RS232 Interface in the Process of Electromagnetic Infiltration

Rafal Przesmycki
Faculty of Electronics, Military University of Technology
Gen. S. Kaliskiego 2 Str., Warsaw 00-908, Poland

Abstract— The article concerns problems of electromagnetic compatibility and compromising emission that is the information security. The article focuses on RS232 Interface for which shows signals of extortion used during of compromising emission measurements. The article presents the results of compromising emissions measurements derived from RS232 Interface. In addition, the article discusses the laboratory stands for measuring compromising emission.

1. INTRODUCTION

Emission of electromagnetic field is a phenome-non constantly accompanying the passage of electric current which is, on the other hand, the basis of operation of all electronic and electric devices. Based on field changes it is possible to conclude about operation of devices being its source. What is more, properties of electromagnetic field permit its remote registration and analysis. The phenomenon of formation of electromagnetic waves carrying information about operation of electronic and electric devices is called com-promising emanation or corona. Since electric and electronic devices started to be used for information processing, often of confidential character, occurrence of compromising emission has acquired a particular importance.

Information security against electromagnetic permeability of devices and electromagnetic systems (IT) is of great importance. This problem increases with a higher and higher use of ICT devices for processing and trans-mitting information which should not fall into the wrong hands. It results from the fact that each electronic device is the source of undesirable (secondary) emission of electromagnetic energy induced in surrounding space and in all close conductors and metal structures.

When signals of undesirable emission are correlated with unclassified information, they can be used for reconstructing that information by intelligence services. The phenomenon of such undesirable emission is called compromising emission and its use by intelligence — penetration or electromagnetic infiltration. Undertakings which aim is to hinder system recognition on the basis of compromising emission are called information protection against electromagnetic penetration or emission safety.

Electromagnetic emissions with the feature of compromising emission can arise at any stage of processing of encoded information in the form of electric current courses. There is also no possibility to conduct tests of the source itself and the channel of information permeability. However such tests can be conducted in laboratory conditions in which examined devices are introduced into operation mode allowing to learn their infiltration susceptibility. In this article an example of such experiments has been presented. It seems that most suitable for illustrating the issue of electromagnetic information permeability are devices or their components which process information in serial way and the rule of encoding is uncomplicated and wellknown [5–7].

2. RS232 INTERFACE

In telecommunications, RS-232 is a standard for serial communication transmission of data. It formally defines the signals connecting between a DTE (data terminal equipment) such as a computer terminal, and a DCE (data circuit-terminating equipment or data communication equipment), such as a modem. The RS-232 standard is commonly used in computer serial ports. The standard defines the electrical characteristics and timing of signals, the meaning of signals, and the physical size and pinout of connectors. The current version of the standard is TIA-232-F Interface Between Data Terminal Equipment and Data Circuit-Terminating Equipment Employing Serial Binary Data Interchange, issued in 1997.

An RS-232 serial port was once a standard feature of a personal computer, used for connections to modems, printers, mice, data storage, uninterruptible power supplies, and other peripheral devices. However, RS-232, when compared to other serial interfaces such as RS-422, RS-485 and Ethernet, is hampered by low transmission speed, short maximum cable length, large voltage swing, large standard connectors, no multipoint capability and limited multidrop capability. In modern personal

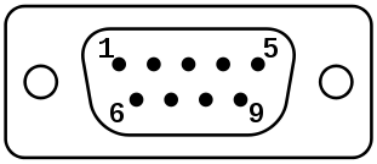

Figure 1: A DB-9 connector in RS232 standard.

computers, USB has displaced RS-232 from most of its peripheral interface roles. Many computers no longer come equipped with RS-232 ports (although some motherboards come equipped with a COM port header that allows the user to install a bracket with a DE-9 port) and must use either an external USB-to-RS-232 converter or an internal expansion card with one or more serial ports to connect to RS-232 peripherals. Nevertheless, thanks to their simplicity and past ubiquity, RS-232 interfaces are still used — particularly in industrial machines, networking equipment, and scientific instruments where a short-range, point-to-point, low-speed wired data connection is adequate.

