# ACTIVE METHODS AND MEANS OF INFORMATION PROTECTION AGAINST LEAKAGE THROUGH CHANNELS OF SIDE ELECTROMAGNETIC RADIATION AND INTERFERENCE

**[1]Foziljonov Kh.I., [2]Faziljanov I.R.**
[1,2]Tashkent University of Information Technologies named after Muhammad al-Khwarizmi
***https://doi.org/10.5281/zenodo.7818479***

***Abstract.*** *This paper discusses active methods and means of protecting information from leaks through the channels of side electromagnetic radiation and interference (SERI). The main disadvantages of active methods of information protection are considered. The main technical parameters of noise generators are given. A block diagram of the complex for intercepting side electromagnetic radiation (SER) is proposed.*

***Keywords:*** *side electromagnetic radiation, interference, frequency spectrum, information security, noise generator, jamming, shielding, SDR receiver.*

The development of new information technologies is accompanied by such negative phenomena as industrial espionage, computer crimes and unauthorized access to secret, official and confidential information [1-2]. Therefore, the protection of information is the most important task for states and organizations.

One of the most probable threats of information interception in data processing systems is considered to be a leak due to the interception of side electromagnetic radiation and interference, created by technical means [3].

An analysis of literary sources has shown that all communication ports of computer equipment, such as the PS / 2 port connector [4], USB (universal serial bus ports or peripherals) [5,6], RJ45 modular connector [7], video signals from VGA, DVI, HDMI and other display ports [8–9] or RS232 serial port [10]. Output devices such as printers [11–15] and video projectors [16] generate electromagnetic radiation during operation (information exchange). These radiations are parasitic, i.e. SER. This channel of information leakage is called spurious electromagnetic radiation and interference. In Europe and Canada, the term "compromising emanation" is used - compromising radiation. In the US, the term "TEMPEST" is used.

SER exist in the frequency range from a few Hz to several GHz and are capable of transmitting (propagating) messages processed in automated systems [17]. The propagation range of SER is estimated at tens, hundreds, and sometimes thousands of meters [18-19].

By receiving and decoding these radiations, it is possible to obtain information about the information processed in the computer [20–22].

The greatest danger from the point of view of information leakage is the radiation of the video system of a personal computer, which includes a monitor and a video adapter.

To receive a SER video system of a personal computer, one needs a computer or laptop with special software [23–25], an SDR receiver with an antenna [26]. Figure 1 shows a block diagram of the complex for intercepting SER [27].


Figure 1. Block diagram for PEMI interception: 1-computer or laptop with special software for decoding SER radiation; 2-SDR receiver for receiving SER radiation; 3- SER source

Figure 2 shows the spectrum of the SER signal. Figure 3.a. the image on the computer monitor screen is shown, and Figure 3.b shows the captured and restored image.

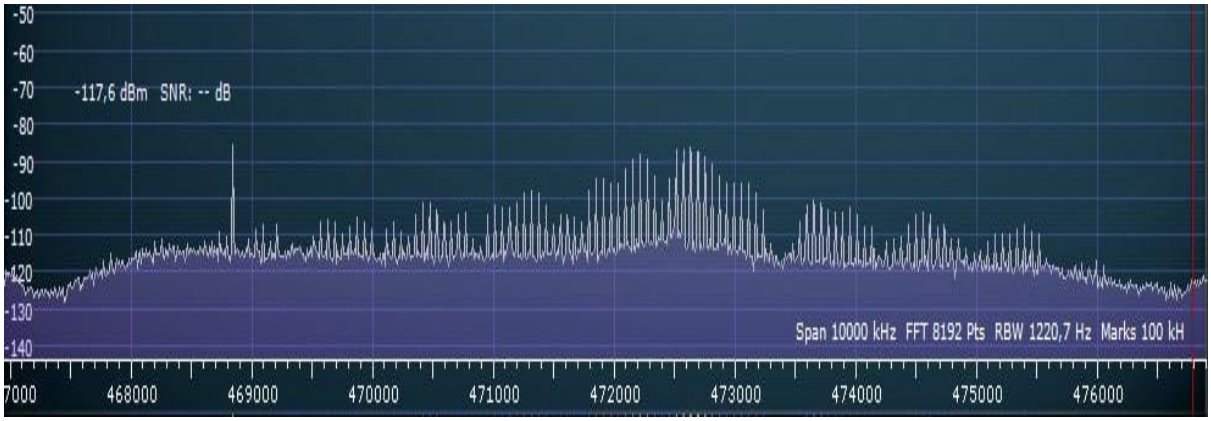


Figure 2. Spectrum of the SER signal


*a* *b*

Figure 3. Demonstration of the image on (a) - on the monitor screen of the attacked computer; (b) - intercepted and reconstructed image.

