32nd European Modeling & Simulation Symposium
17th International Multidisciplinary Modeling & Simulation Multiconference

ISSN 2724-0029 ISBN 978-88-85741-44-7 © 2020 The Authors.
DOI: 10.46354/i3m.2020.emss.025

Evaluation of information protection against leakage through the compromising electromagnetic emanations during data exchange via USB interface

Denis Radchenko[1], Anton Tokarev[1], Alexander Makarov[2,3], Artem Gulmanov[2], and Kirill Melnikov[2,3,*]

[1]Voronezh State Technical University, Moscow Avenue 14, Voronezh, 394026, Russia
[2]National Research University "Moscow Power Engineering Institute", Krasnokazarmennaya st. 14, Moscow, 111250, Russia
[3]National Research Tomsk State University, Lenin Avenue 36, Tomsk, 634050, Russia

[*]Corresponding author. Email address: kirill.a.melnikov@mail.ru

Abstract

The paper deals with the problem of estimating the information security of data exchange through the USB interface with regard to compromising electromagnetic emanations. There is proposed a specialized procedure for detecting and measuring the intensity of informative components of compromising electromagnetic emanations. It is based on the formation of the specialized in-formation packets in the data exchange channel, their transmission being accompanied by the appearance of radio emissions with a linear spectrum. The concentration of power generated by compromising electromagnetic emanations in a set of narrow-band radiations provided by such testing facilitates their detection against the background of other components of compromising electromagnetic emanations having the other sources of origin. Recommendations are given on the choice of testing length in order to maximize the probability of capturing signal samples.

Keywords: Radio monitoring; compromising electromagnetic emanations; detection of informative components; interception of information; USB interface

1. Introduction

1.1. Peculiar properties of compromising electromagnetic emanations

Compromising electromagnetic emanations (CEE) are unwanted radio emission, accompanying information processing in PC units and other technical means (Rembovsky, Ashikhmin, Kozmin, and Smolskiy, 2009). CEE occur, for example, when performing operations such as

- displaying information on the monitor screen;
- keyboard input;
- writing information to data storage;
- reading information from data storage;
- data transmission in communication channels, etc.

The characteristics of the emerging CEE are interrelated with the processed or transmitted data. Therefore, it is possible to recover (intercept) the processed information by analyzing the changes in these emanations with the intelligence receiver applied. In order to check the danger of information leakage through such a technical channel, it is necessary to control the intensity of informative components of CEE. This creates the need to develop algorithms for CEE detection.

1.2. Research into the detection and interception of CEE and its importance

CEE have a low intensity and even with special equipment their interception is a difficult technical task. However, in the rare cases when a certain functioning channel of information creates leakage due to a combination of random factors, the danger of the CEE phenomenon is extremely high because of its invisibility. In this regard, since the openly published paper by Van Eyck (1985), information security specialists pay considerable attention to the CEE checking.

The methodology for calculating and measuring the intensity of electromagnetic fields generated by CEE, as well as the recommendations for calculating the radiuses of areas secure from information leakage can be found, for example, in the studies by Sudarikov and Romashchenko (2011), Lykov and Syagaev (2012), Korolev (2013), Zidong and Yuanhui (2014). Useful information for calculating the attenuation of the CEE on the objects of computerization can be found in the papers by Asotov et al (2015a, 2015b, 2017). A separate group of studies is devoted to the development and description of radio monitoring complexes intended for the analysis of CEE, as well as to detailing the algorithms for assessing the protection of information from leakage through the CEE channel (Buzov, Kalinin, and Kondrat'ev, 2005; Tupota, Kozmin, and Tokarev 2006; Horev 2007; Cazanaru, Coşereanu, and Szilagry, 2011; Frankland, 2011; Filippovich, 2014; Ulas et al, 2014). A number of studies devoted to the issues of intercepting information entered from the keyboard (Vuagnoux and Pasini, 2009; Vuagnoux and Pasini, 2010; Dmitryiev, Stepanyan, and Fisenko, 2013; Ahsan, Islam, and Islam, 2014; Sokolov, Astretsov, and Kobyakov, 2015) or transmitted via USB 2.0 interface (Nowosielski and Wnuk, 2014). Nevertheless, the methods of security assessment presented in common publications remain poorly detailed and very time-consuming, especially in terms of testing the devices and interfaces characterized by the asynchronous nature of data transmission. From this point of view, the estimation of how secure the particular information is from the interception through the CEE channel when recording or reading information to and from a variety of data storage devices is particularly interesting and requires attention. However, before specifying the details of the studies arising from the peculiarities of the processes of data reading and writing from/to information carriers, it is necessary to determine the technological fundamentals of the CEE dangerous component detection.