In RS-232, user data is sent as a time-series of bits. Both synchronous and asynchronous transmissions are supported by the standard. In addition to the data circuits, the standard defines a number of control circuits used to manage the connection between the DTE and DCE. Each data or control circuit only operates in one direction, that is, signaling from a DTE to the attached DCE or the reverse. Because transmit data and receive data are separate circuits, the interface can operate in a full duplex manner, supporting concurrent data flow in both directions. The standard does not define character framing within the data stream, or character encoding.

The RS-232 standard defines the voltage levels that correspond to logical one and logical zero levels for the data transmission and the control signal lines. Valid signals are either in the range of +3 to +15 volts or the range −3 to −15 volts with respect to the "Common Ground" (GND) pin; consequently, the range between −3 to +3 volts is not a valid RS-232 level. For data transmission lines (TxD, RxD, and their secondary channel equivalents), logic one is defined as a negative voltage, the signal condition is called "mark". Logic zero is positive and the signal condition is termed "space". Control signals have the opposite polarity: the asserted or active state is positive voltage and the deasserted or inactive state is negative voltage. Examples of control lines include request to send (RTS), clear to send (CTS), data terminal ready (DTR), and data set ready (DSR).

The standard specifies a maximum open-circuit voltage of 25 volts: signal levels of ±5 V, ±10 V, ±12 V, and ±15 V are all commonly seen depending on the voltages available to the line driver circuit. Some RS-232 driver chips have inbuilt circuitry to produce the required voltages from a 3 or 5 volt supply. RS-232 drivers and receivers must be able to withstand indefinite short circuit to ground or to any voltage level up to ±25 volts. The slew rate, or how fast the signal changes between levels, is also controlled.

Because the voltage levels are higher than logic levels typically used by integrated circuits, special intervening driver circuits are required to translate logic levels. These also protect the device's internal circuitry from short circuits or transients that may appear on the RS-232 interface, and provide sufficient current to comply with the slew rate requirements for data transmission.

Because both ends of the RS-232 circuit depend on the ground pin being zero volts, problems will occur when connecting machinery and computers where the voltage between the ground pin on one end, and the ground pin on the other is not zero. This may also cause a hazardous ground loop. Use of a common ground limits RS-232 to applications with relatively short cables. If the two devices are far enough apart or on separate power systems, the local ground connections at either end of the cable will have differing voltages; this difference will reduce the noise margin of the signals. Balanced, differential serial connections such as RS-422, RS-485, and USB can tolerate larger ground voltage differences because of the differential signaling.

Unused interface signals terminated to ground will have an undefined logic state. Where it is necessary to permanently set a control signal to a defined state, it must be connected to a voltage source that asserts the logic 1 or logic 0 level, for example with a pullup resistor. Some devices provide test voltages on their interface connectors for this purpose.

3. THE LABORATORY STAND FOR MEASURING COMPROMISING EMISSION

In order to determine sources of compromising emission deriving from RS232 interface it is necessary to estimate a contents degree of test signal intentionally generated by RS232 interface (RS232 cable)

in the signal received by measuring position as radiated or conducted compromising emission.

The laboratory stand for conducting tests of determining sources of compromising emission should make reception of generated test signal propagating as radiated or conducted compromising emission possible. In this article attention has been paid to radiated compromising emission [3, 4]. A sample system for testing forcing signals for compromising emission built on the basis of available on the market equipment has been presented in Figure 2.

For RS232 interface as forcing for compromising emission used a requests a binary information sequences between PC and RS232 loop. With the use of receiving antennas [9, 11] signal received by antenna gets through commutator which switches antennas to FSET 22 broadband receiver. In the receiver those signals are filtered and their conversion into lower frequency range takes place. Signal after detection is passed to VIDEO output in the receiver and then it is passed to input of external channel of oscilloscope on which there is a possibility of displaying received information in time domain [3, 4].