In the literature, there are three methods of protection against SER: passive, active, and also combined. The last of these methods includes the main activities of the two previous ones [1-3,29].

The passive method consists of shielding the radiation source, placing the radiation source in a shielded cabinet, or shielding the room as a whole.

The active protection method involves the use of special jammers that provide masking of SER from computer equipment by generating and emitting an electromagnetic noise field in a wide frequency range.

The active method of protection involves the use of special jammers that provide masking of SER from computer equipment by forming and emitting an electromagnetic noise field in a wide frequency range.

To protect objects, as well as individual protection of computer equipment (CT), taking into account the criterion of efficiency / cost, active protection methods, also called active radio masking (RM) methods, are widely used. The active methods of protection themselves can be divided into:

- statistical method;
- method of "common-mode interference";
- energy (power);

The statistical method of RM consists in changing the probabilistic structure of the signal received by the reconnaissance receiver of reconnaissance equipment by emitting a specially formed masking signal, the level of which does not exceed the level of informative SER of CT equipment. However, the practical implementation of the method has certain difficulties and features.

In the method of "common-mode interference" pulses of random amplitude are used as a masking signal, coinciding in shape and time with the information signals of SER. In this case, signal reception loses its meaning, since the a posteriori probability of the presence and absence of a signal remain equal to their a priori values. The indicator of security here is the maximum total error probability at the border of the controlled zone. However, at the moment there is no equipment and approved methods for measuring the above value, which does not allow implementing this method in practice.

In the case of energy masking by the "white noise" method, a broadband noise signal is emitted near computer equipment with an energy spectrum close to uniform over the entire protected frequency range and exceeding the maximum SER level from a working CT.

The disadvantages of this method include hardware difficulties in the implementation of Gaussian noise interference with high noise quality in a wide radio range of protected frequencies, as well as the creation of radio interference to electronic equipment located close to the protected CT facilities and the constant emission of electromagnetic interference can adversely affect living organisms.

At present, it is the energy method that has found wide application in various noise generators. The authors analyzed the existing means of protection against SER. The results of the analysis are shown in Table 1 where the main technical parameters of the jammers are given.

Table 1.

Main parameters of noise generators

| Device name | Frequency range | Noise level adjustment range | Supply voltages | Control options | Generator unit dimensions, mm | Antenna type |
|---|---|---|---|---|---|---|
| SEL-111K "Chiffon" | 10 kHz - 3 GHz | 0 to - 30 dB | 220 V | from panel, wired remote | 225x150x75 | telescopic antenna |

| | | | | | | |
|---|---|---|---|---|---|---|
| shtora-4 | 0.1 - 2500 MHz | 0 to - 20 dB | 220 V | from the panel | 220 x 135 x 135 | telescopic antenna |
| GSh-2500 | 0.1 - 2000 MHz | - | 220 V | from the panel | 700 x 600 x 35 | Frame, pin |
| Grom-ZI-4B | 0.009 - 2000 MHz | 0 to - 20 dB | 220 V | from the panel | 140x230x50 | SI-5002.1 |
| LGSh-501 | 0.001-1.8GHz | - | 220 V | from the panel | 230x100x45 | telescopic antenna |
| GSh-K-1000M | 0.1-1000 MHZ | - | 5 V | - | 7165x125x25 | - |
| GSh - 111B | 10 kHz - 1.8 GHz | 0 to - 30 dB | 220B | from panel, wired | 225x150x75 | telescopic antenna |
| Starkad-32 | 0.01 - 1800 MHz | 0 to - 25 dB | from the LAN | Remote control, | 210x140x36 | Frame IS32-01 |

Analysis of works related to the protection of information from SER by the method of active interference.

In [30], the authors presented SDR-based devices that use a multi-carrier modulation scheme. As a result of this, the SDR device can generate at least two signals, the first signal overlaps the SER frequency band, and the second signal is a pseudo-signal, this signal serves as a false signal to the interceptor receiver.

In [31], the authors developed a mobile jammer that connects to a PC via a VGA port. The interference signal is generated from the PC video interface signals. Radiated interference from the generator masks SER.

In [32], the authors developed a mobile jammer powered by a computer USB port. The device consists of several generators of electromagnetic interference. During operation, the generators form a barrage (masking) interference.

In [33-35], the authors propose the protection of computer information using systems of spatial and linear noise. Consider some types of devices for protecting information from leakage through PEMIN channels.

In [36-37], the authors propose a way to protect the processed information by means of computer technology by noise informative spurious electromagnetic radiation and interference.

