Spectral Characteristics of Intermodulation Emissions during High-Frequency Imposition*

Larysa Kriuchkova[1,*,†], Ivan Tsmokanych[2,†], Nataliia Mazur[1,†] and Ivan Chernihivskyi[1,†]

[1] *Borys Grinchenko Kyiv Metropolitan University, 18/2 Bulvarno-Kudriavska str., 04053 Kyiv, Ukraine*
[2] *State Research Institute of Cyber Security and Information Protection, 6/3 Maksyma Zaliznyaka str., 03142 Kyiv, Ukraine*

Abstract

The processes of forming technical information leakage channels using high-frequency imposition methods are considered. The results of practical studies of the spectral characteristics of intermodulation radiation of electronic equipment interfaces under the influence of high-frequency imposition signals obtained using the Keysight PXA Signal Analyzer N9030B spectrum and signal analyzer using the White periodic antenna SAS-521F-7 are presented. The study was carried out to determine the spectral composition and energy levels of dangerous signals that arise under the influence of high-frequency imposition signals, to solve the problems of ensuring information security at information activity facilities.

Keywords

information interception, high-frequency imposition method, probing signal, dangerous signal, intermodulation radiation, spectral characteristics

1. Introduction

In the context of global informatization of society, the real security of the state largely depends on the security of its information resources and technologies, therefore, the protection of national confidential information is one of the main priorities of the state policy of each country [1, 2].

The threat of information leakage through spurious electromagnetic radiation occupies an important place in the list of threats, as well as due to the introduction of information signals in the power supply lines of information processing equipment, connecting lines of auxiliary equipment and systems, grounding circuits, and external conductors. Foreign literature uses the terms "compromising electromagnetic emanations" or TEMPEST (an abbreviation for "transient electromagnetic pulse emanation standard"—a standard for electromagnetic pulse radiation caused by transient processes in electronic equipment).

The problem of leakage of confidential information through spurious electromagnetic radiation and breakthrough channels has been intensively studied since 1985, after the first open visual demonstration of this method of information interception by the Dutch engineer Wim van Eck [3].

Modern electronics allows you to create miniature and very sensitive receivers. Multi-channel signal reception is used with subsequent correlation processing, which has significantly increased the range of information interception. A dangerous technology, SoftTempest, has been created—a technology for covert data transmission via a channel of spurious electromagnetic radiation using software tools [4].

* *CPITS 2025: Workshop on Cybersecurity Providing in Information and Telecommunication Systems, February 28, 2025, Kyiv, Ukraine*
* Corresponding author.
† These authors contributed equally.
alara54@ukr.net (L. Kriuchkova); ivakobor@ukr.net (I. Tsmokanych); n.mazur@kubg.edu.ua (N. Mazur); i.chernihivskiy@gmail.com (I. Chernihivskyi)
0000-0002-8509-6659 (L. Kriuchkova); 0000-0002-5085-8457 (I. Tsmokanych); 0000-0001-7671-8287 (N.Mazur); 0009-0003-4568-3212 (I. Chernihivskyi)

Research is conducted in two directions:

- Solving problems that arise when intercepting informative signals and extracting confidential information from them (interception problems).
- Solving problems that arise when organizing the protection of confidential information from leakage (protection problems).

Interception of information that is discussed at information activity facilities or processed by technical means can be carried out through special influences on elements of technical means. One of the effective methods of such influence is high-frequency imposition (HFI), in which information leakage channels are formed due to acoustoelectric transformations that occur when confidential signals and a high-frequency probing signal are simultaneously exposed to the elements of technical means unless radical measures have been taken to prevent the penetration of high-frequency currents into the technical means.

The HFI method was invented by Lev Termen in 1943 and implemented in the form of the US Coat of Arms (Fig. 1), which the pioneers presented to US Ambassador Harriman in 1945. Dangerous signals were received by the unique radio receiver “Loss” (Fig. 2).

The existence of this information leakage channel was discovered only in 1952. Western intelligence officers were helped to understand the principle of operation of “Zlatoust” (Fig. 3) by the scientist and chief technical specialist of the British counterintelligence MI-5, Peter Wright. The world officially learned about the possibility of intercepting information using the HFI method in 1960, when the Americans used “Zlatoust” as an argument in the international scandal about the downed American spy plane U-2. Today, “Zlatoust" is stored in the CIA museum in Langley, Virginia.

Figure 1: The bugged Great Seal of the United States “Zlatoust”

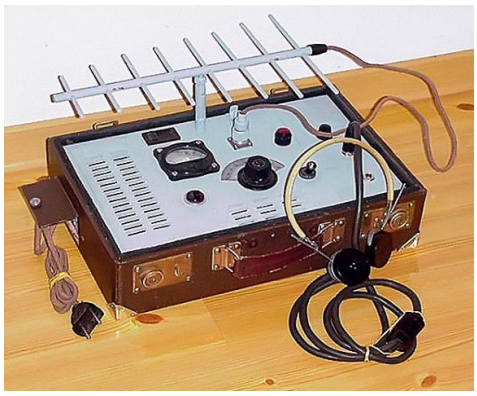

Figure 2: Unique radio receiver “Loss”

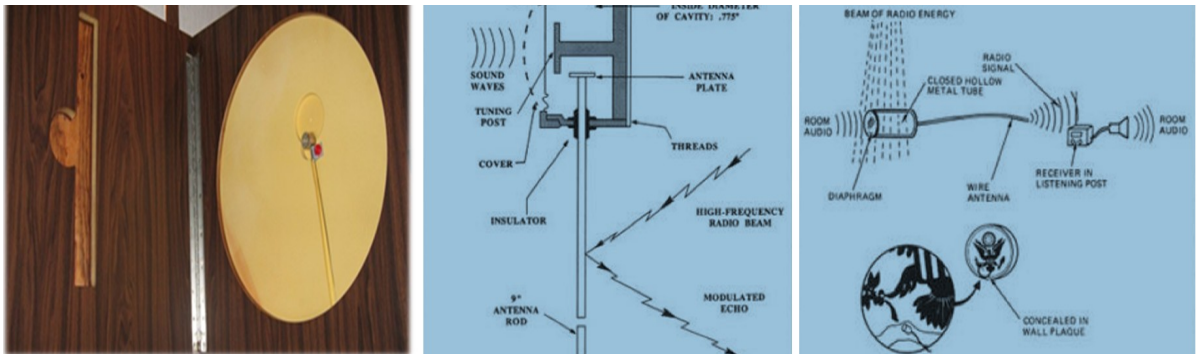

Figure 3: The bugged Great Seal of the United States that hung over the U.S. Ambassador's desk in Moscow contained a passive cavity resonator and went undetected for seven years, from 1945 to 1952. The CIA had no comparable audio technology at the time [5]: a) Interior view of the Great Seal, b) The principle of operation of "Zlatoust", c) The principle of operation of "Zlatoust"

The task of protecting confidential information necessitates the search for frequencies at which leakage channels can be organized, and active monitoring of electronic equipment and data transmission networks for the presence of "suspicious" harmonics in their spectra.

