DOI: https://doi.org/10.15276/aait.04.2021.7
UDC 004.056.53

Protection of computers from side electromagnetic radiation during monitor images formation

Volodymyr M. Lutsenko [1)]
ORCID: https://orcid.org/0000-0001-7632-1730; lutsenkovn@ukr.net
Dmytro O. Progonov [1)]
ORCID: https://orcid.org/0000-0002-1124-1497; progonov@gmail.com. Scopus Author ID: 57201682654
[1)] Igor Sikorsky Kyiv Polytechnic Institute. 37, Prosp. Peremohy. Kyiv, 03056, Ukraine

ABSTRACT

Reliable protection of confidential data processed in critical information infrastructure elements of public institutions and private organizations is topical task today. Of particular interest are methods to prevent the leakage of confidential data by localizing informative (dangerous) signals that both carry an informative component, and have a signal level higher than predefined threshold. The increase in signal energy from personal computers is caused by increasing of its transistors switching speed. Modern passive shielding methods for secured computers, similar to the well-known program TEMPEST, require either costly and large shielding units or technological simplification by using of low-cost fragmentary shielding of computer's individual elements. Therefore, localization of side electromagnetic radiation produced by personal computer is needed. The paper presents a cost-effective approach to reducing the level of computer's electromagnetic radiation by passive method. The radiation are localized and measured by its estimation on personal computer's elements, namely unshielded communication lines between video processor and a monitor, fragments of electric tracks on motherboards, etc. During experiments authors used ad-hoc miniature electric (ball antenna) and magnetic (Hall sensor) antennas connected to selective voltmeters. This approach significantly reduces the cost of equipment and measurements as well as requirements to analytics' qualification for improving computer's protection. Also, the alternative approach for computer protection is proposed. The approach is based on image content protection by distorting the image on the monitor instead of reducing electromagnetic radiation caused by signals from the monitor. The protection includes image scrambling using Arnold transform that randomly "shuffle" the lines in each frame.

Keywords: Electromagnetic radiation; cryptographic processing; video imaging; sensitive data

***For citation*: Lutsenko V. M., Progonov D. O. Protection of computers from side electromagnetic radiation during monitor images formation. *Applied Aspects of Information Technology.* 2021; Vol.4 No.4: 377–385. DOI: https://doi.org/10.15276/aait.04.2021.7**

INTRODUCTION

Reliable protection of confidential data (CD) that are circulated in critical information infrastructure (CII) elements of public institutions and private organizations is topical task today. Special attention is paid to prevention attacks on CII elements, in particular personal computers (PCs) [1].

Currently, PCs are widely used in automated systems (AS) for CD processing, for example as a part of information processing unit (IPU). Ensuring the protection of PCs from unauthorized influence during an information attack requires usage of methods and equipment for estimation the degree of PCs resistance (robustness) to both cyber threats and the impact of physical signals and fields.

A common approach to PC protecting from CD leakage is to use passive protection methods. These methods are aimed at reduction of informative signals level, through the integrated application of methods of IPU shielding, filtering and grounding. Special interest is taken at shielding of side electromagnetic radiation (SEMR) produced by any component of PC.

Widespread implementation of advanced hardware technologies in PCs, for example high-speed data transmission systems, complicates the problem of SEMR localization. The reason is the increasing of signal energy (power) produced by PC elements due to corresponding growth of transistor switches frequency. This is explained by well-known effect that a transistor consumes energy only at the time of transition from one logic level to another, while power consumption at other time (e.g. cut-off state) is absent, so it has nothing to emit. That is, a more powerful PC emits a larger signal that complicates its protection from SEMR.

The paper is aimed at investigation of SEMR produced by PC's installed components. Solving of this task allows determining an element of computers with the highest energy of produced SEMR and reference frequencies of generated electromagnetic radiation. This makes possible using of local (fragmentary) shielding of such elements without usage of costly shielding the whole PC or its motherboard. Also, this introduce opportunity to usage of cryptography-based methods, namely Arnold transform based image scrambling, for additional protection of communication signals

between PC components, namely graphics processing unit (GPU) and a monitor.

RELATED WORKS

Design and implementation of integrated information protection system (IIPS) for CII of agencies and organizations require carrying out special investigation to assess the PCs protection level to attacks [2]. The results of investigation allow selectin appropriate methods and equipment for computer upgrade with the aim of decreasing SEMR level, produced by computer's components. This electromagnetic radiation can include parts of informative (dangerous) signals that have been confirmed in the numerical studies of G. Yadli [3].

The special investigation of PC to assess its protection level is resource-intensive procedure and, generally, this task is not related to developers of IIPS. The solution of this task is complicated by the emergence of advanced technical solutions for general-purpose PC, such as high-speed data transmission between PC's components. In general, the search for effective methods to counteract CD leakage by its processing in information processing unit (IPU), such as PC, is topical task today.