2. The method to detect the informative components of CEE

2.1. Comparative analysis of approaches to the problem of detecting the components of CEE

The approaches used to study the CEE components can be divided into two groups, at least, depending on their functions and functionality as well as on the technological limitations imposed on the data collection procedures.

In some cases, the purpose of research is to study the mechanisms for CEE causation and their patterns characteristic for different kinds of equipment. For example, one wants to determine the possible ways to reduce the level of spurious emissions produced by a particular class of devices. Such studies presuppose the possibility, and even the necessity, of the physical access of the researcher to the individual blocks and nodes of the tested device. In this case, the focus is on the study of the relations between the electrical signals logged at the internal contacts of the tested devices and the radio emissions that appear in a particular frequency band. Such researches include, for example, a paper presented by Lidstedt (2019), where the value of the normalized cross-correlation between the received radio emissions and the signals taken from the contacts of the control circuits of the analyzed device is considered as a “tool” for CEE detection.

Another group of studies includes the ones where a certain device generating CEE is used as it is. That is, in this case, no direct physical connection to the device nodes is possible, and the purpose of the study is to estimate the level of security and protection that the information procession carried out by such a device provides against the malicious interception engineered in technical intelligence environments. A list of approaches and methods that are involved in such conditions in order to reveal the CEE informative components was rather fully presented by Zhigunova (2009), for example. This list includes such five methods as the spectral panoramas comparison method, the audio-visual method, the expert method, the correlation-parametric and the correlation methods. The first of them is the most universal and is based on the development of the specialized (possibly, artificial) operating modes for different units of the tested equipment. In these modes, the signals providing information processing are strictly periodic. In such conditions, on the air, the informative components of CEE of the tested units are concentrated in the form of the narrow-band radio emissions with a linear spectrum that makes them more distinct at the background of the natural additive noise. The operation of many software and hardware systems for CEE detection is based on this technique.

It should be noted, however, that, in a dynamically changing radio environment, when detecting the CEE components in wide frequency ranges, the spectral panoramas comparison method makes it possible to reveal multiple "false targets", and, therefore, it is usually used as a means of generating a set of "suspicious" frequencies only. During the further phases of the study, each component of this set should be separately retested for containing informative content by means of the other methods mentioned above. As a result, the procedure for detecting the informative components of CEE appears to be rather lengthy and laborious.

2.2. Designing the equipment for the detection of the CEE informative components

Thus, in order to detect the CEE components in wide frequency ranges, there should be provided the switching between the test modes of the examined equipment units that are characterized by the periodicity of information signals. This allows us to propose an alternative method for detecting the CEE informative components (Tokarev et al, 2016). It is based on the arrangement and maintenance of the software control of the operating mode of the tested equipment units, providing automatic switching of the test mode with a periodic type of the signals on and off. Detection of the CEE informative components by alternating change of the operating modes of the tested unit can be carried out, only if there have been accumulated R_y time series of the received signals that correspond to the active mode (marked by the periodic behavior of the processing signals), together with R_z time series of the received signals that correspond to the passive mode. Next, for each time series there should be calculated the periodograms

$$X_{(r)}(n) = \left|\dot{c}_{(r)}(n)\right|,$$

where $\dot{c}_{(r)}(n)$ is the discrete complex spectrum for the r-th time series calculated by means of the fast Fourier transformation

$$\dot{c}_{(r)}(n) = \frac{1}{N}\sum_{k=0}^{N-1} s_{(r)}(k)w(k)\,exp\left(-j2\pi\frac{nk}{N}\right),$$
$$0 \le n \le N-1.$$