Based on the results of the analysis, the following conclusions can be drawn:

• Most of the technical means of protection against SER work on the basis of the RM energy method;

• A powerful source of radiation is not good for human health;

• The presence of a masking signal indicates the presence of protected information;

• From the analysis of devices, literature and patents, it becomes obvious that when protecting information from SER CT, such interference as aiming, imitation and structural interference is not used;

• It is necessary to research and develop methods and means of protecting information from SER CT using aiming, imitation and structural interference;

Thus, the analysis of active methods and means of protecting information from SER CT showed that noise generators based on the energy (force) method are most widely used in practice. Active protection methods should be used when passive protection methods are inefficient or economically expensive and technical implementation of which is practically impossible.

**REFERENCE**

1. Белов, Е. Б., Лось, В. П., Мещеряков, Р. В., & Шелупанов, А. А. (2006). Основы информационной безопасности.
2. Зайцев, А. П., Мещеряков, Р. В., & Шелупанов, А. А. (2012). Технические средства и методы защиты информации.
3. Liu, T., & Li, Y. (2019). Electromagnetic Information Leakage and Countermeasure Technique: Translated by Liu Jinming, Liu Ying, Zhang Zidong, Liu Tao. Springer.
4. Vuagnoux, M., & Pasini, S. (2009, August). Compromising electromagnetic emanations of wired and wireless keyboards. In USENIX security symposium (Vol. 8, pp. 1-16).
5. Boitan, A., Bărtușică, R., Halunga, S., Popescu, M., & Ionuță, I. (2018). Compromising electromagnetic emanations of wired USB keyboards. In Future Access Enablers for Ubiquitous and Intelligent Infrastructures: Third International Conference, FABULOUS 2017, Bucharest, Romania, October 12-14, 2017, Proceedings 3 (pp. 39-44). Springer International Publishing.
6. Boitan, A., Halunga, S., Bîndar, V., & Fratu, O. (2020). Compromising electromagnetic emanations of usb mass storage devices. Wireless Personal Communications, 1-26.
7. Wampler, C., Uluagac, S., & Beyah, R. (2015, December). Information leakage in encrypted ip video traffic. In 2015 IEEE Global Communications Conference (GLOBECOM) (pp. 1-7). IEEE.
8. Kuhn, M. G. (2003). Compromising emanations: eavesdropping risks of computer displays (No. UCAM-CL-TR-577). University of Cambridge, Computer Laboratory.
9. Zhang, N., Lu, Y., Cui, Q., & Wang, Y. (2017). Investigation of unintentional video emanations from a VGA connector in the desktop computers. IEEE Transactions on Electromagnetic Compatibility, 59(6), 1826-1834.
10. Macovei, A., Boitan, A., Trip, B., Butnariu, V., Roşu, G., & Halunga, S. (2018, October). Detection of electromagnetic emissions transmitted on the power line through electrical conduction. In 2018 International Conference on Applied and Theoretical Electricity (ICATE) (pp. 1-4). IEEE.
11. Smulders, P. (1990). The threat of information theft by reception of electromagnetic radiation from RS-232 cables. Computers & Security, 9(1), 53-58.
12. Boitan, A., Bărtușică, R., Halunga, S., & Bîndar, V. (2018, December). Video signal recovery from the laser printer LCD display. In Advanced Topics in Optoelectronics, Microelectronics, and Nanotechnologies IX (Vol. 10977, pp. 492-495). SPIE.
13. Kubiak, I., & Loughry, J. (2019). LED arrays of laser printers as valuable sources of electromagnetic waves for acquisition of graphic data. Electronics, 8(10), 1078.
14. Grzesiak, K., & Przybysz, A. (2010). Emission security of laser printers. Concepts and Implementations for Innovative Military Communications and Information Technologies; Military University of Technology: Warsaw, Poland.
15. Kubiak, I. (2018). Laser printer as a source of sensitive emissions. Turkish Journal of Electrical Engineering and Computer Sciences, 26(3), 1354-1366.
16. Boitan, A., Bătuşică, R., Halunga, S., & Fratu, O. (2019, September). Electromagnetic vulnerabilities of LCD projectors. In Proceedings of the 6th Conference on the Engineering of Computer Based Systems (pp. 1-6).