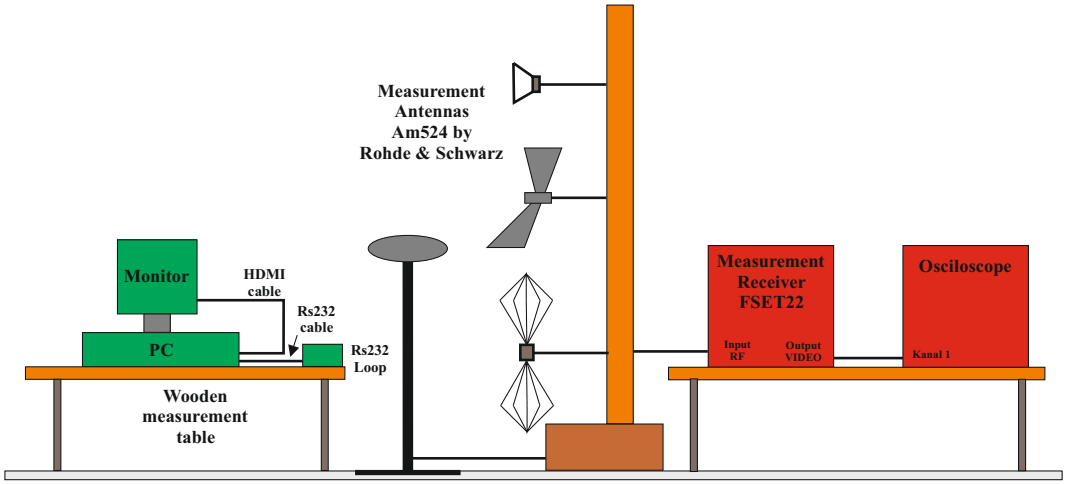

Figure 2: Block diagram of the laboratory stand for testing compromising emission.

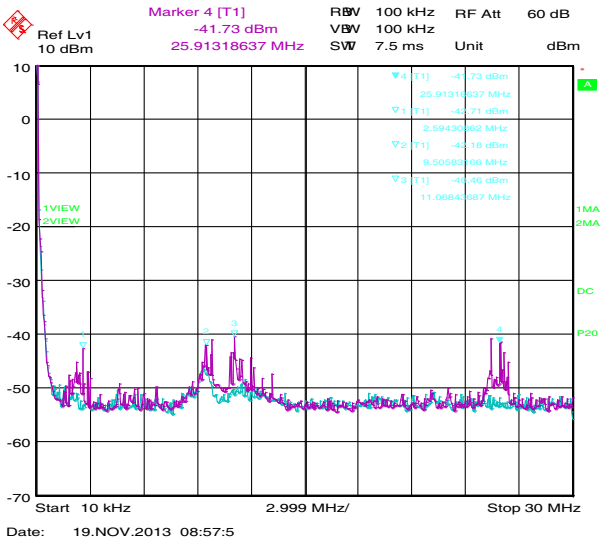

Figure 3: Radiated emission deriving from RS232 interface while the transmission data is OFF (blue color) and while transferring a pseudorandom string transmitted at 115200 bps (purple color) in frequency range 100 kHz–30 MHz.

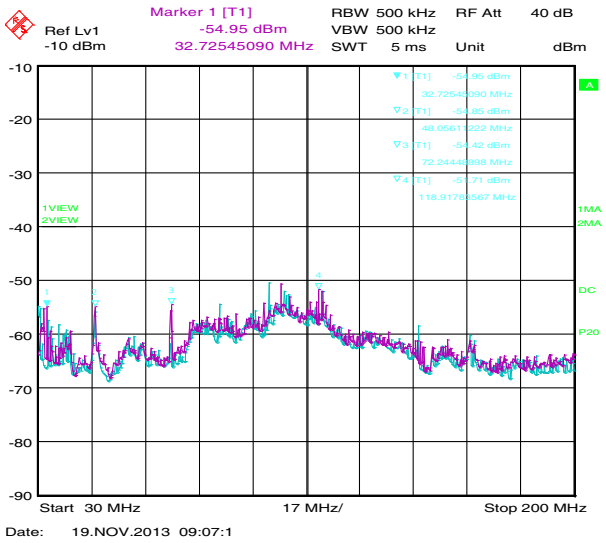

Figure 4: Radiated emission deriving from RS232 interface while the transmission data is OFF (blue color) and while transferring a pseudorandom string transmitted at 115200 bps (purple color) in frequency range 30 MHz–200 MHz.