Here k is the ordinal number of a sample out of the time series $s_{(r)}(k)$; $w(k)$ are the samples of the weight function used to reduce the effect of the spectrum components infiltration upon the neighboring frequencies; n is the reference number that determines the frequency in the periodogram $X_{(r)}(n)$. Based on the values of the n-th samples obtained for the active mode of operation of the tested equipment, it is necessary to form a vector $\vec{y} = \left\{y_{(1)}(n), y_{(2)}(n), \ldots, y_{(R_y)}(n)\right\}$. Similar values obtained in the passive operating mode of the tested equipment should be combined into a vector $\vec{z} = \left\{z_{(1)}(n), z_{(2)}(n), \ldots, z_{(R_z)}(n)\right\}$. To check the belonging of the emanations appearing at the n-th frequency to the informative components of the CEE, the statistics proposed by Tokarev et al (2016) should be used:

$$Q_{yz}(n) = \frac{E_S(n)}{E_N(n)} \underset{H_0}{\overset{H_1}{\substack{>\\<}}} c, \tag{1}$$

where

$$E_S(n) =$$
$$= \sum_{r=1}^{R_y} y_r^2(n) + \sum_{r=1}^{R_z} z_r^2(n) - \frac{1}{R_y + R_z}\left[\sum_{r=1}^{R_y} y_r(n) + \sum_{r=1}^{R_z} z_r(n)\right]^2,$$

$$E_N(n) =$$
$$= \sum_{r=1}^{R_y} y_r^2(n) - \frac{1}{R_y}\left[\sum_{r=1}^{R_y} y_r(n)\right]^2 + \sum_{r=1}^{R_z} z_r^2(n) - \frac{1}{R_z}\left[\sum_{r=1}^{R_z} z_r(n)\right]^2,$$

and c is the selected decision threshold. The studies held by Tokarev, Pitolin, Beletskaya, and Bulgakov (2016) show that the statistics (1) are very sensitive and allows correct recognition of even very weak CEE informative components. Thus, it is recommended to select the decision threshold from the criteria

$$Q_{yz}(n) = 1.15 \le c \le 1.5.$$

2.3. The problem of creating test modes with the periodic signal behavior for the tested blocks that perform asynchronous information transfer

Summing up, one should note that if the blocks tested for information leakage through the CEE allow performing their switching from the passive mode to the mode of periodic signal processing, the control of the CEE components created by these blocks can be carried out very effectively. But for blocks carrying out the asynchronous packet data transfer it is very difficult to facilitate such a mode. In the further part of the paper we will discuss the possibility and the technology of creating such a mode in relation to the recording or reading of information from data storage with USB interface.

3. The signal structure when working with the USB interface

3.1. The peculiarities of the USB interface

Physically, the USB interface is a four-wire bus. Information exchange is carried out through the two differential signal lines "D+" and "D-" with NRZI coding. The other two lines are used to supply +5 V voltage to the devices. The range of values of the voltage amplitude in the differential pair for Low-Speed and Full-Speed modes ranges from 0.8 to 2.5 V, and for High-Speed from "minus" 50 to 500 mV (nominal value is equal 200 mV). The resistance of the lines is 100 Ohms. The bit width of the interface is 1 bit

(Universal Serial Bus Specification, 2000).

An informative signal is transmitted through the interface as a serial potential NRZI (Non Return To Zero Invert) code. When transmitting informative "1" by the differential pair, the current direction does not change, informative "0" corresponds to the change of the current direction to the opposite. Therefore, to create a periodic structure signal in the data lines, a sequence of zero bytes should be passed through them. The clock frequency of the signal in the interface depends on interface standard and the device operation mode; the frequency of informative pulses generated by the test is 1/2 of the clock frequency of the interface. The parameters of the interfaces are defined by the standard. Parameters of informative signals are given in Table 1. Actual frequency values may differ slightly from those shown in the Table 1.

Table 1. The parameters of the informative signals for different interface operation modes.