In addition, there is a need to determine the feasibility of high costs for secure PCs creation. Therefore, the study of PC's passive protection effectiveness as well as performance analysis of advanced device controlling modes (interaction with hard drives, connection, GPU) can make possible effective and low-cost PC's protection.

THE SCOPE OF THE RESEARCH

The paper is aimed at development of methods for imaging signals preprocessing for prevention unauthorized access to CD even in case of interception of generated SEMR by an attacker.

To achieve this goal, the following tasks were considered and solved in the work:

1) Experimental estimation of SEMR produced by typical PC by processing video data and its displaying at monitor;

2) Review of modern methods for counteracting to CD leakage by an attacker unauthorized access both to the graphic data bus, and interception of SEMR created by the given buses;

3) Development of graphic data preprocessing method for prevention unauthorized access to CD in case of SEMR interception by a malefactor.

The object of research is the processes of information processing in typical PCs, as well as the generated SEMR. The subject of the research is modern methods of increasing PC protection from unauthorized access to CD by intercepting and analyzing of SEMR generated by data processing systems.

STUDY OF THE ELECTROMAGNETIC RADIATION LEVEL FOR PERSONAL COMPUTERS

The PC protection methods can be divided into active and passive ones. Passive methods are aimed at reducing the level of physical signals containing CD, while active methods are used to mask these signals by increasing the level of interference (noises). It should be noted that passive methods are the main protection methods, while active methods used only when a given degree of IPU protection is not achieved by passive methods.

The most widespread methods of passive protection include [4, 5]:

1. The use of autonomous or stabilized power sources for IPU;

2. The use noise reduction filters in power supply circuits of IPU, as well as lighting and socket network lines within the controlled zone and allocated rooms;

3. Grounding and shielding of IPU's components, shields of connecting lines.

These methods can be used both individually and in combination, while IPU's grounding is mandatory.

Usually, the implementation of IPU's shielding is based at closing the PC in a shielding case. The design, construction and maintenance of shielding systems are an expensive procedure in general case. However, it does not guarantee achieving protection level defined by technical requirements. Therefore, the question of new protection methods expediency that considerably reduces protection cost and term of works is raised.

Representation of graphical information on a monitor screen is one of the most dangerous functions of the PC in terms of the possible formation of information leakage channels [6, 7], which threatens IIPS as a whole. Before being shown on a monitor, the digital image data is processed by the PC's central processing unit. Then preprocessed data are copied from RAM to a GPU's memory. A digital image is created in the video memory to be played back on the screen. Then, the graphical data is transmitted from video memory to a digital-to-analog converter, where it is converted into an analog form and only then enters the monitor with a cathode-ray tube (CRT). With the advent of liquid crystal displays (LCDs), the need for digital-to-analog signal conversion disappeared. But this element is still present in some video cards in case of connecting analog monitors via a VGA connector.

ISSN 2617-4316 (Print)
ISSN 2663-7723 (Online)

The monitor displays graphical data in the form of dots (picture elements, pixels). These pixels form a single image that is updated from 50 to 120 times per second, depending on the type of display and the data provided by GPU. CRT-based monitors update the display with lines, while LCDs update each pixel as a separate (independent) element.

From the theoretical point of view, the sources of SEMR on a video card can be: conversion circuits, the area near the connector between the monitor and the system unit, memory and GPU itself. The experimental studies of SEMR level generated during PC working were performed in the work to test mentioned theoretical assumptions.

The measurement was carried out in two stages: the preparation and measurements ones. At the first stage, the SEMR levels in the video circuit were measured during PC's monitor operation in the test mode.

The general scheme of measurements is shown at Fig.1 [8, 9], [10]. The experiment's results make it possible to determine SEMR frequencies that are related to a PC.

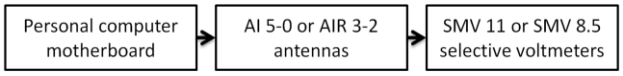

Fig. 1. **General scheme of measurements of side electromagnetic radiation of personal computer components**
Source: **results of study [7]**

Typical antennas AI 5-0 and AIR 3-2 (Fig. 1) are used as a sensitive element of the receiver [11]. These antennas meet the regulatory documents of Ukraine requirements in the domain of information technical protection. Selective voltmeters are used as the measuring unit of the receiver, namely: SMV-11 for the frequency range up to 30 MHz and SMV 8.5 for the frequency range up to 1 GHz. A sign of the informative signal carrier frequency presence during test is a sound signal. Based on the results of the first stage, a list of frequencies with the corresponding signal levels and the type of antenna used to obtain these signals is formed.