17. А.В. Иванов. Оценка защищенности информации от утечки по каналам побочных электромагнитных излучений и наводок: учебное пособие: Изд-во НГТУ, 2018. – 64 с.
18. Васильев, Р. А., & Ротков, Л. Ю. (2018). Обнаружение побочных электромагнитных излучений и наводок с помощью программно-аппаратного комплекса «легенда». Нижний Новгород.
19. de Meulemeester, P., Scheers, B., & Vandenbosch, G. A. (2020, July). Eavesdropping a (ultra) high-definition video display from an 80 meter distance under realistic circumstances. In 2020 IEEE International Symposium on Electromagnetic Compatibility & Signal/Power Integrity (EMCSI) (pp. 517-522). IEEE.
20. Kubiak, I. (2014). Digital processing methods of images and signals in electromagnetic infiltration process. Image Processing and Communications, 18(1), 5-14.
21. И.Р. Фазилжанов., Х.И. Фозилжонов, “Перехват побочных электромагнитных излучений монитора персонального компьютера,” Сборник докладов Республиканской научно-технической конференции «Значение информационно-коммуникационных технологий в инновационном развитии отраслей экономики». Часть 1, Ташкент, 2021, с.34-36.
22. De Meulemeester, P., Bontemps, L., Scheers, B., & Vandenbosch, G. A. (2018, May). Synchronization retrieval and image reconstruction of a video display unit exploiting its compromising emanations. In 2018 International Conference on Military Communications and Information Systems (ICMCIS) (pp. 1-7). IEEE.
23. Tempest for eliz [Online]. Available: https://github.com/eried/Research/tree/master/HackRF/TempestSDR.
24. Erik Thiele, Tempest for Eliza [Online]. Available: http://www.erikyyy.de/tempest.
25. “SDRuno User Manual v1.41,” SDRplay, 21-Jul-2020. [Online]. Available: https://www.sdrplay.com/help/. [Accessed: 13-May-2021].
26. Давронбеков, Д., & Фозилжонов, Х. (2021). СРАВНИТЕЛЬНЫЙ АНАЛИЗ ПРОГРАММНО-ОПРЕДЕЛЯЕМЫХ РАДИОСИСТЕМ ДЛЯ ИССЛЕДОВАНИЯ ПОБОЧНЫХ ЭЛЕКТРОМАГНИТНЫХ ИЗЛУЧЕНИЙ И НАВОДОК. InterConf, 415-419.
27. Ogli, F. K. I. (2021, November). Study of the Spectrum of Side Electromagnetic Radiations of Video Interface DVI. In 2021 International Conference on Information Science and Communications Technologies (ICISCT) (pp. 1-3). IEEE.
28. Лыньков, Л. М., Богуш, В. А., Борботько, Т. В., Украинец, Е. А., & Колбун, Н. В. (2004). Новые материалы для экранов электромагнитного излучения. Доклады Белорусского государственного университета информатики и радиоэлектроники, (3 (7)), 152-167.
29. Домарев, В.В. Безопасность информационных технологий. Системный подход. – Киев: ООО ТИД Диа Софт, 2004. – с. 992.
30. Yao, K., Lan, S., Xia, M., & Chen, L. (2018, July). Active countermeasure using EMI honeypot against TEMPEST eavesdropping in high-speed signalling. In 2018 USNC-URSI Radio Science Meeting (Joint with AP-S Symposium) (pp. 55-56). IEEE.
31. Suzuki, Y., & Akiyama, Y. (2010, July). Jamming technique to prevent information leakage caused by unintentional emissions of PC video signals. In 2010 IEEE International Symposium on Electromagnetic Compatibility (pp. 132-137). IEEE.

32. Иванов, В. П., & Залогин, Н. Н. (2010). Маскировка побочных излучений и наводок, создаваемых вычислительной техникой. Технические решения. Защита информации. Инсайд, (3), 68-75.
33. Казыханов, А. А., & Байрушин, Ф. Т. (2017). ЗАЩИТА ИНФОРМАЦИИ ОТ УТЕЧКИ ПО КАНАЛАМ ПЭМИН. Инновационное развитие, (4), 23-24.
34. Зимина, Ю. В. (2017). Средства и методы обеспечения безопасности бизнеса. Системы пространственного электромагнитного зашумления. Молодой ученый, (4), 439-446.
35. Патент РФ RU 2493594 от 20.09.2013г., C2 G06F 21/00, H04K 3/00. Лепеха Ю. П. Способ защиты обрабатываемой информации средствами вычислительной техники путем зашумления информативных побочных электромагнитных излучений и наводок, устройство защиты информации для реализации способа
36. Патент РФ RU 2421917 от 20.00.2011г., C1 H04K 1/04, H03B 29/00. Дёмин В. М., Лепеха Ю. П., Поярков Л. А. Способ защиты системы обработки информации от побочных электромагнитных излучений, устройство для реализации способа и генератор шумового сигнала для реализации устройства