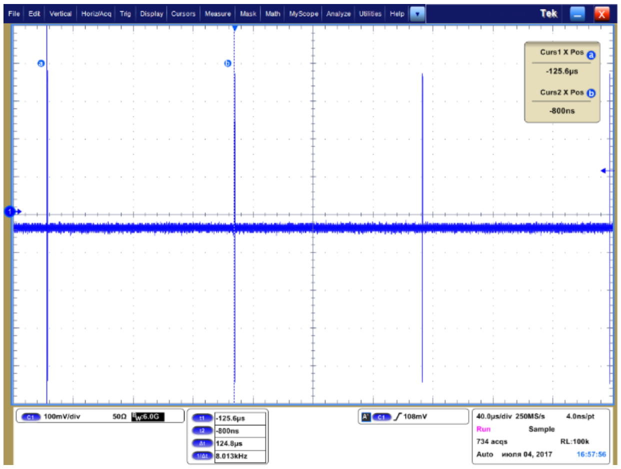
Interface operation mode	Clock frequency of the interface, MHz	Clock frequency of the informative pulses, MHz	Pulse duration τ_{pulse}, ns	Standard
Low-Speed	up to 1.5	up to 0.750	666.7	USB 1.0
Full-Speed	up to 12	up to 6	83.33	USB 1.1
High-Speed	up to 480	up to 240	2.08	USB 2.0

3.2. Creating an active (test) mode when writing or reading data to and from USB data storage

In order to understand the physical basis of creating a test mode, it is necessary to take into account that the data is transmitted through the interface in packets (for example, 512 bytes long for Full-Speed) in accordance with a certain exchange Protocol. Moreover, even in the absence of explicit data transmission operations, service information packets are transmitted over the signal lines (Universal Serial Bus Specification, 2000). In particular, when connecting a flash drive without activating the processes of reading and writing information at the physical level, you can observe the relatively periodic sequence of SOF (Start of Frame) packets shown in Figure 1. These synchro packages are displayed on a larger scale in Figure 2. As it can be seen from Figure 2, synchro packets have a rather complex shape and duration of about 0.12 µs, and it is not possible to remove them from the signal lines (in accordance with the standard) during normal operation of the USB interface.

When data exchange between PC and external storage is activated, data packets appear on signal lines in addition to synchro packets. In Figure 3, it is presented a part of the activity of the signal lines, reflecting the coexistence on these lines of service packages and data packages. It should be borne in mind that even with an infinite write cycle, the signal lines are not 100% busy and the transmission intervals of the data packets alternate with the transmission intervals of only the service clock packets. A similar variant of signal lines occupancy that is observed in the course of writing data to a flash drive, shown in Figure 4.

So, when the procedure of writing data to an external data storage is starting, a complex, batch mode of signal exchange in the signal lines of the USB interface is still maintained. Throughout the data package, consisting only of zero characters, in the signal lines the oscillation is really formed close by the shape to the meander and having a frequency (for USB 2.0) 240 MHz (see Figure 5). However, these packets are separated by extended pauses and sets of service sync packets.



Curs1 X Pos -125.6µs
Curs2 X Pos -800ns

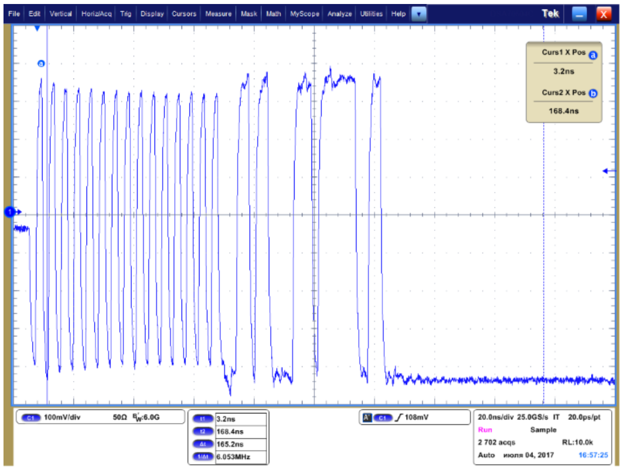
C1 100mV/div 50Ω BW:6.0G

t1 -125.6µs
t2 -800ns
Δt 124.8µs
1/Δt 8.013kHz

A C1 ∫ 108mV

40.0µs/div 250MS/s 4.0ns/pt
Run Sample
734 acqs RL:100k
Auto июля 04, 2017 16:57:56