At the second stage, the position of the PC element with the highest level of SEMR at certain frequencies is determined. In this case, the PC is configured in the same test mode, as in the first stage. The measuring equipment is tuned to one of the frequencies, which was determined at the previous stage as dangerous (signal energy at this frequency significantly exceeds the signal levels at other considered frequencies).

In contrast to the previous stage, an ad-hoc antenna is used for these studies. A Hall sensor is used to register the magnetic field from ring-shaped sources at low frequencies, while a small ball (point) for tracking of electrical field relative strength is used. The relative levels of signals near individual elements of the PC's motherboard are determined with a point antenna.

It should be noted that signal's exact parameters (magnitude and frequency) are not needed, while we are looking for the places with the strongest SEMR in comparison with other elements of the board. This can be achieved by changing the mutual positions for PC's components and receiving antenna to find out the maximum value of the magnetic and electrical components of the electromagnetic field. Therefore, it makes no sense to calibrate the antenna for estimation exact parameters of SEMR sources parameters.

Considered procedure is repeated for all frequencies according to the list of frequencies obtained at the first stage. The distance varies from 0 to 2-3 cm, and the angle of the antenna varies from 0^0 to 90^0.

It should be noted that the proposed method allows not only localizing a SEMR sources, but also the relationships between them through electromagnetic fields. Also, several additional parameters are checked, namely characteristics of SEMR influenced at a motherboard busses, mutual influences between these busses, locations of field concentrators on bends of traced conductors and on electronic components, directions of radiation, places of field formation separately by magnetic and electrical components.

Based on the proposed method results, graphs of the SEMR level dependence on frequency for certain PC's elements are constructed (Fig. 2).

The measurement results (Fig. 2) illustrate the signal levels and frequencies at which the test signal is detected. According to the experimental results, three dangerous places were identified: the GPU, video memory and the area of the connector, while a monitor screen has relatively small SEMR level. The identified SEMR sources can be protected either by creating separate shielding units, or preprocessing of transmitted signals with cryptographic methods.

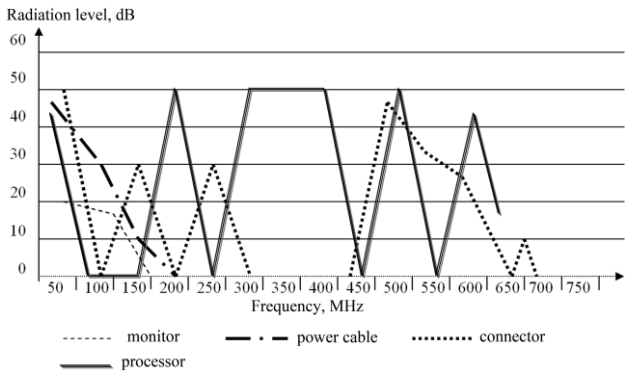

Fig. 2. **The dependency of the radiation level on frequency for each element of the video path**
Source: **experimental studies of the authors**

Thus, the development of video signals preprocessing methods to reduce the likelihood of access to CD by interception of generated SEMR is of special interest.

PROPOSED METHOD FOR VIDEO SIGNALS PROTECTION AGAINST INTERCEPTION

Given the considered results of experimental research, it is of interest to develop methods of graphic data protection that taking into account the features of data exchange between the GPU and monitor. Solving the problem is complicated by presence on modern market of various types of video data transmission protocols whose characteristics differ significantly.

One of the most common video data transmission protocols are the following [12, 13], [14, 15]:

- DVI (Digital Video Interface) – one of the most widespread protocols for video data transmitting to displays, including LCD monitors.
- HDMI (High Definition Multimedia Interface) – the common protocol for transmitting both video and audio data, in particular high-definition video.
- DisplayPort – the widespread protocol for high-definition video transmission for LCD monitors, in particular multiplexing various video streams using a single cable.
- MHL (Mobile High-Definition Link) – the protocol for video and audio data exchange between mobile devices, such as smartphones and tablets, and display devices (TVs, monitors). The protocol is based on combining the functionality of HDMI and USB protocols for the formation of a digital data stream from a mobile device and further processing of this stream on a display device.

The DVI interface has been widely used in last decades as the primary method of transmitting graphics data from a video processor to a monitor. The protocol is based on usage of Transition Minimized Differential Signaling (TMDS) method for data streaming [16]. The TMDS is based on utilization of three channels for data and service information with a bandwidth up to 3.96 Gbps per channel in simplex mode, and up to 7.92 Gbps in duplex mode. The achievable resolution for the DVI is up to 2560x1600 pixels (30 Hz frame rate, simplex mode), or 3840x2160 pixels (30 Hz frame rate) for duplex mode.