Foreign governments and transnational companies actively monitor technical channels of information transmission. The implementation of such activities led to the introduction of closed standards TEMPEST and HIJACK in the USA. HIJACK refers to the interception of digital signals as a result of processing and transmission, and TEMPEST—electromagnetic signals.

The publication presents the results of research on the spectral characteristics of intermodulation radiation, carried out to determine the spectral composition and energy levels of dangerous signals that arise under the influence of high-frequency jamming signals, to solve the problems of ensuring information security at information activity facilities.

2. The physical essence of the processes of forming information leakage channels using HFI methods

To ensure information protection from leakage through HFI channels, it is important to understand the physical nature of the processes of formation of dangerous signals and radiation.

The high-frequency imposition method is based on the use of the physical phenomenon of reflection of high-frequency energy supplied from a special generator from an unmatched load representing the total resistance of any nonlinear or parametric circuit of basic technical means (BTM) and auxiliary technical means and systems (ATMS), the value of which changes under the influence of a dangerous signal according to the law inherent in this signal [6–8].

The effectiveness of the high-frequency "imposition" method is generally defined as the result of the interaction of the following technical systems:

- Information interception systems.
- Systems for transmitting, processing, and storing information.
- Communication systems (lines).

The a priori results of the interaction of these systems can be assessed by conducting a systems analysis of the functioning of a complex technical system consisting of the three specified components.

When the circuits and elements of the BTM are exposed to probing high-frequency oscillations, the latter in some cases turn out to be modulated by dangerous, comparatively low-frequency signals circulating in these circuits and can be isolated during their subsequent processing in the information interception system. Thus, probing high-frequency oscillations become carriers of information of a dangerous signal and create a channel for possible information leakage.

High-frequency probing signals used in the interception of information by the high-frequency imposition method are received via communication lines to the BTM and then penetrate these devices in the following ways:

- Along chains formed by parasitic electrical and magnetic connections between elements of devices.
- Using electromagnetic radiation from some sections of wires and circuits and the reception of these radiations by other wires and circuits (antenna effect).
- Directly through direct galvanic connection circuits (for example, when connecting a probe oscillation generator to grounding and power supply systems).

The source of the probing signal can be a high-frequency transmitter located outside the controlled area, "disguised" as a transmitter of cellular communication networks, digital and analog television networks, radio relay lines, an FM radio transmitter, etc.

In the simplest case, a harmonic (sinusoidal) oscillation can be used as a probing oscillation. Analytical expression of such oscillations generally has the form:

$$F(t)=A_0\cos(\omega_0 t+\phi_0) \tag{1}$$

where A_0 is the oscillation amplitude; $(\omega_0 t+\phi_0)$ is the oscillation phase.

At constant parameter values, the oscillation determined by the specified ratio does not carry any meaningful information about the state of the object of observation.

If, in accordance with the controlling low-frequency dangerous signal, the parameters of this oscillation will change, then the resulting oscillation can be represented in the form:

$$F(t)=A(t)\times\cos\Phi(t) \tag{2}$$

That is, the probing oscillation in this case will be characterized by two main time-varying quantities: amplitude $A(t)$ and phase angle $\Phi(t)$,

The mathematical expression describing intermodulation radiation when probing with a broadband signal can be represented by the expression:

$$S(t)=U_c\times[1+\alpha(t)]\times g(t-\tau)\times\cos(\omega_0 t+\varphi(t))+U_c\times\mu\times\lambda(t)\times g(t-\tau)\times\cos(\omega_0 t+\varphi(t)+\Phi) \tag{3}$$

where U_c is the average amplitude of the received signal; $\alpha(t)$, $\varphi(t)$ is fluctuations in the amplitude and phase of the signal due to internal noise of the probing oscillation generator; $\lambda(t)$ – normalized ($|\lambda|_{max}$) message to be extracted by the intercepting party; $\mu=\sqrt{M^2+m^2}$ is full amplitude-phase modulation index (M is amplitude modulation index, m is phase modulation); $\Phi=arctg(\frac{m}{M})$ is modulation angle; $g(t)$ is a pseudorandom sequence modulating the probing signal; τ is a delay of the reflected signal relative to the probing signal.

The process consisting of the fact that this or that parameter of the probing oscillation changes in time by the low-frequency signals (dangerous signals) processed in the BTM is a process of unwanted (parasitic) modulation.

Amplitude-modulated oscillation

$$u(t)=U_H\cos\omega_0 t+\frac{m}{2}U_H\cos(\omega_0+\Omega)t+\frac{m}{2}U_H\cos(\omega_0-\Omega)t \tag{4}$$

is a complex oscillation. The first term of the sum is an acting (probing) high-frequency oscillation and, as noted above, does not carry any information about a dangerous signal, while the two-second terms are informative, forming an envelope and representing new frequency components of harmonic nature, the amplitudes of which are defined as $m\cdot U_H/2$. Since all the intercepted

information is contained precisely in these additional members, therefore, to reduce or eliminate information leakage, it is necessary to reduce or eliminate the values m and U_H.

Thus, the essence of high-frequency imposition consists of obtaining modulated high-frequency oscillations (when the modulating signal is an intercepted dangerous signal) under the influence of the original unmodulated high-frequency oscillation on the nodes of technical means (BTM and ATMS).

The additional frequency components that appear at the same time, forming a high-frequency information signal, have frequencies $(\omega_0+\Omega)$ and $(\omega_0-\Omega)$, shifted relative to the probing high-frequency oscillation ω_0 by the value of the modulating frequencies and, therefore, under the condition $\omega \gg 0$, are also recognized as high-frequency.

The phenomenon under consideration is accompanied by the process of linear transfer of the spectrum of a low-frequency signal (speech, telecode, etc.) to the radio frequency range. The linearity of the nature of this process lies in the fact that during its implementation the type and relationship between the components of the spectrum of the primary information signal remain unchanged.

In addition, based on (4), this phenomenon can be considered as the result of the multiplication of two initial oscillatory processes interacting with each other in the electrical circuits of the BTM. The process of such multiplication of two oscillations can be carried out in two ways.

