level of computer equipment. The cost of such upgrade depends on the size of the required security zone and ranges from 20-70% of the cost of computer equipment.

**Grounding of technical systems**

When mounting electromagnetic shielding, it is necessary to ground the screen of the SEMRG source, which is understood as an intentional electrical connection of the screen to the grounding device. Moreover, high-quality grounding of devices is one of the most important conditions for protecting information from leakage by ground circuits. Grounding – a device consisting of grounding conductors and conductors that connect grounding conductors to electronic and electrical devices, appliances, etc.

The purpose of grounding is to ensure the flow of parasitic currents into the ground, which are formed on the screens, housing and other connections of the technical means, thereby eliminating the accumulation of potential to dangerous limits. Today, there are different types of grounding devices. The most commonly used ones are: single-point serial grounding circuit; single-point parallel grounding circuit; multi-point grounding circuit and combined (hybrid) circuits.


Figure 3 – Serial single-point grounding circuit

Fig. 3 shows the simplest serial single-point grounding circuit used at low frequencies. However, it has a disadvantage associated with the flow of reverse currents of various circuits over a large section of the grounding circuit. As a result, dangerous signals from third-party circuits may appear.

A single-point parallel circuit (Fig. 4) does not have such drawback. However, such a circuit requires increased quantity of laid ground wires. Due to this, there may be a problem with ensuring a small resistance of the ground sections.

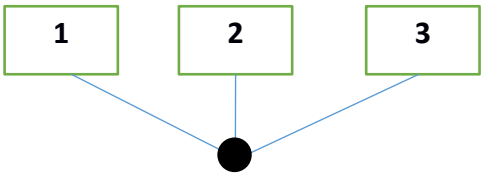


Figure 4 – Single-point parallel ground circuit

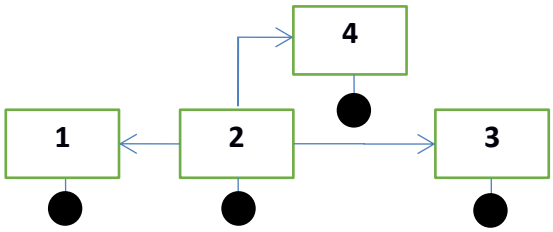


Figure 5 – Multi-point grounding circuit

Multi-point grounding circuit (Fig. 5) does not have the above disadvantages, but it requires measures to eliminate closed circuits. It is used at high frequencies. The key characteristic of grounding is the electrical resistance of the grounding circuit. The lower the resistance, the more efficient the grounding (Rp≤4 Ohms).

**Separation transformers and filters that suppress interference**

Filtration is the main and effective means of suppressing (attenuating) conductive interference (electromagnetic interference propagating through conductors) in power supply circuits, in signal circuits of the interface and on printed circuit boards, and in ground wires. Anti-interference filters reduce conductive interference from both external and internal sources of interference. Separation transformers provide wiring of primary and secondary circuits based on guidance signals. That is, the guidance of the primary winding of the transformer should not fall into the secondary one.

## Conclusions

Findings: the protection of information from leakage by technical channels via side electromagnetic radiation and guidance when processing them using technical means, is an important component of the overall information security system of the state and society, which requires ongoing upgrade of existing methods and means of information protection, with mandatory consideration of the specific aspects of constantly emerging new types and models of information security threats.

## References

Yarochkin, V. I. (1994). *Texnicheskie kanaly` utechki informacii.* Moskva: Institut povy`sheniya kvalifikacii informacionny`x rabotnikov.

Xorev, A. A. (1998). Zashhita informacii ot utechki po texnicheskim kanalam. Moskva: Gostexkomissiya Rossii.

Lastivka, H. I., & Shpatar, P. M. (2018). TEKhNIChNYI ZAKhYST INFORMATsII V INFORMATsIINYKh TA TELEKOMUNIKATsIINYKh SYSTEMAKh. Chernivtsi: Chernivetskyi natsionalnyi universytet. Retrieved from http://radiotech.cv.ua/documents/book/KONSPEKT_KANAL.pdf.

Yarutich, A. O. (2019). Zakhyst informatsii vid vytoku tekhnichnymy kanalamy. Nauka onlain: Mizhnarodnyi elektronnyi naukovyi zhurnal. (1). Retrieved from https://nauka-online.com/ua/publications/natsionalnaya-bezopasnost/2019/1/zahist-informatsiyi-vid-vitoku-tehnichnimi-kanalami

Xorev, A. A. (2008). *Texnicheskaya zashhita informacii.1*, Moskva: NPCz «Analitika».