The HDMI interface is used today for multimedia data exchange for PC (between GPU and a monitor) and Hi-Fi devices (digital receivers, audio amplifiers, TVs) [17]. The multimedia data transmission is carried out using five pairs of conductors and separate (unshielded) conductors for service data exchange. Audio and video data are transmitted using four pairs of wires, while the fifth pair can be used to multiplex Ethernet data protocols (up to 100 Mbps) for connected devices. Also, the HDMI offers extensive capabilities for additional data transmission (control signals of connected devices, HDMI CEC), as well as the protection of multimedia data from unauthorized copying using High-bandwidth Digital Content Protection (HDCP) technology [18].

The DisplayPort is one of advanced interface for connecting display devices (monitors, TVs) to a PC. The main difference between this protocol and HDMI is the increase of channel bandwidth (up to 25.92 Gbps for DisplayPort 1.4, and up to 18.00 Gbps for HDMI 2.0) without introducing significant changes to the hardware [19]. Both HDCP technology and additional methods, such as DPCP (Display Content Port Protection) technology based on the use of AES encryption method with a 128-bit key, are used for data protection [19]. Like the MHL interface, the DisplayPort makes it possible to perform multiplexing of multimedia and digital data streams as well as transmit up to 100 watts of power to the connected device via a single cable.

The MHL interface was proposed in 2010 to expand the transfer of multimedia data from mobile devices to monitors and TVs using USB hardware. The interface is based on multiplexing and compression of data on the mobile device side, and subsequent demultiplexing and error correction on the display device side. Today, the MHL protocol is widely used to connect mobile devices to monitors/TVs, as well as data exchange with car multimedia systems.

It should be noted that the considered protocols provide opportunities for data protection against unauthorized copying during transmission between connected devices. As an example, we may mention HDCP based on mutual authentication of connected devices as well as end-to-end data encryption [18]. The authentication protocol is used by mutual verification of HDCP-transmitter and HDCP-receiver.

The protocol uses cross-checking of a set of built-in secret keys via next three stages [18]:

- Establishing a shared secret;
- Sent message to HDCP-repeater about key selection vectors and connected HDCP-recipients;
- Initialization of HDCP cipher parameters to encode the frame contents that transmitted from a graphics adapter to a monitor.

Each HDCP device is stored a unique set of forty 56-bit device private keys (DPK) and a

ISSN 2617-4316 (Print)
ISSN 2663-7723 (Online)

corresponding 40-bit key selection vector (KSV) [18]. During data exchanging, the devices create a shared secret based on mentioned keys that is used as a symmetric key to decrypt HDCP data.

The HDCP encryption procedure consists of bitwise addition (XOR) of a data stream with a pseudo-random sequence generated by the HDCP cipher. The HDCP cipher updates the shared key every 56 bits, which complicates the task of cipher hacking.

The HDCP technology provides mutual authentication of connected devices to counteract unauthorized data transmission to third-party users, and it is characterized by high cryptographic security of messages protection methods [18]. However, this technology requires licensing and it is adapted for use only with multimedia data. This limits usage of HDCP to protect the open lines of communication between a GPU and a monitor when transmitting only graphics data.

For overcoming this limitation, method of graphic data protection was proposed. The method is based on modifying the protocol of data transmission from a GPU to a monitor, namely preliminary "mixing" (scrambling) of the current frame content to counteract its recovery by an attacker in the case of SEMR interception.

The proposed frame content preprocessing is carried out in several stages. At the first stage, scrambling of frame's rows is performed using a pseudo random number generator. The generator's parameters are part of the secret key, which is shared between a GPU and a built-in monitor's processor. Then, the image's rows are rearranged in the video memory according to the generated sequence. Finally, the rows are sent to the monitor, whose signal processor restores the original sequence of image's rows.

In the general case, the resistance of the proposed method to hacking when intercepting rows of the current frame by a third-party user is $L_x!$, where L_x is the number of rows for current frame. However, this estimate can be significantly reduced by taking into account high correlation of adjacent rows brightness values. This leads to decrease the complexity of the brute force search up to $O(L_x \log(L_x))$ – the difficulty of sorting the image rows by the criterion of adjacent pixels brightness correlation. To overcome this limitation, we propose to use frame pre-scrambling using the Arnold transform (AT) [20, 21, [22, 23]:

$$\begin{pmatrix} x_{i+1} \\ y_{i+1} \end{pmatrix} = \mathrm{mod}\left(\mathbf{R}_{2\times 2} \times \begin{pmatrix} x_i \\ y_i \end{pmatrix}, M_D \right), \mathbf{R}_{2\times 2} = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix}, \quad (1)$$

$$\begin{pmatrix} x_i \\ y_i \end{pmatrix} = \mathrm{mod}\left(\mathbf{R}^{-1}_{2\times 2} \times \begin{pmatrix} x_{i+1} \\ y_{i+1} \end{pmatrix}, M_D \right), \mathbf{R}^{-1}_{2\times 2} = \begin{pmatrix} 2 & -1 \\ -1 & 1 \end{pmatrix}, \quad (2)$$

where: x, y are pixel's coordinates in frame $\mathbf{D}_{x,y}$, respectively; mod() is modulo operation; i is the number of the current iteration of AT.