The first method is based on the use of elements with nonlinear conductivity. From the theory of electrical and radio engineering circuits, it is known that if a certain nonlinear element with a volt-ampere characteristic approximated by the expression:

$$i=i_0+\alpha u+\beta u^2+\gamma u^3 \tag{5}$$

if two voltages u_c and u_r are in effect, then the output current of this element will contain many combination components with frequencies

$$\omega_K=(\pm r\,\omega_r \pm q\,\Omega_c) \tag{6}$$

where r and q are positive integers (including noise), and their amplitudes and phases will depend, respectively, on the amplitudes and phases of the applied voltages u_c and u_r. Thus, elements with nonlinear conductivity make it possible to implement the process of multiplying two initial voltages and, along with various combinations of their higher harmonic components, to obtain frequencies equal to the sum and difference of the frequencies of the informational hazardous and auxiliary (probing) voltages.

The second method of multiplication is based on the use of linear circuits with variable parameters (parametric circuits). Thus, if some quadrupole, linear for the probing voltage, has a periodically changing transfer coefficient

$$K(t)=K_0(1+\cos\Omega t) \tag{7}$$

then when applying the oscillation voltage to its input, we get the output of the four-terminal

$$u_{вых.}=K(t)\times u_r \tag{8}$$

and then

$$u_{out}=K_0(1+\cos\Omega t)\times u_{mr}\cos(\omega_r t+\phi\omega) \tag{9}$$

that is, as a result of the multiplying action of this system, it is possible to identify stresses that are similar in their expression (3).

Thus, only as a result of the nonlinear or parametric multiplication of two voltages, on the corresponding selective load it is possible to isolate a signal of the form

$$u = u_m(t)\cos[\omega t + \phi\omega(t)] \tag{10}$$

corresponding to the desired one, the changes in the amplitude u_m or phase φ of which are completely determined by the laws of change in the amplitudes and phases of the input voltages of dangerous signals.

As a result of numerous studies, it has been shown that in the circuits of the BTM and ATMS, in which there are nonlinear elements and microphones (and their like), modulated oscillations arise due to a change in their resistance under the combined effect of a dangerous—informative signal of acoustoelectric transformations, including a high-frequency probing signal. In general, modulating elements of BTM circuits—random modulators—can be divided into two groups:

- Nonlinear and linear active resistances (microphones, diodes, transistors, vacuum tubes).
- Nonlinear and linear reactive resistances (inductances of transformers, chokes, relay windings, bell coils, capacitance of condenser microphones, etc.).

Elements of the 1st group are mainly the cause of AM oscillations in resistive circuits. Elements of the 2nd group are FM oscillations or oscillations of a more complex form (for example, AM and FM).

The occurrence of unintentional modulation in the BTM can occur only under very specific conditions. To assess these conditions, first of all, we will clarify the mechanism of the effect of high-frequency oscillations on circuits containing loads whose conductivity changes according to the law of change of the low-frequency signal Ω. As an example, we will consider the process when changing the parameter of at least one of the elements of the circuit (for example, the resistive resistance in a carbon microphone under the influence of an acoustic field). For the case when $Z = R$ and $Z_m = R_1$ the circuit consists of a voltage source of frequency

ω $e = U_M \cos\omega t$ and two series-connected resistances, constant— R and variable—$R_0 : R + R_1$.

Under the influence of sound vibrations, the membrane vibrates and, by pressing on the carbon powder contained in the microphone, changes its conductivity.

Let us assume that the microphone is strictly linear, and that the conductivity is a linear function of the sound pressure. Then for the conductivity of the variable element we have

$$g = g_0 + kP \tag{11}$$

Let the change in sound pressure

$$P = P_m \cos\Omega t \tag{12}$$

Then for the conductivity of the alternating section of the circuit we can write

$$g(t) = g_0 + kP_m \cos\Omega t = g_0 + g_1 \cos\Omega t \tag{13}$$

Denoting $m = \frac{g_1}{g_0}$ (modulation coefficient for conductivity), we have $g(t) = g_0(1 + m\cos\Omega t)$.

If the expression is valid for the electromotive force e created by an external high-frequency generator in the circuit under consideration:

$$e = E_m \cos\omega_0 t \tag{14}$$

where ω_0 is the frequency of the high-frequency generator, then the current in the circuit will be equal to the product of the electromotive force e and the conductivity of the circuit:

$$i_{out} = eg = E_m g_0(1 + m\cos\Omega t)\cos\omega_0 t \tag{15}$$

We obtain the usual expression for amplitude-modulated oscillation since the product $E_m g_0(1 + m\cos\Omega t)$ can be considered as the amplitude of oscillations $E_m(1 + m\cos\Omega t)$ of

frequency ω_0 , changing with frequency Ω at a constant value of the circuit conductivity, i.e. linear parametric amplitude modulation takes place.

Amplitude modulation can also be implemented in the presence of oscillatory circuits and nonlinear elements in the circuits.

The following can be taken as the main parameters for evaluating the high-frequency imposition method:

- Frequency range of the applied probing signals.
- Level and shape of probing signals.
- Maximum distance at which the method in question can be used.
- Permitted methods of connecting probing equipment to information transmission systems.
- Possibilities of methods for isolating, processing, and recording modulated high-frequency oscillations received from the BTM and ATMS equipment.
- Probability of obtaining secret information from information transmission systems using the high-frequency imposition (probing) method.

3. Experimental research

To conduct experimental studies, the methods given in [9, 10]. The structural diagram of the experimental setup is shown in Fig. 4.

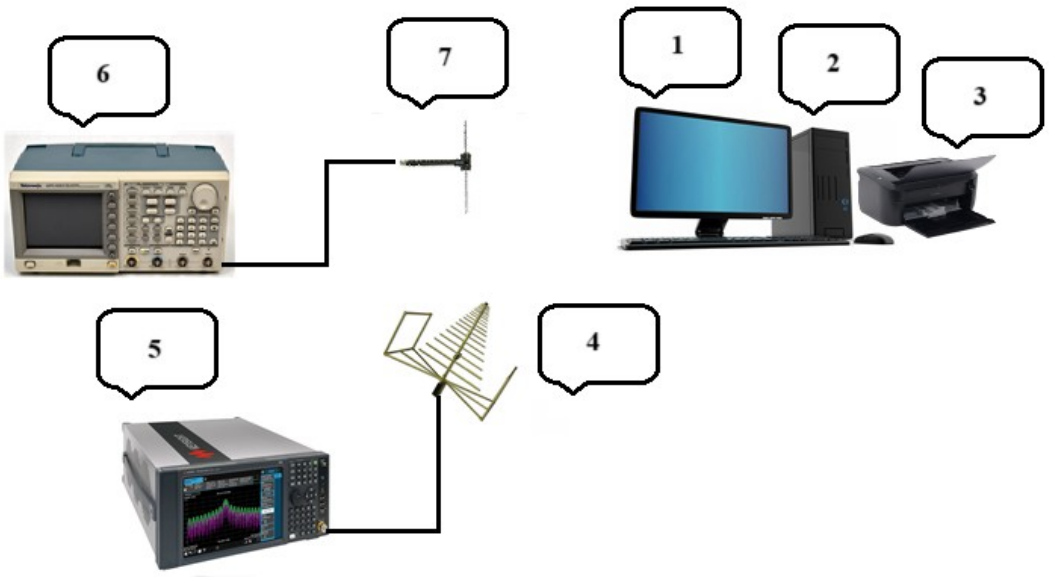

Figure 4: Structural diagram of the experimental setup, where: 1—system unit, 2—monitor, 3—printer, 4—white-periodic measuring antenna, 5—spectrum analyzer, 6—generator, 7—Antenna electric EMA-2000

Experimental studies were conducted using a Keysight PXA Signal Analyzer N9030B spectrum and signal analyzer using a White periodic antenna SAS-521F-7 in a class II shielded room [11].