Figure 1. Narrow vertical highlights correspond to service synchro packets transmitted at intervals of about 125 µs



Curs1 X Pos 3.2ns
Curs2 X Pos 168.4ns

C1 100mV/div 50Ω BW:6.0G

t1 3.2ns
t2 168.4ns
Δt 165.2ns
1/Δt 6.053MHz

A C1 ∫ 108mV

20.0ns/div 25.0GS/s IT 20.0ps/pt
Run Sample
2 702 acqs RL:10.0k
Auto июля 04, 2017 16:57:25

Figure 2. Detailed view of synchro packages

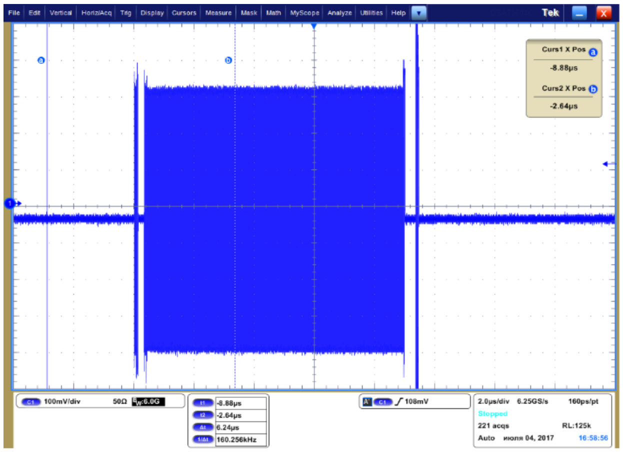


Figure 3. Appearance of the information package when recording information on flash data storage

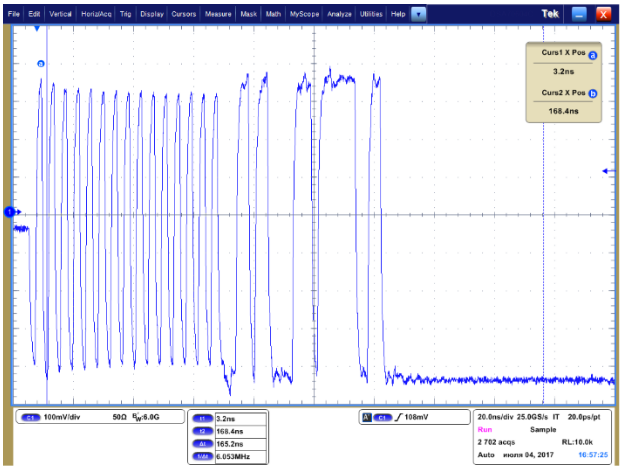


Figure 4. The exchange of synchro packets during recording information on flash-drive data storage

If instead of zero bytes one sends packets consisting only of units, the character of the generated signals will change. The peculiarities of the coding procedure will lead to the appearance of a meander with the approximately 6 times lower frequency (see Figure 6).

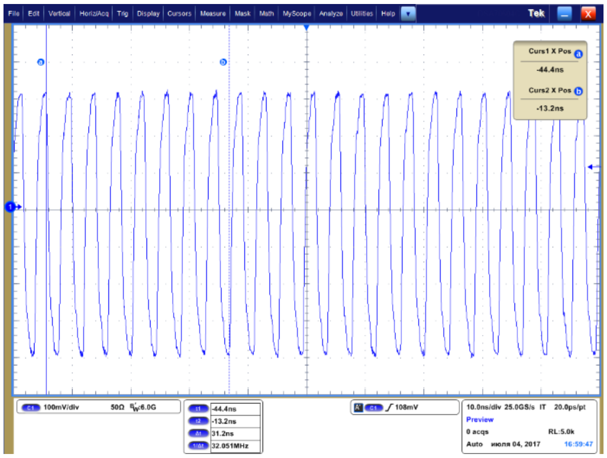


Figure 5. The structure of the data packet when transmitting a sequence of zero bytes