It should be noted that period of PA, namely the number of iterations (1) after which the original image is restored, nonlinearly depends on frame $\mathbf{D}_{x,y}$ size, which complicates estimation of message parameters [24, 25], [26, 27]. The number of iterations of the PA can be used as the secret key of scrambling in this case.

The example of image pre-processing using the AT (15 iterations) is shown at Fig. 3.

It should be noted that even usage of relatively small number of AT iterations allows bringing a processed image into a pseudo-random signal (Fig. 3).

The AT can be applied to images that have an equal number of rows and columns (L_x=L_y). In the general case, the L_x and L_y depend on the monitor parameters that limit direct applying of PA to the current frame.

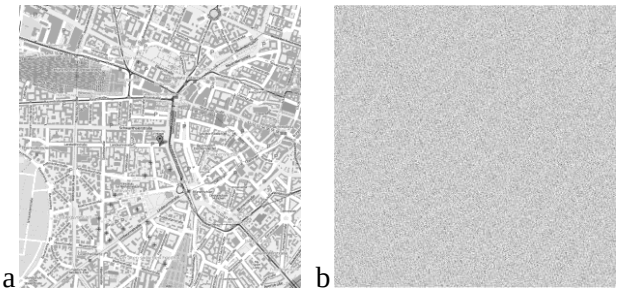

Fig. 3. **Example of grayscale image preprocessing using Arnold transform (15 iterations): a – the original image; b – processed image**

Source: **computer modeling by authors**

To overcome this limitation, we proposed to use the following image preprocessing procedure:

- Selection of sliding window (SW) size w that will be used for AT applying to frame content ($1<w<\min(L_x,L_y)$);
- Pseudo-random selection of k positions of SW (coordinates (x_i, y_i), $1<i<k$, $1<x_i<(L_x-w)$, $1<y_i<(L_y-w)$) for frame content scrambling;
- Application of AT to frame's pixels within each SW position by gradual applying of each sliding window.

Restoration of frame view is performed by applying of inverse Arnold transform for each sliding window.

It is worth noting that the selection of sliding windows positions can be performed as follows:

- By taking into account the current frame content (for example, applying of AT only for SD displayed as text or image);

- Pseudo-random selection of frame's rows / columns according to uniform distribution.

Pseudo-random selection of the SW position can lead to reprocessing of the frame's pixels several times if the positions of the sliding window overlap. In this case, the complexity of frame content restoration in the case of interception of the current frame by an attacker can be estimated as difficulty of a complete search of the possible size and mutual positions of the SWs for the current frame

$$F = \mathrm{O}\left(\left(L_x - w\right)^k \cdot \left(L_y - w\right)^k \cdot f_{\mathrm{AT}}\left(w\right)\right), \qquad (3)$$

where $f_{AT}(w)$ is a function for estimating the number of AT iterations by processing of a matrix of size *w*x*w* elements.

For additional improvement of frame recovery complexity, a frame can be pre-divided into non-intersecting blocks. Then, the AT with the predefined number of iterations is applied to each of the blocks.

The advantages of proposed approach include:

- Pseudo-chaotic view of obtained results complicates the restoration of original frame by an attacker – significant variation of individual pixels "trajectory" movement at each stage of transformation;
- The phenomenon of pixels mixing (interleaving) within a frame – increases the robustness of the preprocessed frames to the removal / change of a set of pixels;
- The possibility of using a more technological approach to ensure the PC security at the stage of motherboard assembling, without applying of special features, namely: shielding of a separate board or the system block as a whole, usage of special tracing of conductors, design of protective filters for PC units, special design of grounding circuit, etc.
- Simplification of existing PCs modernization for secure working by taking into account the requirements of IIPS;
- Reduction of metal consumption by PC boards, which leads to decrease the probability of random antennas appearance in the form of additional large metal screens, in the presence of a reactive component in the "screen-ground" connections. Also, this leads to increase the probability of SEMR irradiation out of predefined frequency range, where shielding units can obtain features for receiving and retransmitting generated SEMR.
- Reducing the cost of creating a PC in a protected design;
- Objectivity of protective equipment usage by taking into account of intervention into design and location of PC components.

DISCUSSIONS

The effectiveness of proposed approach was analyzed by full-scale experiments using mentioned ad-hoc antennas. Obtained experimental results allow estimation spectral parameters of captured SEMR signal for a test PC (Fig. 2). Then, the inconsistent refinements of monitor signal processing unit was performed. The improvements mimic the operating system operations to form an almost arbitrary sequence of frame's rows, which are displayed on the monitor screen.