1. Figs. 5–7 show the spectra of the intermodulation radiation of the monitor interface under the influence of the HF signal of the influence of high-frequency imposition on the interface of the monitor of a personal computer—Acer EB192QBBI. The spectra images clearly show changes in the frequency characteristics of the signal, which indicates the possibility of interception of data transmitted through the video interface.

The image in Fig. 5 demonstrates the monitor signal characteristic, where informative parameters are clearly defined due to the influence of high-frequency imposition. At 74.251 MHz the maximum level is 46.28 dBμV.

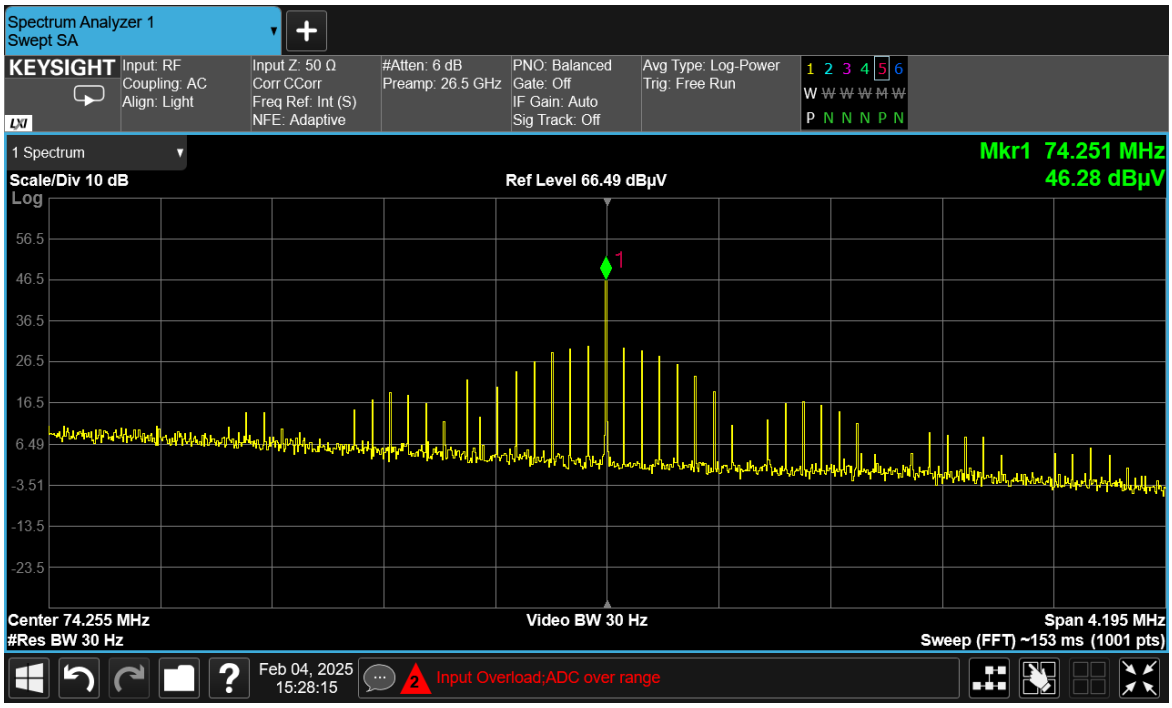

Figure 5: The spectrum of intermodulation radiation of the monitor interface under the influence of the HFI signal at the frequency 74.251 MHz

At 222.752 MHz the maximum level is 25.07 dBµV and side harmonics are visible due to the influence of high-frequency interference on them.

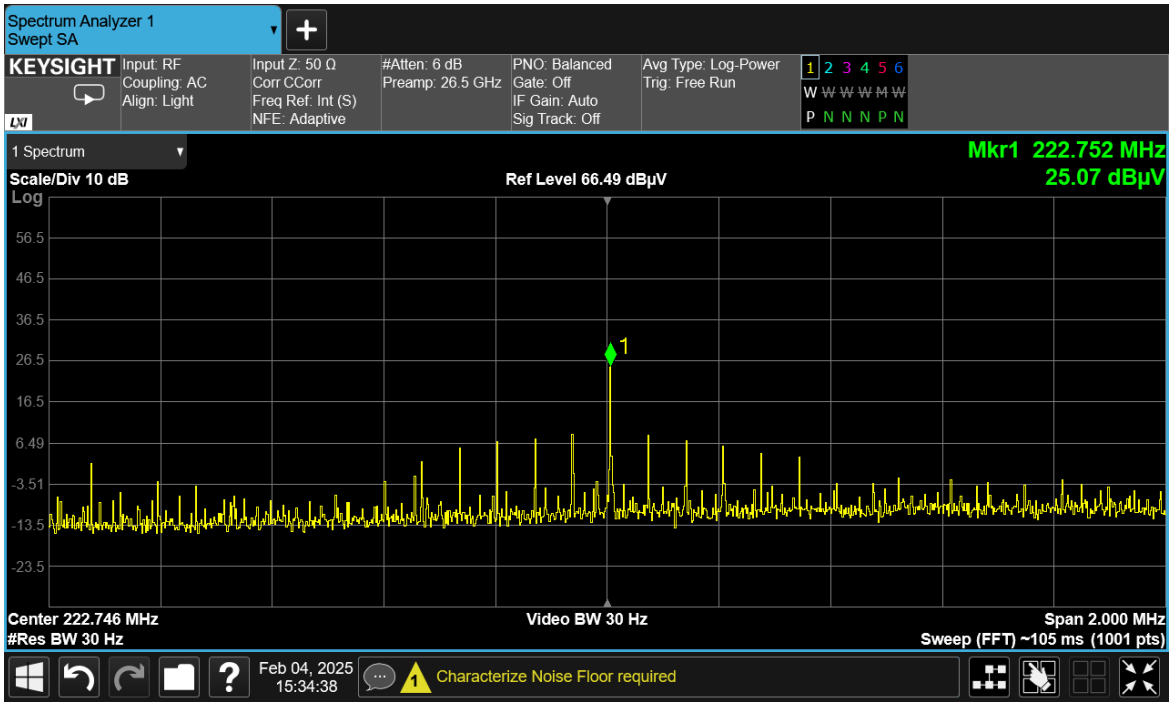

Figure 6: The spectrum of intermodulation radiation of the monitor interface under the influence of the HFI signal at the frequency 222.752 MHz

At a frequency of 371.254 MHz, the maximum level is 16.97 dBμV and side harmonics are visible due to the influence of high-frequency imposition on them.