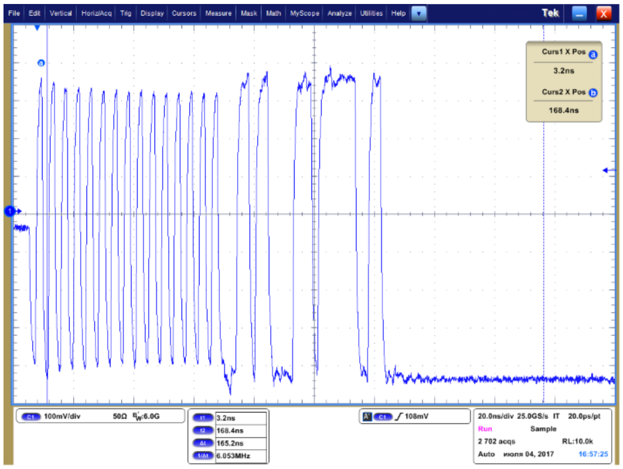


Figure 6. The structure of the data packet when transmitting a sequence of zero bytes

The behavior of data exchange in read mode is not different from the above demonstrated.

4. Results and Discussion

4.1. The procedure for evaluating the information security of writing and reading data from data storage with USB interface

The above information formed the basis for the operation of the procedure for checking data storage devices with a USB interface, which is part of the special software SMO-RAPIRA, designed to work with radio monitoring complexes produced by the research and production company "IRCOS" (Moscow, Russia). This software is designed for the comprehensive testing of the computerization objects focusing on determining the level of protection the information has against the leakage through the CEE (Rembovsky, Ashikhmin, Kozmin, and Smolskiy, 2018).

The test "tst_usbdrive" can be used for testing flash drives, card readers, etc. When several drives are connected to the system, their testing is carried out in series under the manual control of the operator. Since the information exchange is involved, the data storage device and PC as the transmitter and the receiver of information, the object of testing is "bundle": PC and data storage. To carry out the test, you should install a testing program on the PC that participate in the exchange and operates in the environment of Microsoft Windows operating systems, starting from XP to Windows 10 x32 or x64. You must provide permission for writing data to the root directory of the selected logical drive of the tested drive, the size of the free space on which must be at least 1 MB.

In the immediate environment of the inspected PC, the receiving antenna of the radio monitoring complex should be placed, which will be used to search for informative components of CEE.

After starting the test "tst_usbdrive" the operator needs to

a) open the USB drive test settings and specify the logical partition that belongs to the target physical data storage;

b) specify "fill Type" = "Zeros" to generate the test signal with the highest possible frequency;

c) specify the size of the data buffer, the recommended value of which is at least 256 KB.

During estimation of the information security of data exchange via USB interface, it is recommended to use sufficiently large size of the data buffer, the length of the test should be at least 1 minute to collect data in a wide band of radio frequencies, and there should be carried out the switching from the active to the passive operating modes of the test to maximize the probability of capturing signal samples corresponding to the moments of information data packets transmission.

In parallel with the activation of the "tst_usbdrive" test, the radio monitoring system operating under SMO-RAPIRA software starts analyzing the radio environment, accumulating data time series for a wide band of radio frequencies during periodic switching of the tested units from the passive state to the active state and back. Upon completion of the data collection stage, the accumulated time series are converted into the frequency domain and, for the sets of samples characterizing the change in the intensity of the spectrum components at different frequencies, the procedure for checking the belonging of these samples to the informative components of CEE is performed in accordance with the recommendations of section 1.3 of this paper.