Updated test PC was used during repeated measurements with mentioned ad-hoc antennas. Measurements of the spectrum components were performed with an electric ball antenna. Obtained results allow us to state that the spectrum of the SEMR signal (Fig. 2) is indeed distorted. Moreover, the envelope of the spectral components (Fig. 2) becomes more linear, i.e. the spectral "image" of the PC is destroyed.

Indeed, it is too early to talk about the degree of original spectrum distortion for the final quantitative conclusions. To do this, it is necessary to accumulate statistics of such distortions that allows determining mathematical indicators of distortions, such as the entropy quality factor of spectrum components randomness, the variance of the spectrum envelope nonlinearity, etc. Nevertheless, we can say that observed distortions have a positive trend in terms of monitor security.

In addition, proposed method complicates synchronization of SEMR interception within single frame duration. This is also a positive factor. The stability of frame restoration security increases according to the considered exchange protocols in comparison with the case of direct data transmission. It depends on the algorithm for determining the sequence of frame's rows, which is displayed on the screen at the moment. Final conclusions can be drawn after examining the operation of a large number of monitors of different types.

CONCLUSION

It should be noted that degree of frame spectral distortion (Fig. 2) still requires the definition and provability of such a definition. To do this, the entropy quality factor of the randomness of the spectrum envelope must be determined. Also, obtained spectrum (Fig. 2) is selected from a set of similar graphs obtained for different PCs, and does not allow to make these calculations. It turned out

ISSN 2617-4316 (Print)
ISSN 2663-7723 (Online)

that spectrum envelope is linearized after mixing the frame rows, and this gives hope that repeating these experiments on different images on the screen will suggest that the spectrum envelope ceases to be non-correlated with specific computer and any image displayed on the screen.

In addition, considered method of identifying PC components as a source of SEMR allows an individual approach to the analysis of security for each element of PC system and the development of appropriate methods for its protection. This means either an improvement of small objects shielding, or the development of an operating system with the described specific sweep of frames content on the screen. This can increase the security of PC without the need for comprehensive use of passive or active security techniques.

According to the results of research, the cases have been identified that proved possibility of hardware implementation of proposed solutions. It allows obtaining the effect of smoothing the steepness of SEMR pulses fronts by corresponding reducing the power of irradiation.

In general, proposed approach is rational and simplifies the procedure for designing IIPS for AS, namely reducing abilities of a PC to create SEMR leakage channels. This makes possible PC protection improvement by only introduction of a secure operating system with the proposed methods.

REFERENCES

1. DSTU 3396.0-96 “Information protection. Technical protection of information. Basic principles”, version from 01.01.1997 (in Ukrainian). – Available from: https://tzi.com.ua/downloads/DSTU%203396.0-96.pdf. – [Accessed: March 2021].

2. ND TZI 3.7-003-05 “The procedure for creating an integrated information security system in the infocommunications system” (in Ukrainian). – Available from: http://www.dut.edu.ua/uploads/l_1057_37661772.pdf. – [Accessed: March 2021].

3. Motuz, O. V. “Side electromagnetic radiation: moments in history” (in Ukrainian). *Information Protection*. 2001; Vol. 1: 86–89.

4. “TEMPEST standard”. NATO SDIP-27, Level B. laboratory test standard for tactical mobile equipment/systems. – Available from: https://www.ia.nato.int/niapc/tempest/certification-scheme. – [Accessed: March 2021].

5. “TEMPEST standard”. NATO SDIP-27, AMSG NSTISSAM. – Available from: https://www.interelectronix.com/ru/tempest.html. – [Accessed: March 2021].

6. Horev, A. A. “Evaluation of the effectiveness of protecting computer equipment from information leakage through technical channels” (in Russian). *Spezyalnaya Technika*. 2007. Vol. 4.

7. Lutsenko, V. M. & Hudyakov, V. O. “Determining the vulnerability of information activities as part of the information security systems development” (in Ukrainian). *Legal, Regulatory and Metrological Support of Information Security System in Ukraine*. 2010; Vol. 2 (21): 49–54.

8. Lutsenko, V. M. & Yakymenko, B. M. “Research of methods of protection of local sources of incidental radiations of personal computers at creation of KSZI” (in Ukrainian). *Zahist Informacii*. Kyiv: Ukraine. 2011; Vol. 2 (51): 95–98.

9. Lutsenko, V. M., Arkhipov, O. E. & Hudyakov, V. O. “On the question of the use of shielding structures and cabins”. *Legal, Regulatory and Metrological Support of Information Security System in Ukraine* (in Ukrainian). 2002; Vol. 4: 66–77.

10. Lutsenko, V. M., Arkhipov, O. E. & Hudyakov, V. O. “Features of use of technical protection devices of the information against leakage due to incidental electromagnetic radiations and interferences” (in Ukrainian). *Legal, Regulatory and Metrological Support of Information Security System in Ukraine*. 2002; Vol. 4: 178–182.