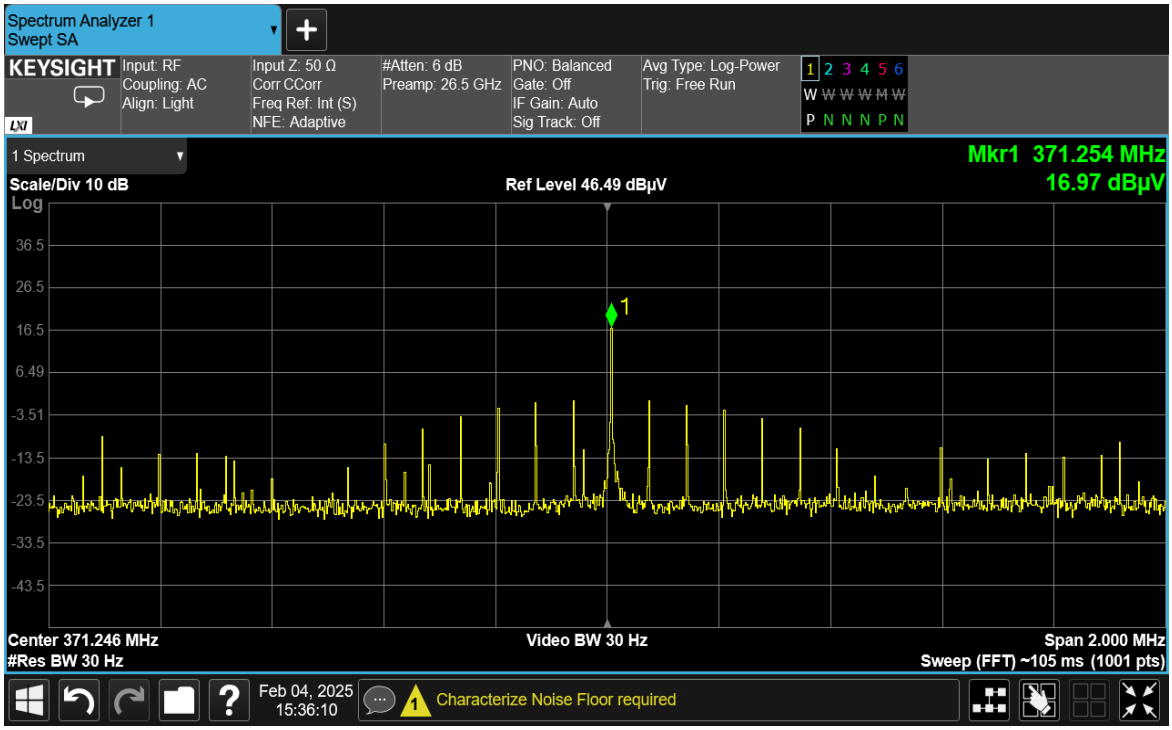

Figure 7: The spectrum of intermodulation radiation of the monitor interface under the influence of the HFI signal at the frequency 371.254 MHz

2. The intermodulation emission spectra shown in Figs. 8–10 demonstrate how HFI can activate spurious emissions in the interface of the flash drive—Apacer USB 3.1 16 GB, facilitating data interception. The emissions resulting from HFI can be used to reproduce information transmitted via the USB interface.

The history of the Universal Serial Bus (USB) interface, which is today the de facto standard for peripheral devices [*n*], dates back to 1994. The basis for the creation of the new technology was the growing need for a convenient interface for connecting peripheral devices, since the COM, LPT and PS/2 interfaces typical of those years had low bandwidth and did not support hot plugging, and their connectors were inconvenient to use due to their large size due to the large number of contacts.

Another advantage of serial USB interfaces over parallel interfaces is that they do not have the skew phenomenon, which significantly reduces the achievable clock speed limit. Skew in parallel interfaces also limits the permissible length of interface cables [12].

Fig. 8 shows the spectrum of intermodulation radiation of the USB interface and shows the activation of harmonics at a frequency of 840.01 MHz with a power of 17.83 dBμV, which creates the basis for intercepting read/write commands.

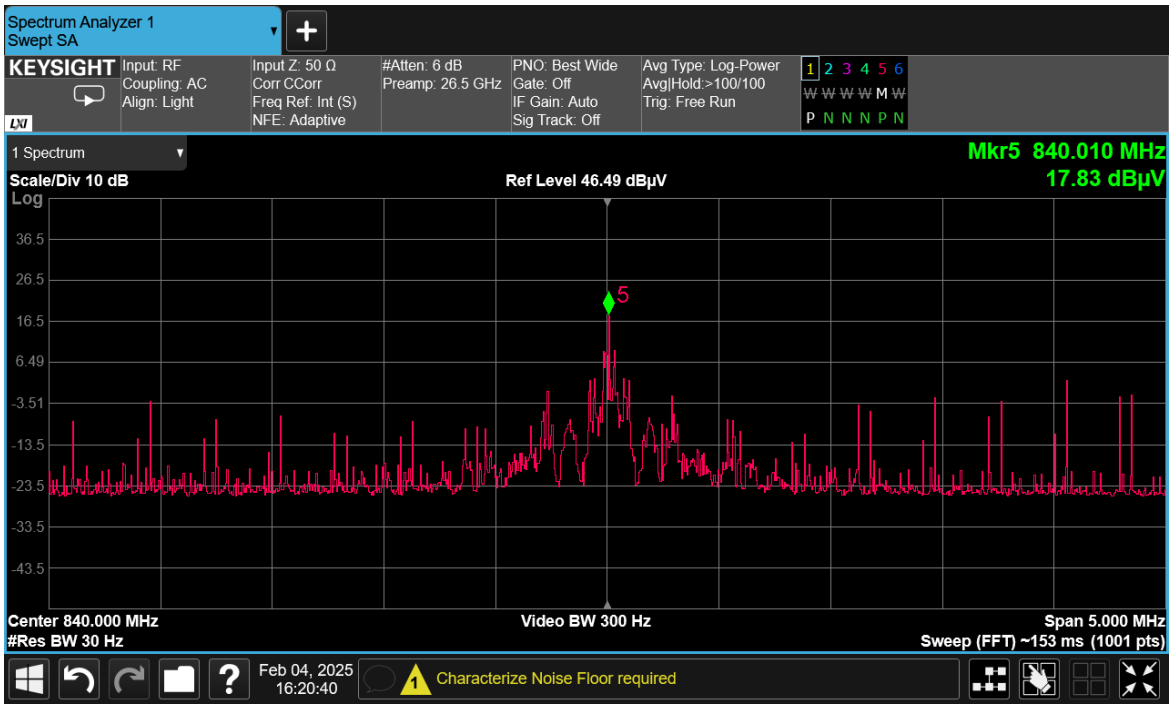

Figure 8: The spectrum of intermodulation radiation of the USB interface under the influence of the HF signal at the frequency 840.01 MHz

Fig. 9 shows the spectrum of intermodulation radiation of the USB interface, namely the increase in activity at a frequency of 600.01 MHz with a power of 24.43 dBµV, which allows partial identification of transmitted data packets.