Khoroshko, V. O., Cherednychenko, V. S., & Shelest, M. Y. (2008). *Osnovy informatsiinoi bezpeky.* Kyiv: DUIKT.

Buzov, G. A., Kalinin, S. V., & Kondrat`ev, A. V. (2005). *Zashhita ot utechki informacii po texnicheskim kanalam.* Moskva: Goryachaya liniya – Telekom.

Zajcev, A. P., Shelupanov, A. A., & Meshheryakov, R. V. (2009). *Texnicheskie sredstva i metody` zashhity` informacii.* Moskva: OOO «Izdatel`stvo Mashinostroenie». Retrieved from

http://window.edu.ru/resource/611/63611/files/tsmzi.pdf.

Xorev, A. A. (2010). Texnicheskie kanaly` utechki informacii, obrabaty`vaemoj sredstvami vy`chislitel`noj texniki. *Special`naya Texnika*. (2). Retrieved from http://www.bnti.ru/showart.asp?aid=954&lvl=04.03.&p=1.

Karpov, A. V., & Lepeshkin, O. M. (2018). MODELIROVANIE TEXNICHESKIX KANALOV UTECHKI INFORMACZII NA RASPREDELENNYX OBEKTAX UPRAVLENIYA. *International Journal of Advanced Studies*, (1), 69-83. Retrieved from https://www.researchgate.net/publication/325322929_MODELIROVANIE_TEHNICESKIH_KANALOV_UTECKI_INFORMACII_NA_RASPREDELENNYH_OBEKTAH_UPRAVLENIA.

Globalnoe issledovanie utechek konfidentsialnoy informatsii v pervom polugodii 2019 goda. Retrieved from https://www.infowatch.ru/sites/default/files/report/analytics/russ/Global_Data_Leaks_Report_2019_half_year.pdf?rel=1

Issledovanie utechek informatsii ogranichennogo dostupa v gossektore. Mir – Rossiya. 2018 god. Retrieved from https://www.infowatch.ru/sites/default/files/analytics/files/%D0%90%D0%BD%D0%B0%D0%BB%D0%B8%D1%82%D0%B8%D1%87%D0%B5%D1%81%D0%BA%D0%B8%D0%B9%20%D0%BE%D1%82%D1%87%D0%B5%D1%82%20%D1%83%D1%82%D0%B5%D1%87%D0%BA%D0%B8%20%D0%B2%20%D0%B3%D0%BE%D1%81%D1%81%D0%B5%D0%BA%D1%82%D0%BE%D1%80%D0%B5.%202018.pdf

Macy Bayern. 5 major data breach predictions for 2019 Retrieved from https://www.techrepublic.com/article/5-major-data-breach-predictions-for-2019/

RD TPI 1.1-001-99 Technical protection of information on software-managed public PBX systems. General provisions. Approved by Order No. 26 of the Department of Special Communication Systems and Information Protection of the Security Service of Ukraine dd. 28.05.99.

RD TPI 2.5-001-99 Technical protection of information on software-managed public PBX systems. Specifications of functional security services. Approved by Order No. 26 of the Department of Special Communication Systems and Information Protection of the Security Service of Ukraine dd. 28.05.99.

RD TPI 4.7-001-2001 Technical protection of speech information in symmetric subscriber analog telephone lines. Means of determining the presence and the distance to the location of contact connection of technical intelligence tools. Guidelines for developing test methods. Approved by Order No. 11 of the Department of Special Communication Systems and Information Protection of the Security Service of Ukraine dd. 06.04.2001.

RD TPI P-001-2000 Means of active protection of speech information with acoustic and vibroacoustic radiation sources. Classification and general technical requirements. Guidance. Approved by Order No.41 of the Department of Special Communication Systems and Information Protection of the Security Service of Ukraine dd. 04.09.2000.

Regulations on technical information protection in Ukraine. Approved by Presidential Decree No. 1229 dd. 27.09.99.

Temporary recommendations for technical protection of information from leakage through channels of indirect electromagnetic radiation and interference. Approved by Order of the Department of Special Communication Systems and Information Protection dd. 09.06.95.