If the informative components of CEE can be detected and their intensity recorded by the radio monitoring system significantly exceeds the background noise, it is necessary to evaluate the danger of detected CEE from the standpoint of the possible information leakage. The specific mechanism of such an evaluation depends on the requirements for information security, but the approaches described, for example, in the papers by Tupota, Kozmin, and Tokarev (2006) as well as Horev (2007) can be recommended as a basic recommendation. At the same time, for the correct application of the calculation ratios proposed in these studies, it is necessary to take into account the correction for the packet behavior of data exchange when using the USB interface. For this purpose, based on the information from the test "tst_usbdrive", it is necessary to compare the amount of data transmitted or read in 1 second from the data storage V_{real} with the maximum possible amount of such data

$$V\ 1/\tau_{pulse}{}_{max}$$

that could be transmitted (received) at the same time, if the data exchange went without pauses, in a continuous mode (see Table 1).

A smaller amount of real data exchange is associated with the existence of pauses between data packets. At the same time, the components of CEE registered by the radio monitoring complex reflect the power of these packets together with all the pauses accompanying the data transmission process, and therefore the real power of the packet signals, which could be registered with accurate synchronization of the data collection process with the moments of packet formation, will be noticeably greater.

Thus, in the analysis of information protection against the leakage through the CEE, the power of informative components of CEE registered by the radio monitoring complex should be increased by

$$k = V_{max}/V_{real}\ 1/V_{real}\tau_{pulse}\ [\text{times}].$$

5. Conclusions

The proposed algorithm for detecting and testing the informativeness of the CEE components is focused on the use of broadband radio monitoring equipment and the creation of quasi-harmonic data packets at the data exchange buses. Such an artificial mode contributes to the appearance of an emanation of a set of narrow-band spectrum lines on air, accompanying the process of writing or reading information. This approach allows for more accurate measurements of the components of the CEE against the background noise.

The solutions proposed and described in the paper can be useful for information security specialists in evaluation the protection of information at the computerization objects against the leakage through the CEE.

Funding

This study was financially supported by the Ministry of Science and Higher Education of the Russian Federation (research project No. FSWF-2020-0022).

References

Ahsan, A., Islam, R., and Islam, A. (2014). A countermeasure for compromising electromagnetic emanations of wired keyboards. *Proceedings of 2014 17th International Conference on Computer and Information Technology (ICCIT)*, pp. 241-244, December 22-23, Dhaka (Bangladesh).

Asotov, D.V., Matveev, B.V., Chernoyarov, O.V., and Lysina, E.A. (2015a). Radio waves attenuation model for a ray approximation. *Proceedings of 2015 International Siberian Conference on Control and Communications (SIBCON)*, pp. 1-5, May 21-23, Omsk (Russia).

Asotov, D.V., Matveev, B.V., Faulgaber, A.N., and Salnikova, A.V. (2015b). The exact and approximate task solution of a ray tracing at their transition in a medium with finite conductivity. *Proceedings of 25th International Crimean Conference Microwave and*

Telecommunication Technology (CriMiCo-2015), vol. 2, pp. 1200-1201, September 6-12, Sevastopol (Russia).

Asotov, D.V., Salnikova, A.V., Matveev, B.V., and Chernoyarov, O.V. (2017). The algorithms for the ray tracing based on the analytical solutions. *Proceedings of 2017 2nd International Conference on Mechatronics, Control and Automation Engineering (MCAE2017)*, pp. 186-191, September 17-18, Shenzhen (China).

Buzov, G.A., Kalinin, S.V., and Kondrat'ev, A.V. (2005). *Protection from information leakage through technical channels* [in Russian]. Moscow, Russia: Goryachaya Liniya-Telekom.

Cazanaru, D., Coşereanu, L., and Szilagry, A. (2011). Evaluation of the compromising radiation by electromagnetic compatibility tests. *University Politehnica of Bucharest Scientific Bulletin-Series A-Applied Mathematics and Physics*, 73 (2), 185-192.

Dmitryiev, U.A., Stepanyan, A.B., and Fisenko, U.K. (2013). Control of protection of confidental information for input from the PC keyboard [in Russian]. *Artificial Intelligence*, (3), 549-553.