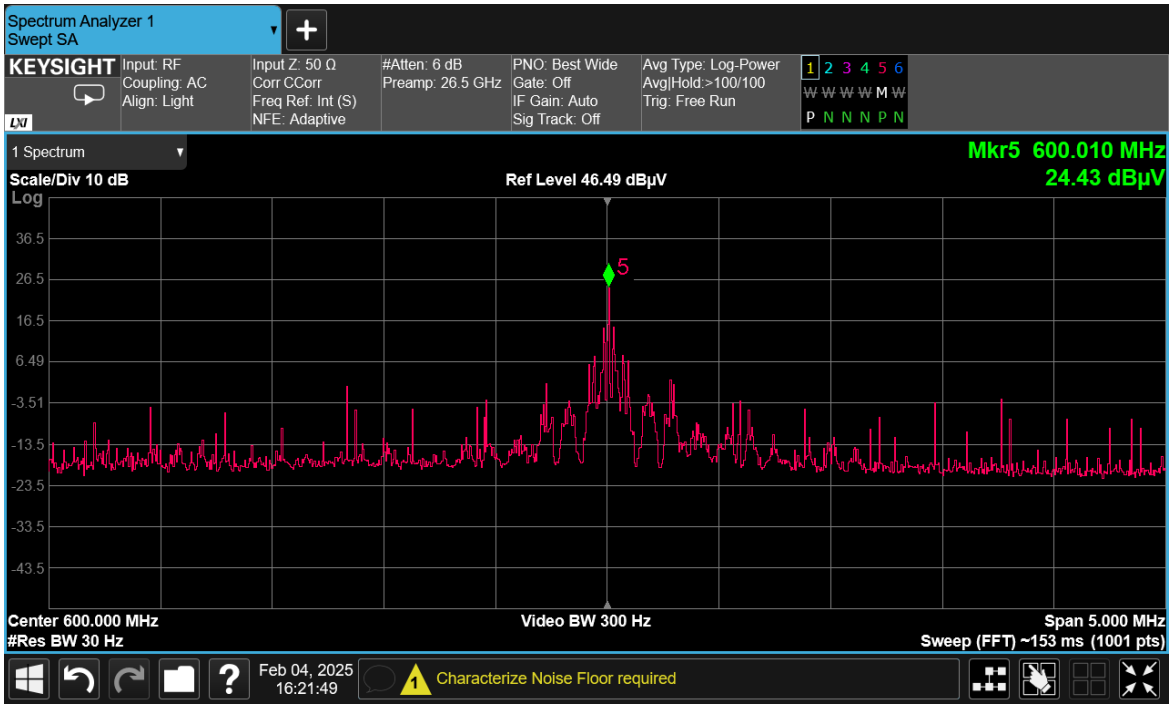

Figure 9: The spectrum of intermodulation radiation of the USB interface under the influence of the HF signal at the frequency 600.01 MHz

Fig. 10 shows the spectrum of intermodulation radiation of the USB interface, which shows the maximum amplification of informative parameters at a frequency of 360.005 MHz with a power of 35.57 dBµV, which should greatly facilitate the restoration of the structure of the transferred files.

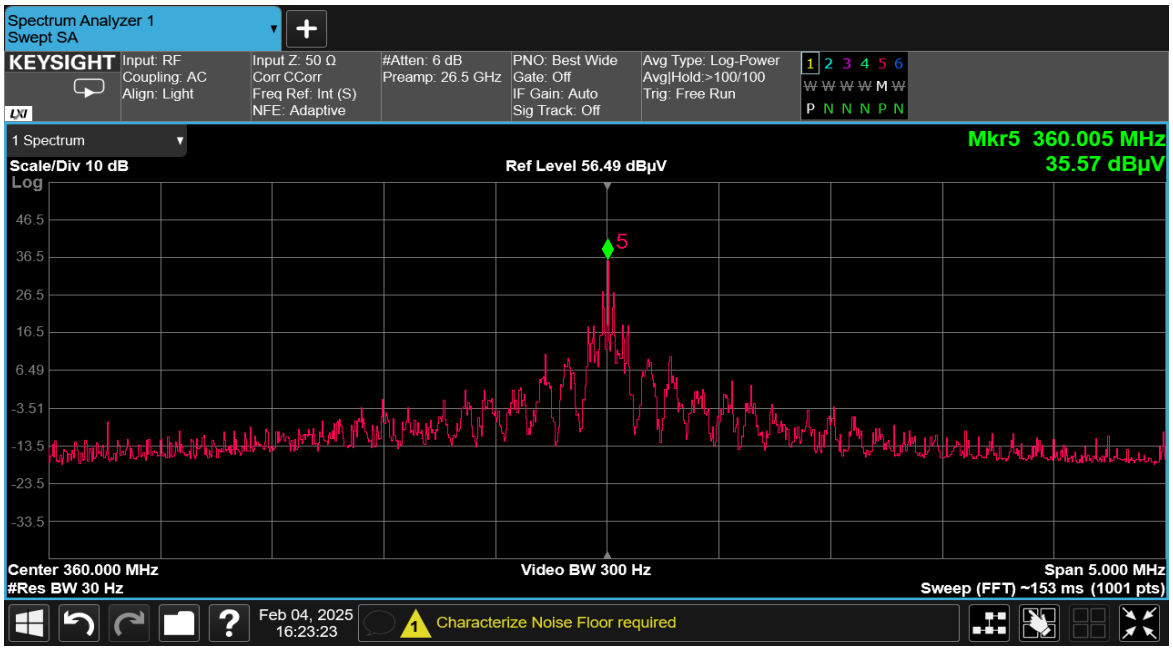

Figure 10: The spectrum of intermodulation radiation of the USB interface under the influence of the HF signal at the frequency 360.005 MHz

3. Spectra of intermodulation radiation on the printer interface—Canon i-SENSYS MF3010 demonstrates that the amplification of side emissions allows interception of information transmitted to the printer. These signals can contain both text data and graphic information.