4. MEASUREMENT RESULTS

Simple observation of the frequency spectrum obtained while working RS232 interface in selected binary sequence of transfer mode does not answer on the potential for compromising emissions. In order to determine the distinctive features of the RS232 (data lines) at which the reflected component having a frequency spectrum or time-domain binary sequences using during tests conducted with RS232 interface working have been chosen. The selected binary sequences are: pseudorandom string transmitted at 19200 bps, pseudorandom string transmitted at 115200 bps, idle status (no data transfer on the interface).

During the test emission for RS232 can be identified by the fact that transmission started by comparing the time course and its spectrum transmission lines after switching the transmission and idle (no force data on the interface). In order to compare waveforms and their spectrum of these two conditions below shows the measurement results for the states when the data lines and the interface is forced, when such transmission is not forced. The measurement results for pseudorandom string transmitted at 115200 bps are shown in Fig. 3, Fig. 4, Fig. 5 and Fig. 6.

Very often evaluation of spectrum itself is insufficient due to difficulties resulting from rating of

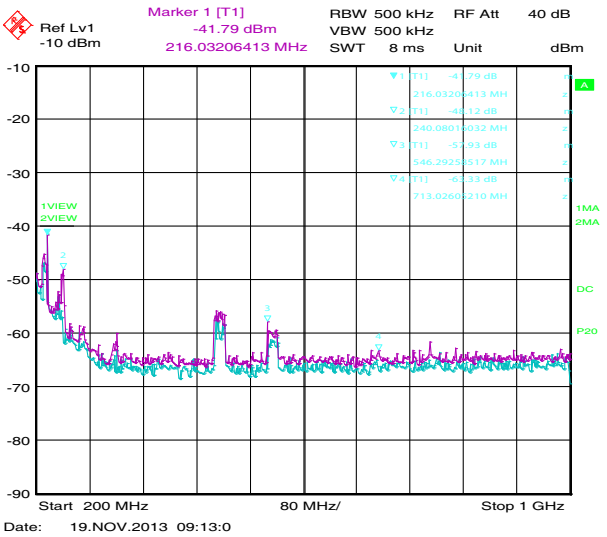

Figure 5: Radiated emission deriving from RS232 interface while the transmission data is OFF (blue color) and while transferring a pseudorandom string transmitted at 115200 bps (purple color) in frequency range 200 MHz–1000 MHz.

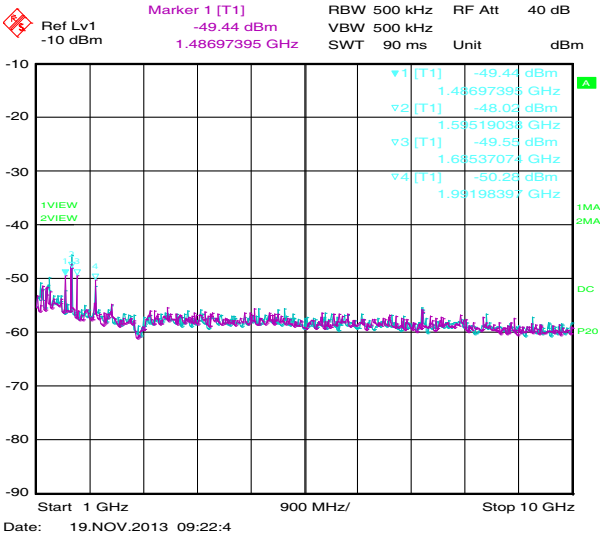

Figure 6: Radiated emission deriving from RS232 interface while the transmission data is OFF (blue color) and while transferring a pseudorandom string transmitted at 115200 bps (purple color) in frequency range 1 GHz–10 GHz.