Frankland, R. (2011). Side channels, compromising emanations and surveillance: Current and future technologies. *Technical Report RHUL-MA-2011-07*. Retrieved from http://www.rhul.ac.uk/mathematics/techreports

Horev, A.A. (2007). Assessing the effectiveness of the protection of the support technologies [in Russian]. *Special Equipment*, (2), 48-60.

Korolev, M.V. (2013). Method of calculation of the zone boundary protection of information in the far field radiation source [in Russian]. *IT Security*, 20(1), 58-62.

Lidstedt, J. (2019). *Evaluating compromising emanaons in touchscreens*. Master thesis. Linköping, Sweden: Linköping University.

Lykov, Y.V., and Syagaeva O.O. (2012). The analysis of the sources of the compromising electromagnetic emanations in a modern PC [in Russian]. *Radio Engineering. All-Ukrainian Interdepartmental Scientific and Technical Collection*, 169, 196-207.

Nowosielski, L., and Wnuk, M. (2014). Compromising emanations from USB 2 interface. *Proceedings of Progress in Electromagnetics Research Symposium (PIERS)*, pp. 2666-2670, August 25-28, Guangzhou (China).

Rembovsky, A.M., Ashikhmin, A.V., Kozmin, V.A., and Smolskiy, S.M. (2018). *Radio monitoring automated systems and their components*. New York, USA: Springer International Publishing.

Rembovsky, A.M., Ashikhmin, A.V., Kozmin, V.A., and Smolskiy, S.M. (2009). *Radio monitoring. Problems, methods, and equipment*. New York, USA: Springer.

Sokolov, R.I., Astretsov, D.V., and Kobyakov, V.U. (2015). Potential detection spectral component of compromising emanations signal USB keyboard interface [in Russian]. *Proceedings of 2nd International Conference of Students, Postgraduates and Young Scientists "Information technologies, telecommunications and management systems"*, pp. 152-160, December 14-15, Ekaterinburg (Russia).

Sudarikov, A.V., and Romashchenko, M.A. (2011). The review of technical devices for measuring the characteristics of electromagnetic fields [in Russian]. *Proceedings of International Symposium "Reliability and quality"*, vol. 2, pp. 213-215, May 23-31, Penza (Russia).

Tokarev, A.B., Pitolin, V.M., Beletskaya, S.Y., and Bulgakov, A.V. (2016). Detection of informative components of compromising electromagnetic emanations of computer hardware. *Int. J. of Control Theory and Applications*, 9 (30), 9-19.

Tupota, V.I., Kozmin, V.A., and Tokarev, A.B. (2006). Application of the multifunctional complex ARC-D1TI for evaluating information protection from leaking over the CEE channel [in Russian]. *Special Equipment*, (1), 38-46.

Ulas, C., Sahin, S., Memisoglu, E., Asık, U., Karadeniz, C., Kılıc, B., and Sarac, U. (2014). Automatic TEMPEST test and analysis system design. *Int. J. on Cryptography and Information Security*, 4 (3), 1-12.

Universal Serial Bus Specification (2000, April 27). Retrieved from https://www.usb.org/documents

Vuagnoux, M., and Pasini, S. (2009). Compromising electromagnetic emanations of wired and wireless keyboards. *Proceedings of 18th USENIX Security Symposium*, pp. 1-16, August 10-14, Montreal (Canada).

Vuagnoux, M., and Pasini, S. (2010). An improved technique to discover compromising electromagnetic emanations. *Proceedings of 2010 IEEE International Symposium on Electromagnetic Compatibility (EMC)*, pp. 121-126, July 25-30, Fort Lauderdale (USA).

Wim van Eck, (1985). Electromagnetic radiation from video display units: An eavesdropping risk? *Computers & Security, 4*(4), 269-286.

Zhigunova, Y.A. (2009). *Methodological and software support for controlling and monitoring the identification of informative harmonics of the hardware produced electromagnetic radiation*. Ph.D. thesis [in Russian]. Irkutsk, Russia: Irkutsk State Transport University.

Zidong, Z., and Yuanhui, Y. (2014). Quality evaluation model of information reconstruction via electromagnetic emanation. *TELKOMNIKA Indonesian Journal of Electrical Engineering*, 12(3), 1960-1964.