Fig. 11 shows the spectrum of intermodulation radiation on the printer interface at a frequency of 840.011 MHz, the radiation of which has a power of minus 2.56 dBµV, which allows at least initial identification of the structure of printed commands, and possibly minimal graphic information.

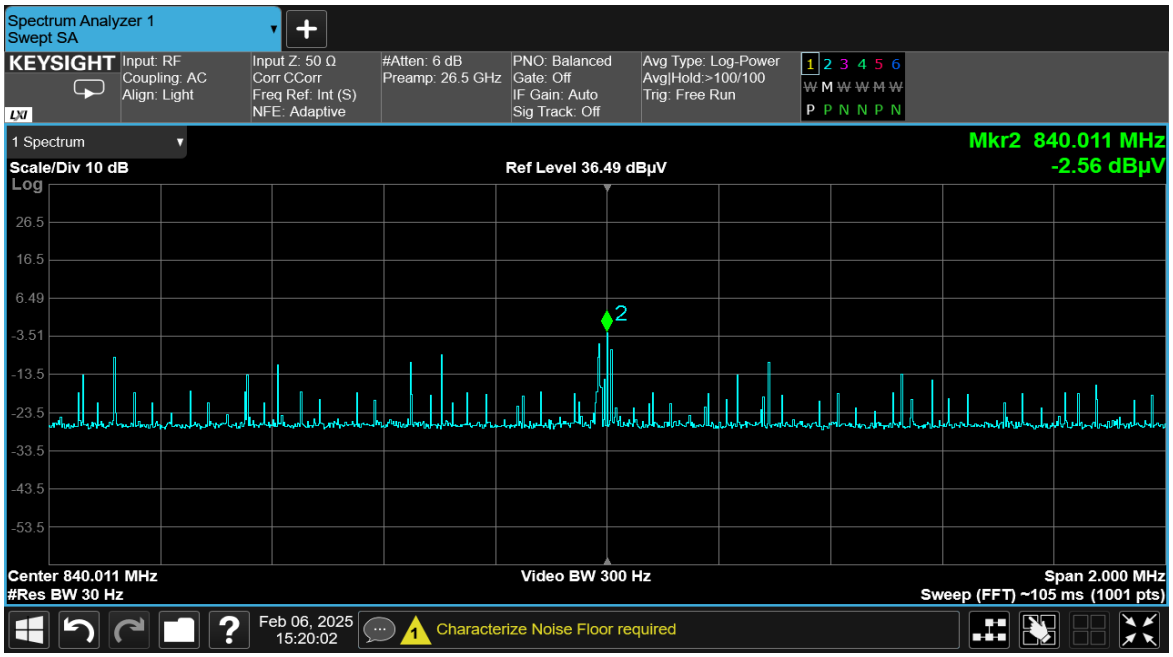

Figure 11: The spectrum of the printer's intermodulation radiation under the influence of the HF signal at the frequency 840.011 MHz

Fig. 12 shows the spectrum of intermodulation radiation of the printer interface at a frequency of 240.003 MHz with a power of 10.28 dBμV, which in theory can ensure the interception of text data transmitted for printing.

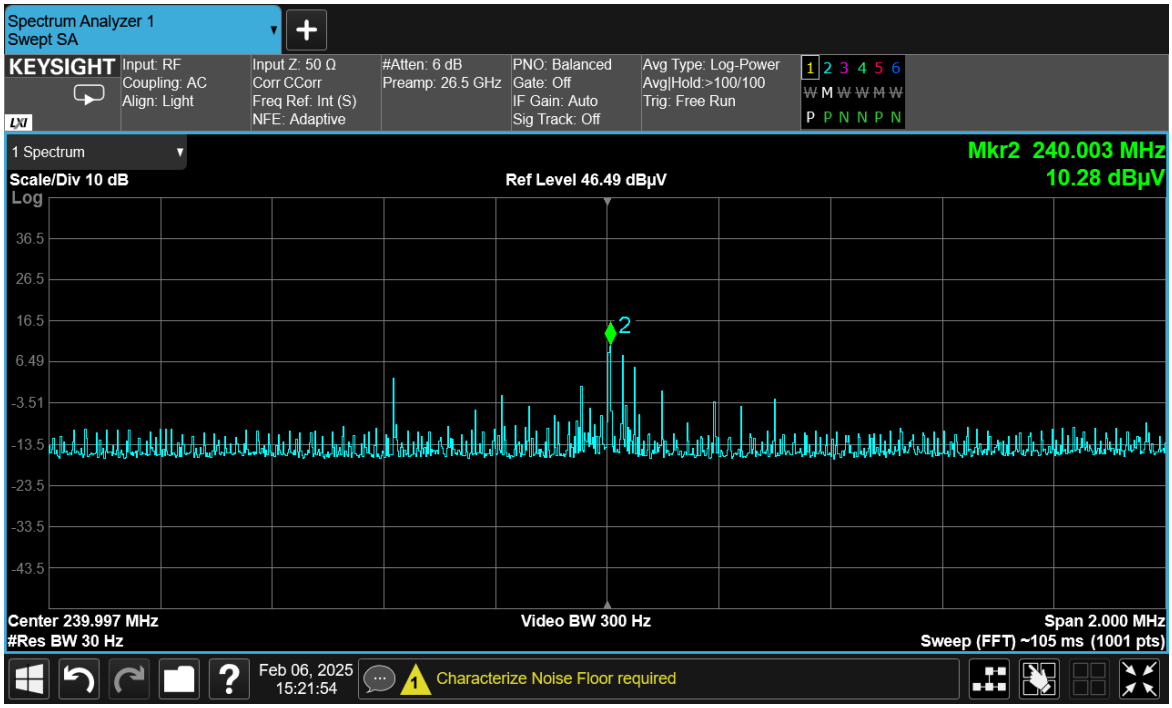

Figure 12: The spectrum of the printer's intermodulation radiation under the influence of the HF signal at the frequency 240.003 MHz

Fig. 13 shows the spectrum of intermodulation radiation of the printer interface at a frequency of 720.01 MHz with a power of minus 0.13 dBμV, which in theory can also provide interception of text data transmitted for printing.