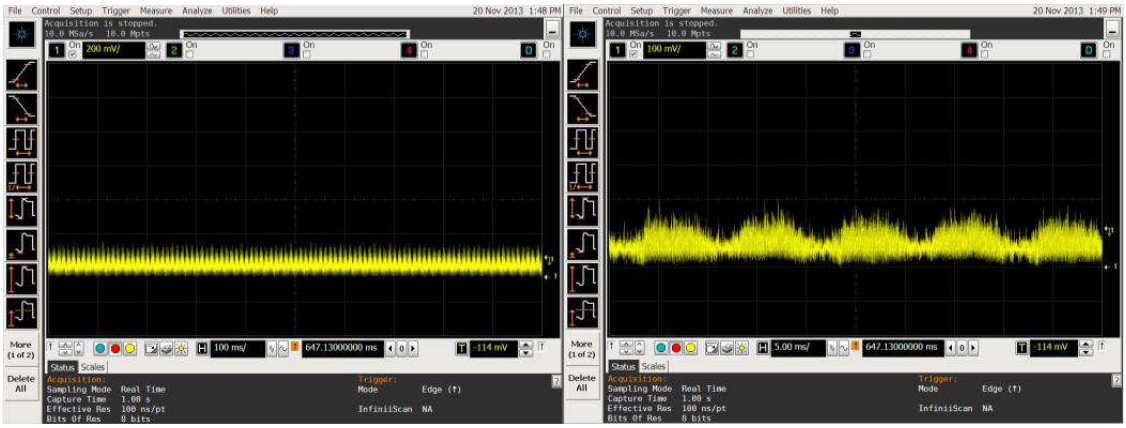

Figure 7: Oscillogram for RS232 interface while the data transmission is OFF. The signal received by antenna for $f = 115,2$ kHz given from VIDEO output of FSET22 receiver.

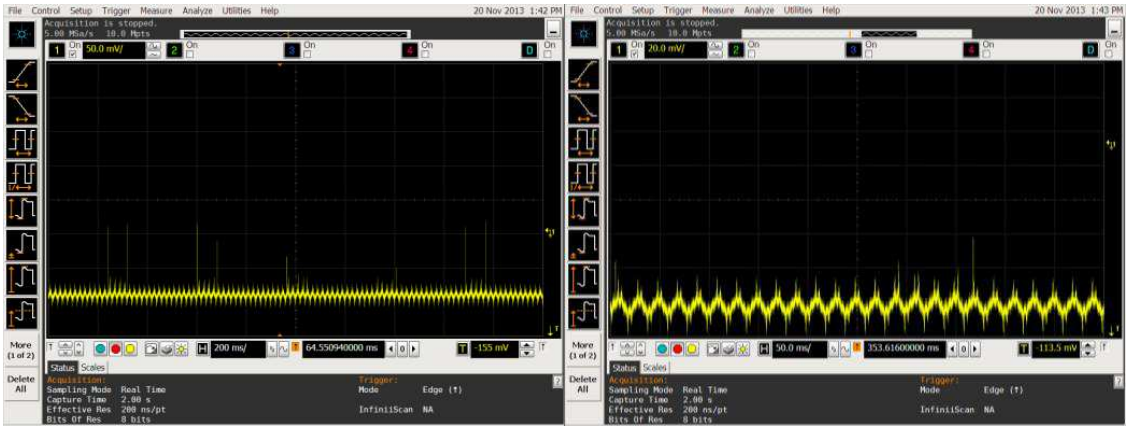

Figure 8: Oscillogram for RS232 interface while the data transmission is OFF. The signal received by antenna for $f = 19,2\,\mathrm{kHz}$ given from VIDEO output of FSET22 receiver.

