Analytical Estimation Methodology of Compromising Emanations Level Using Monte-Carlo Method

Perepadia Viktoriia[1]
Zabolotnyj Volodymyr[2]

[1] *Kharkiv National University of Radio Electronics, 14 Nauky Ave, Kharkiv UA-61166, Ukraine,viktoriia.perepadia@nure.ua*
[2]*Kharkiv National University of Radio Electronics, 14 Nauky Ave, Kharkiv UA-61166, Ukraine, volodymyr.zabolotnyi@nure.ua*

Abstract. *Based on the electromagnetic field theory and the Maxwell equations, the paper describes the physical content and the way of the compromising emanations propagation into the far zone. This allows finding the dependence and methods of influence on of the test signal parameters, which represents a plurality of electrical impulses, with the change in the field strength at the point of conducting reconnaissance at the input of the receiving antenna, namely, in the distant zone of the technical channel of information leakage at the expense of compromising emanations. The main attention is paid to the Monte-Carlo statistical test method, which is used to generate parameters of videotract signals, which determine its shape in the distant zone. Applying the Monte Carlo method for generating values and will allow reasonably to formulate the realization of random parameters of videotract signals for their correct use during the estimation of compromising emanations level and development of measures protection.*

Keywords: *compromising emanations, technical protection of information, information leakage, statistical test method, distant zone, Monte Carlo method.*

I. Introduction and Problem statement

The most dangerous mode of the personal computer operation, in terms of information leakage, is the mode of the image playback on the monitor screen. This is due to the principle of the video adapter work, which consists of specialized circuits for generating electrical signals for controlling the hardware part of the image playback. The main element, which generates a powerful compromising emanations signal, is an electrical circuit, the equivalent of which is the frame with electric current. Physical processes and phenomena, that occur in it, are described by the corresponding Maxwell equations [1].

For the development of effective protection means from information leakage through technical channels at the expense of compromising emanations it is extremely important to quantify the compromising emanations level of hazardous signals. Referring to the normative and technical document «TP EOT-95», the values of the indicator of information leakage through technical channels at the expense of compromising emanations are absolute values (at the boundary of the controlled zone) of the intensity of the electric and/or magnetic field. It is advisable to estimate the reconnaissance range precisely in a far zone, because the distance, to which electromagnetic waves propagate, can reach tens of meters, and a potential reconnaissance device can be situated exactly within the far zone.

Typically, the intensity of the electric and magnetic field is determined experimentally with the help of measuring equipment, or experimentally-analytically with the use of control equipment. Since these methods have a number of significant drawbacks, the purpose of the work is to develop precisely an analytical estimation methodology of the compromising emanations level of the test signal harmonics of a personal electronic computer videotract.

II. The Estimation of Compromising Emanations Level Using Monte-Carlo Method

In the practice of information technical protection, compromising emanations studies are explored on the basis of test signals. As test signals in most cases a signal of the type "meander" is chosen, that is, the sequence of regular signals "pixel black/pixel white" (fig. 1).

The defining parameters of the test signal are pulse amplitude A, pulse length at half-amplitude level (fig. 1).

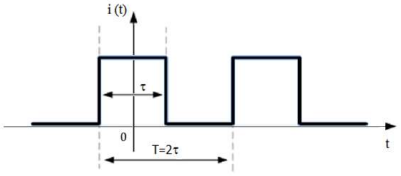

Figure 1. Signal of the type "meander"

In the previous paper [5], the way of determining the spectrum of a single pixel formation signal with the above characteristics is described. The method is based on the properties of the relations between the time and frequency characteristics of the signals during differentiation, integration, time shifting, scaling, based on the properties of Fourier transformations.

As a result of previous studies [6], it was found that in the distant zone, at the antenna input of the receiver, the shape of the explored compromising emanations signal is determined by the form of a second derivative from the form of the output electric current in the electric circuit circle of the video signal emitter in the form of the frame with electric current. In addition, the characteristic feature of the signals circulating in the real electrical circuits of the computer equipment, is the presence of such parameters as: δ is the length of the smooth transition of the signal between the linear parts (between the stationary value and the linear variable, and vice versa); Δ is the length of the approximation of the linear component of the pulse front (growth/decrease of the signal from *0* to *A*), which determine the shape of the signal. Moreover, there is an insignificant difference between smooth transitions bottom and top of pulses. The difference is due to the mechanism of their formation, namely the cutoff mode or the saturation regime, which are characteristic for the transistor operation of the pulsed circuits. The presence of the above parameters reduces

the radiation level of the signal at high frequencies [7]. This allows to minimize the compromising emanations level, thus providing the necessary level of information security. In turn, the pressing question remains the finding of the influence method on the values Δ and δ during the signal formation in the electrical circuit.

Since it is not always possible to determine the magnitude of the intensity of the electric field *E*, or its value is not accurate, the only correct approach for estimating technical protection of information is probabilistic. Its essence is to represent the desired quantities in the form of a range of values, that satisfy certain requirements.