11. Lutsenko, V. M., Arkhipov, O. E., Medvid, M. O. & Hudyakov, V. O. “Basic devices of automated measuring systems for side electromagnetic radiation research” (in Ukrainian). *Modern Problems and Achievements of Radio Engineering, Telecommunications and Information Technologies*. Zaporizzya: Ukraine. 13-15 April, 2006. p. 12–14.

12. Sudhama, A., Cutone, M., Hou, Y., Goel, J., Dale, S., Jacobson, N., Allison, R. & Wilcox, L. “Visually lossless compression of high dynamic range images: A large-scale evaluation”. *SID Symposium Digest of Technical Papers.* 2021; 49 (1): 1151–1154. DOI: https://doi.org/10.1002/sdtp.12106.

13. Mohona, S., Au, D., Kio, O., Robinson, R., Hou, Y., Wilcox, L. & Allison, R. "Subjective *assessment* of stereoscopic image quality: The impact of visually lossless compression". *12th International Conference on Quality of Multimedia Experience (QoMEX)*. Athlone, 2020. p. 1–6. DOI: https://doi.org/10.1109/QoMEX48832.2020.9123129.

14. Kubiak I., Przybysz A. "DVI (HDMI) and DisplayPort digital video interfaces in electromagnetic eavesdropping process". *International Symposium on Electromagnetic Compatibility – EMC EUROPE*. Barcelona: 2–6 September 2019. DOI: https://doi.org/10.1109/EMCEurope.2019.8872097.

15. Patnaik A., De S., Zhang Y.-J., Drewniak J. L., Wang C. & Pommerenke C. "EMI analysis of DVI link connectors". *IEEE Transaction on Electromagnetic Compatibility*. 2018; Vol. 60 Issue 1: 149–156. DOI: https://doi.org/10.1109/TEMC.2017.2702707.

16. "Digital video interface specification (Rev.1.0). VESA, digital display working group". 1999. 76 p. – Available from: https://glenwing.github.io/docs/DVI-1.0.pdf . – [Accessed: March 2021].

17. "HDMI specifications and programs. HDMI forum". – Available from: https://www.hdmi.org/spec/index. – [Accessed: March 2021].

18. "HDCP specification. Digital content protection consortium". – Available from: https://www.digital-cp.com/hdcp-specifications. – [Accessed: March 2021].

19. "DisplayPort specification". *Video Electronics Standards Association (VESA)*. – Available from: https://www.displayport.org. – [Accessed: March 2021].

20. Chen, F., Wong, K., Liao, X. & Xiang, T. "Period distribution of generalized discrete Arnold Cat Map". *Theoretical Computer Science*. 2014; Vol. 552: 13–25. DOI: https://doi.org/10.1016/j.tcs.2014.08.002.

21. Sinha R., San N., Asha B., Prasad S. & Sahu S .S. "Chaotic image encryption scheme based on modified Arnold Cat Map and Henon Map". *International Conference on Current Trends towards Converging Technologies (ICCTCT)*. Coimbatore: March 2018. DOI: https://doi.org/10.1109/ICCTCT.2018.8551137.

22. Shalaby, M., Saleh, M. & Elmahdy, H. "Enhanced Arnold's Cat Map-AES encryption technique for medical images". *2nd Novel Intelligent and Leading Emerging Sciences Conference (NILES)*. Giza: 24–26 October 2020. DOI: https://doi.org/10.1109/NILES50944.2020.9257876.

23. Progonov, D. O. & Kuschch, S. M. "Detection of stego images with data hidden in the transformation domain". Visn. NTUU KPI (in Ukrainian). *Ser. Radioteh. Radioaparatobuduv*. 2014; Vol. 57: 128–142. – Available from: http://radap.kpi.ua/radiotechnique/article/viewFile/809/759-radap.pdf. – [Accessed: March 2021].

24. Bhaskar H., Rohith S. & Mahesh M. "Two level image encryption scheme using Arnold Map and combined key sequence of logistic Map and Tent Map". *Twelfth International Conference on Wireless and Optical Communications Networks (WOCN)*. Bangalore: 9–11 September 2015. DOI: https://doi.org/10.1109/WOCN.2015.8064518.

25. Huang M.-Y., Huang Y.-M., Wang M.-S. "Image encryption algorithm based on chaotic maps". *International Computer Symposium (ICS2010)*. Tainan: 16–18 December 2010. DOI: https://doi.org/10.1109/COMPSYM.2010.5685529.

26. Brindha M. "Periodicity analysis of Arnold Cat Map and its application to image encryption". *International Conference on Inventive Computing and Informatics (ICICI)*. Coimbatore: 23–24 November 2017. DOI: https://doi.org/10.1109/ICICI.2017.8365401.