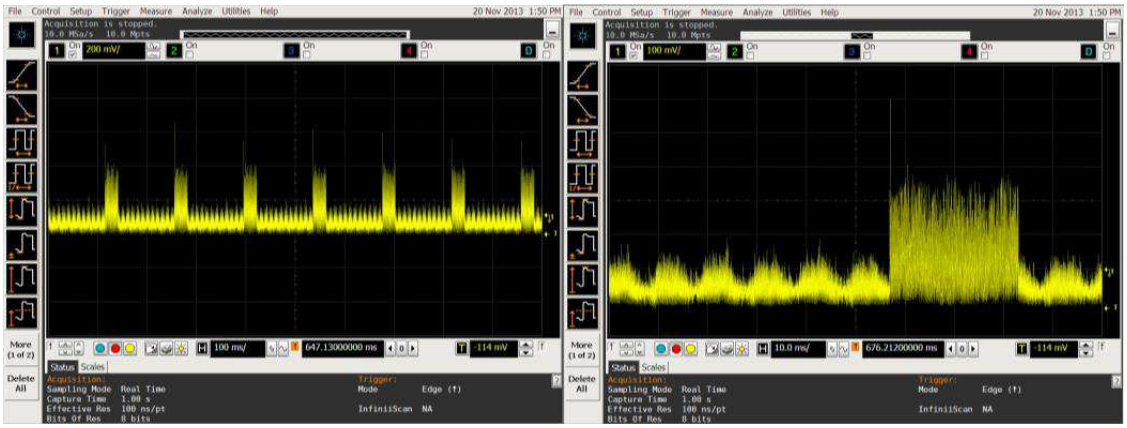

Figure 9: Oscillogram for RS232 interface while the data transmission is ON with 115200 bps speed. The signal received by antenna for $f = 115,2\,\mathrm{kHz}$ given from VIDEO output of FSET22 receiver.

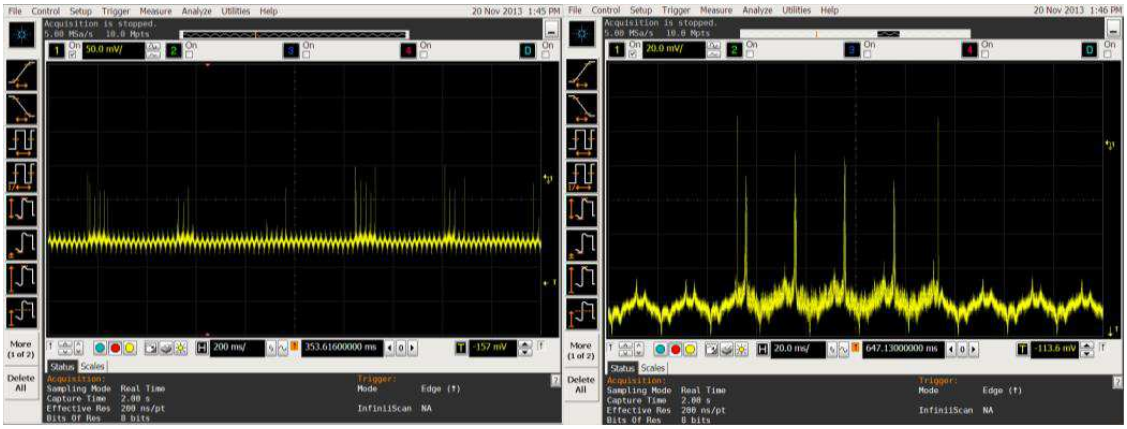

Figure 10: Oscillogram for RS232 interface while the data transmission is ON with 19200 bps speed. The signal received by antenna for $f = 19,2\,\mathrm{kHz}$ given from VIDEO output of FSET22 receiver.

appearing signals at particular frequencies. Because of that it is necessary to use other methods consisting in the use of more advanced measuring devices. Anyway in most cases qualification of emissions occurs with the use of visual method. It should be remembered though that in doubtful cases or in such ones where visual assessment is impossible evaluation methods based on digital methods of processing of recorded signals are used [1, 2].

Identification is a process or a result of processes of identifying a particular object with other

object. It may include distinguishing common features, capturing similarities between a tested object and other objects of the same category, estimating values of observed parameters of a particular object. Using any methods of signal identification of compromising emission requires determination of distinctive features characteristic for model information signals and determination of a similarity degree of those features for analogous parameters of tested signals [1, 2, 8, 10].

On the basis of an analysis of radiated emission levels by RS232 interface probable signal reception frequencies of compromising emission have been determined. To test whether radiated signals within that frequency range actually have the character of compromising emission, a series of recordings of those signals has been made with the use of digital oscilloscope and analyzed [6, 7].