The Monte Carlo method allows to solve probabilistic problems by statistical methods. The theory of this method indicates how to choose random values for calculations and how to evaluate the obtained results. The method is based on multiple runs (random implementations), based on the constructed model with the subsequent statistical data processing in order to determine the numerical characteristics of the object under study (process) in the form of its parameter's statistical estimates.

The imitation modeling by the Monte Carlo method allows to construct a mathematical model with uncertain parameters, and, knowing their probabilistic distributions, as well as the relationship between the change of parameters (correlation), obtain the distribution of the investigated function. Probabilistic distribution regulates the probability of choosing values from a certain interval. Within the model of the probabilistic risk analysis model, a large number of iterations are conducted to determine how a productive indicator behaves (within what range it fluctuates, what distribution) in the case of substitution of a variable in a model according to a given distribution.

For this, in the first place, it is necessary to model a sample of values Δ and δ , using Monte Carlo method within the specified limits. The distribution of values during the modeling is uniform, which ensures their greatest uncertainty. It is important to take into account some limitations associated with physical processes occurring in the computer equipment:

$$0 \le \delta \le \Delta \le \tau \,. \qquad (1)$$

Except the obvious inequalities (1), it is necessary to ensure the inequality implementation (2), which rejects such distortion of the simulated video pulses, that reduce their amplitude.

$$\delta \le \tau - \Delta \,. \qquad (2)$$

Generating of random values is carried out according to formulas (3) and is checked for compliance with restrictions (1) and (2).

$$\begin{cases} \Delta = \Delta_{\min} + \xi_1(\Delta - \Delta_{\min}), \\ \delta = \delta_{\min} + \xi_2(\delta_{\max} - \delta_{\min}), \end{cases} \qquad (3)$$

where $\Delta_{\min}$ is the value of the length of the approximation of the linear component of the pulse front, it is determined by the characteristics of the semiconductor components of the electronic circuit videotract;

$\delta_{\min}$ is the minimum value of the length of smooth transitions in the pulse, it is determined by the parasitic reactivity components of the electronic circuit videotract;

ξ_1, ξ_2 are the corresponding random variables values within 0-1.

Based on the foregoing, taking into account (3), the value Δ and δ should be situated in the selected region (fig. 2).

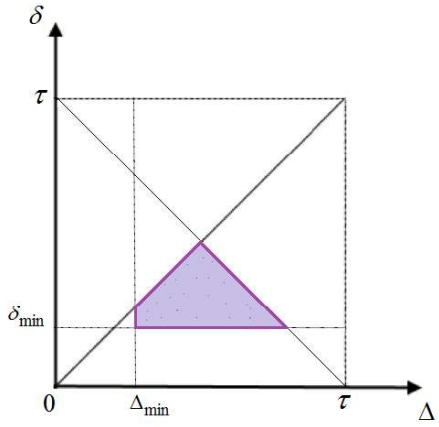

Figure 2. The region of values Δ and δ

III. CONCLUSIONS

As a result of the analysis, it was proposed the analytical estimation methodology of the compromising emanations level of the test signal harmonics of a personal electronic computer videotract. The described methodology has a number of advantages over the existing experimental ones. The obtained approach avoids obligatory activation of the computer equipment for the estimation of the information leakage technical channel, which makes it possible to scan compromising emanations before it is used. In addition, it is possible to assess the intelligence accessibility of computer equipment before it is manufactured.

Further researches will be will be dedicated to the substantiation of certain values Δ and δ to optimize the spectrum of harmonics in a given frequency band in accordance with the standards of protection.

REFERENCES

[1] J. Jin, *Theory and computation of electromagnetic fields*. Hoboken: Wiley, 2015.

[2] T. Simpson, *Maxwell on the electromagnetic field*. New Brunswick, NJ: Rutgers University Press, 1997.

[3] S. Alessio, *Digital Signal Processing and Spectral Analysis for Scientists*. Cham: Springer International Publishing, 2016.

[4] V.I. Zabolotnij, Ye.V. Gerasimenko, V.I. Perepadya. "Doslidzhennya zmin formi signalu u kanali pobichnih elektromagnitnih viprominyuvan monitoru [Investigation of the signal shape change in the compromising emanations channels of the monitor]." *Radiotehnika*, no. 176, pp.116-121, 2014.(In Ukrainian)

[5] V.I. Zabolotnyj, E.V. Gerasimenko. "Transformaciya formy signala v kanale pobochnyh elektromagnitnyh izluchenij [The waveform transformation in the compromising emanation channel]", in *Materialy Shestnadcatoy mezhdunarodnoy nauchno-prakticheskoy konferenciyi «Bezopasnost' informacii v informacionno-telekomunikacionnyh sistemah»* [*Procceding of 16th International Scientiffic and Practical conference "Information Security in Information and Telecommunication Systems"],* 2013, 155-159.(In Russian).

[6] S. Alessio, *Digital Signal Processing and Spectral Analysis for Scientists*. Cham: Springer International Publishing, 2016.

[7] D. Mukhopadhyay and R. Chakraborty, *Hardware security*. Boca Raton, Florida: CRC Press, 2015.