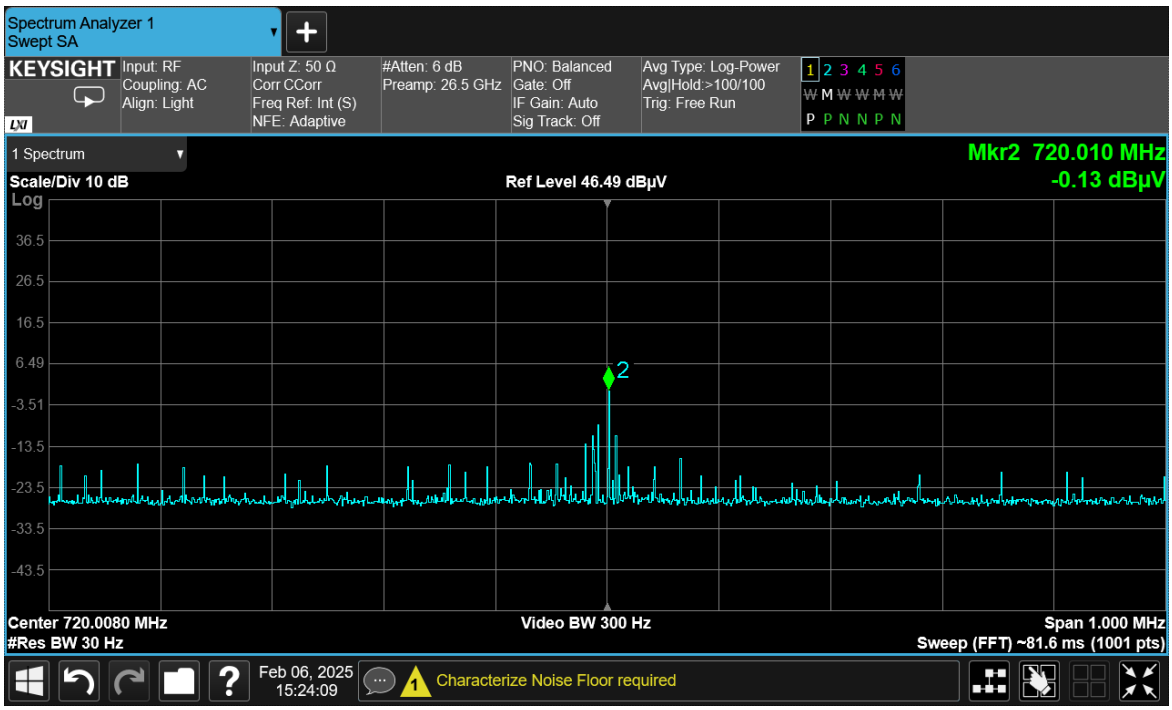

Figure 13: The spectrum of the printer's intermodulation radiation under the influence of the HF signal at the frequency 720.01 MHz

The results obtained emphasize that thanks to high-frequency imposition, it is possible to significantly enhance the informative components of the signal, facilitating the interception of data from various interfaces of a personal computer.

Conclusions

The problem of protecting the equipment of the BTM and ATMS from interception by the method of high-frequency imposition can be solved most effectively if we consider it from the systemic positions as a problem of ensuring electromagnetic compatibility (EMC) of technical systems of transmission, processing, and storage of information. To assess the electromagnetic environment at information activity objects, it is necessary, first of all, to apply methods based on natural measurements.

Considering the variety of types of information processing equipment, the issue of individual measurement of the spectral characteristics of each sample separately is relevant to ensure information security from leakage.

High-frequency imposition can significantly enhance the informative components of the signal, facilitating the interception of data from various interfaces of a personal computer.

The most effective way to protect BTM and ATMS equipment from the possibility of information leakage when using high-frequency imposition is to ensure the maximum possible attenuation for high-frequency currents in all external and internal circuits of this equipment (communication lines, power supply networks, control, and others) and very low attenuation in the grounding system, which is achieved by complete electromagnetic shielding in a wide frequency range of circuit and design elements in combination with broadband filtering and decoupling elements in interstage and interblock communication circuits and the implementation of a low-impedance grounding system for high frequencies.

The use of active protection methods can be recommended in combination with well-executed passive protection by shielding, filtering, and decoupling, to further increase the degree of protection effectiveness.

Fulfillment of the requirements for shielding, filtering, and decoupling in a wide frequency range (from 10 kHz to 30 MHz and more) and some others, set out above, aimed at eliminating the possibility of interception via the leakage channel formed when using the high-frequency imposition method, during the development of BTM and ATMS equipment will significantly reduce the likelihood of information leakage via the overwhelming majority of other currently known information leakage channels.

It is advisable, based on the above, to develop special requirements and recommendations for developers of BTM and ATMS equipment, to ensure their mandatory implementation when creating BTM and ATMS equipment, for which a priori requirements are imposed to ensure security over the high-frequency imposition channel.

Declaration on Generative AI

While preparing this work, the authors used the AI programs Grammarly Pro to correct text grammar and Strike Plagiarism to search for possible plagiarism. After using this tool, the authors reviewed and edited the content as needed and took full responsibility for the publication's content.

References

[1] Regulation on technical protection of information in Ukraine, approved by the Decree of the President of Ukraine dated, 1999. URL: https://zakon.rada.gov.ua/laws/show/1229/99#TTex

[2] Law of Ukraine "On information protection in information and telecommunication systems." URL: https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#Text

[3] Wim van Eck, Electromagnetic radiation from video display units: An eavesdropping risk? URL: http://cryptome.org/emr.pdf
[4] M. Kuhn, R. Anderson, Soft tempest: Hidden data transmission using electromagnetic emanations, Information Hiding. IH 1998. Lecture Notes in Computer Science, vol. 1525, 1998, 124–142. doi:10.1007/3-540-49380-8_10
[5] R. Wallace, H. K. Melton, H. R. Schlesinger, Spycraft: The secret history of the CIA's spytechs from communism to Al-Qaeda, 2009.
[6] L. Kriuchkova, et al., Influence of protective signals on dangerous signals of high-frequency imposition, in: Cybersecurity Providing in Information and Telecommunication Systems, vol. 3654, 2024, 419–425.
[7] L. Kriuchkova, et al., Experimental determination of protective signal parameters for effective "swinging" of the carrier frequency of high-frequency imposition, in: Cybersecurity Providing in Information and Telecommunication Systems II, vol. 3826, 2024, 251–259.
[8] L. Kriuchkova, I. Tsmokanych, Aspects of determining the parameters of protective effects on probing signals of high-frequency imposition, Cybersecur. Educ. Sci. Tech. 2(18) (2022) 197–204.
[9] D. Golev, V. Kononovych, S. Khomych, Methods for assessing information security of telecommunications: Teaching aid, Odeisa, Ukraine: O. S. Popov Odessa National Academy of Telecommunications, 2013.
[10] DSTU EN ISO/IEC 15408-1:2022 Information technology. Protection methods. Evaluation criteria. Part 1. Introduction and general model, EN ISO/IEC 15408-1:2020, IDT; ISO/IEC 15408-1:2009, IDT.
[11] GOST 30373-95. Electromagnetic compatibility of technical means. Test equipment. Shielded chambers. Classes, basic parameters, technical requirements and test methods.
[12] Universal serial bus, Revision 2.0, 2000.