Measurements were performed while transferring data in the form of pseudorandom binary sequences between PC and RS232 loop with two data transmitted speed. Examples of the results shown in the pictures from Fig. 7 to Fig. 10.

5. CONCLUSION

The presented above time courses of radiated emission signals by RS232 interface show clearly that those signals have an evident connection with contents of transmitted signal (pseudorandom strings) and thus they have the character of compromising emission signals. Time courses directly identify the contents form of transmitted data. On the basis of the measurements obtained from the oscilloscope waveforms appearing on the interface transmission lines and their spectrograms received using a spectrum analyzer and oscilloscope can be concluded that: by selecting the pattern of transmitted binary sequence in the test computer device can be formed character the time course of signal transmission lines RS232 interfaces in such a way that it can be easily identified on the oscillogram.

Based on the presented of measurement results we can be concluded that:

- by selection of the binary sequence pattern information it is not possible to increase the levels of the components in the frequency spectrum of signals transmitted through the RS232 interface, which could lead to the location of transmission occurring at the interfaces of RS232;
- components present in the frequency spectrum of signals transmitted via the RS232 interface of the order of single megahertz which results in virtually no currently able to reconstruct and decode the information transmitted by the interface.

ACKNOWLEDGMENT

The project is financed from NCBiR means within the Agreement No. DOB-1-4/1/PS/2014 in the years 2015–2020.

REFERENCES

1. Grzesiak, K., I. Kubiak, S. Musiał, and A. Przybysz, "Elektromagnetyczne bezpieczeństwo informacji," Wydawca, WAT, Zegrze, 2012.
2. Grzesiak, K., I. Kubiak, S. Musiał, and A. Przybysz, "Generator rastra w procesie infiltracji elektromagnetycznej," Wydawca, WAT, Zegrze, 2012.
3. Przesmycki, R. and L. Nowosielski, "USB 3.0 interface in the process of electromagnetic infiltration," *PIERS Proceedings*, 1019–1023, Shanghai, China, Aug. 8–11, 2016.
4. Przesmycki, R., "Measurement and analysis of compromising emanation for laser printer," *PIERS Proceedings*, 2661–2665, Guangzhou, China, Aug. 25–28, 2014.
5. Nowosielski, L. and J. Lopatka, "Measurement of shielding effectiveness with the method using high power electromagnetic pulse generator," *PIERS Proceedings*, 2687–2691, Guangzhou, China, Aug. 25–28, 2014.
6. Ziółkowski, C. and J. M. Kelner, "Influence of receiver/transmitter motion direction on the correlational and spectral signal properties," *2016 10th European Conference on Antennas and Propagation (EuCAP)*, 1–4, Davos, Switzerland, Apr. 10–15, 2016, doi: 10.1109/EuCAP.2016.7481225.
7. Kelner, J. M. and C. Ziółkowski, "Influence of receiver/transmitter motion direction on the correlational and spectral characteristics — Simulation analysis," *2016 10th International Conference on Signal Processing and Communication System (ICSPCS)*, 545–550, Gold Coast, QLD, Australia, Dec. 19–21, 2016, doi: 10.1109/ICSPCS.2016.7843381.
8. Bugaj, M., "Measurements of wall attenuation in closed spaces inside a building," *PIERS Proceedings*, 2681–2686, Guangzhou, China, Aug. 25–28, 2014.

9. Bugaj, M., J. Bugaj, and W. Marian, "U shape microstrip wideband antenna," *PIERS Proceedings*, 1046–1049, Shanghai, China, Aug. 8–11, 2016.
10. Bugaj, M., "Attenuation measurements of materials used in construction of buildings," *PIERS Proceedings*, 2671–2675, Guangzhou, China, Aug. 25–28, 2014.
11. Bugaj, M., J. Bugaj, and W. Marian, "Design of WLAN microstrip antenna for 5.17–5.835 GHz," *XI Conference on Reconnaissance and Electronic Warfare Systems 2017, Proceedings of SPIE*, Vol. 10418, Oltarzew, Poland, 2017, DOI: 10.1117/12.2270174, ISBN: 978-1-5106-1294-5; 978-1-5106-1295-2.