27. Prusty A., Pattanaik A. & Mishra S. "An image encryption & decryption approach based on pixel shuffling using Arnold Cat Map & Henon Map". *International Conference on Advanced Computing and Communication Systems*. Coimbatore: 19–21 December 2013. DOI: https://doi.org/10.1109/ICACCS.2013.6938729.

Conflict of interest: the authors declare no conflict of interest

Received 09.02.2021
Received after revision 12.03 .2021
Accepted 16.03.2021

ISSN 2617-4316 (Print)
ISSN 2663-7723 (Online)

DOI: https://doi.org/10.15276/aait.04.2021.7
УДК 004.056.53

Захист комп'ютерів від побічних електромагнітних випромінювань при формуванні зображень монітору

Володимир Миколайович Луценко [1)]
ORCID: https://orcid.org/0000-0001-7632-1730; lutsenkovn@ukr.net
Дмитро Олександрович Прогонов[1)]
ORCID: https://orcid.org/0000-0002-1124-1497; progonov@gmail.com. Scopus Author ID: 57201682654
Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського», просп. Перемоги, 37. Київ, 03056, Україна

АНОТАЦІЯ

Забезпеченню надійного захисту конфіденційних даних, що циркулюють в елементах критичної інформаційної інфраструктури державних установ та приватних організацій, сьогодні є надзвичайно актуально та важливою задачею. Особливий інтерес привертають методи попередження витоку конфіденційних даних за рахунок локалізації «небезпечних сигналів» тобто таких, які згідно визначенням в технічному захисті інформації несуть в собі інформативну компоненту і одночасно мають рівень сигналу більший, ніж дозволений для небезпечних сигналів в нормативних документах технічного захисту інформації. Підвищення енергії сигналів від персональних комп'ютерів зумовлено нарощуванням швидкості перемикань його транзисторних ключів. Сучасні пасивні методи екранування, такі, як при створенні персональних комп'ютерів в захищеному виконанні (аналогічно як в відомій програмі TEMPEST) вимагають, або великих витрат при екрануванні великих функціональних блоків комп'ютера, або малих витрат і технологічного спрощення при фрагментарному екрануванні його окремих малих за розміром елементів. Відповідно, є необхідність точного визначення місця джерел побічних електромагнітних випромінювань. Тому автори використовували мініатюрні саморобні антени і електричних (кулькова антена) і магнітних (датчик Холла) полів, що підключені до селективних вольтметрів. При такому підході значно скорочуються витрати на техніку, вартість робіт, кваліфікацію кадрів при доведенні персонального комп'ютера до захищеного виконання. Тобто, наведеним в роботі є економічно вигідний підхід до зменшення рівня побічних електромагнітних випромінювань персонального комп'ютера пасивним методом. побічних електромагнітних випромінювань визначаються прицільно від окремих елементів персонального комп'ютера, неекранованих ліній зв'язку між відеопроцесором та монітором, фрагментів трас електричних доріжок на платах та ін. Наведений, також, альтернативний підхід, при якому ведеться не стільки боротьба з сигналами від монітора, скільки з захистом змісту зображень шляхом спотворення зображення на моніторі. Використовуються методи скремблювання зображення з використанням перетворення Арнольда, спрямовані на випадкове «перемішування» строк в кожному кадрі.

Ключові слова: побічні електромагнітні випромінювання; криптоперетворення; відеозображення; інформація з обмеженим доступом

ABOUT THE AUTHORS

Volodymyr M. Lucenko – Candidate of Engineering Sciences, Associate Professor, Associate Professor of the Department of Information Security. Igor Sikorsky Kyiv Polytechnic Institute. 37, Peremohy Av., Kyiv, 03056, Ukraine
ORCID: https://orcid.org/0000-0001-7632-1730; lutsenkovn@ukr.net
***Research field*:** Iinformation security; artificial intelligence; biological and medical cybernetic; neurocomputer technology

Володимир Миколайович Луценко – кандидат техніч. наук, доцент, доцент каф. Інформаційної безпеки. Київський політехнічний інститут імені Ігоря Сікорського, пр. Перемоги, 37. Київ, 03056, Україна

Dmytro O. Progonov – Candidate of Engineering Sciences, Associate Professor, Associate Professor of the Department of Information Security. Igor Sikorsky Kyiv Polytechnic Institute, 37, Peremohy Av., Kyiv, 03056, Ukraine
ORCID: https://orcid.org/0000-0002-1124-1497; progonov @gmail.com. Scopus Author ID: 57201682654
***Research field*:** Digital media steganalysis; digital image forensics; machine learning; advanced signal processing

Дмитро Олександрович Прогонов – кандидат техніч. наук, доцент, доцент каф. Інформаційної безпеки. Київський політехнічний інститут імені Ігоря Сікорського, пр. Перемоги, 37. Київ, 03056, Україна