www.czasopisma.pan.pl PAN www.journals.pan.pl

jet INTL JOURNAL OF ELECTRONICS AND TELECOMMUNICATIONS, 2020, VOL. 66, NO. 3, PP. 481-486
Manuscript received February 6, 2020; revised July, 2020. DOI: 10.24425/ijet.2020.134002

Impact of IT Equipment Location in Buildings on Electromagnetic Safety

Leszek Nowosielski

***Abstract*—Signal attenuation caused by the propagation path between the compromising emanation source (the location of secured IT equipment) and the location of the antenna of the potential infiltrating system has a direct influence on the electromagnetic safety of IT equipment. The article presents original analytical relationships necessary to estimate the attenuation values introduced by the propagation path of the potential compromising emanation signal, which correspond to the most probable locations of IT equipment in relation to the location of the potential infiltrating system. The author of the article analyzes various location scenarios for IT equipment – a potential source of compromising emanations – with a potential infiltrating system located either within or outside the boundaries of a building, in which said IT equipment is located. The aforementioned scenarios are characterized by the lowest propagation path attenuation of potential compromising emanation generated by the secured IT equipment and provide for location masking of the potential infiltrating system. Example design of protective solutions for IT equipment elaborated by article author in the form of a shielding enclosure is presented in the article as well.**

***Keywords*—IT equipment, EMC electromagnetic compatibility, compromising emanations**

I. Introduction

DUE to the unbelievably fast development rate of modern technology in the recent years, and telecommunications technologies in particular, coupled with the introduction of computer technologies in virtually all facets of our lives, information became a critical resource, and is essential to success in both business and politics. As the vast majority of information is now processed using various types of IT equipment, safeguarding it from unauthorized access is more important than ever before. Emissions of electromagnetic disturbances unintentionally generated by IT equipment pose a high risk in this respect. Under favorable conditions, unauthorized parties may use this emitted interference to reproduce information processed by the equipment, in a process known as electromagnetic infiltration. Any electromagnetic emission, whose signal may be correlated with useful information, and can be used to reproduce said information, is called a compromising emission. Therefore, it is important to recognize and mitigate the risk of electromagnetic eavesdropping in IT equipment used for information processing. The article presents original analytical relationships necessary to estimate the attenuation values, introduced by the propagation path of the potential compromising emanation signal, for the most probable scenarios for the location of IT equipment in relation to the location of the potential infiltrating system. The article analyses various location scenarios for secured IT equipment, constituting a potential source of compromising emanation, with the potential infiltrating system located both inside or outside the building housing said equipment. The aforementioned scenarios are characterized by the lowest propagation path attenuation of potential compromising emanation generated by the secured IT equipment and provide for location masking of the potential infiltrating system.

The paper presents analytical relationships for calculating the attenuation value of the propagation path for a potential compromising emission signal A_{dr}, introduced by the propagation path between the source of the compromising emission (the location of the secured IT equipment), and the location of the antenna of the potential infiltrating system, which has a direct impact on the electromagnetic safety of IT equipment.

The article describes the protection of IT devices in the form of shielding housings against radiated compromising emissions. The article does not include the analysis of threats resulting from the possibility of penetration of conducted compromising emissions generated by IT devices to power lines. The above issue will be discussed in the next article covering the above subject.

II. Impact of IT Equipment Location in Buildings on Its Electromagnetic Security

The *S/N* ratio of the compromising emission signal level *S* and the level of environmental interference *N* at the receiver input of the potential infiltrating system is affected by several parameters. Primary parameters have been defined as components of the following analytical relationship, which determines the *S/N* ratio of the compromising emission signal level to the level of environmental interference at the input of the receiver of the potential infiltrating system [8].

$$\frac{S}{N} = E_{B,max} + G_a + G_r - A_s - A_{dr} - E_{n,B} - F_r \,, \qquad (1)$$

where:

$E_{B,max}$ - allowed level of electric field strength for radiated emissions from IT equipment, as specified by standards harmonized with the electromagnetic compatibility directive [1],

B - the IF filter width of the pass-through band of the measuring (infiltrating) receiver used during electric field strength measurements of emitted disturbances,

Leszek Nowosielski is with Military University of Technology, Faculty of Electronics, Poland (e-mail: Leszek.Nowosielski@wat.edu.pl).

G_a - gain of the receiving antenna used for electromagnetic infiltration,
G_r - signal processing gain of the compromising emission signal,
A_s - shielding effectiveness of IT equipment enclosure,
A_{dr} - attenuation brought by the propagation of the signal between the compromising emission source and the infiltrating system,
$E_{n,B}$ - electric field strength of environmental interference,
F_r - noise factor of the measuring (infiltrating) receiver.

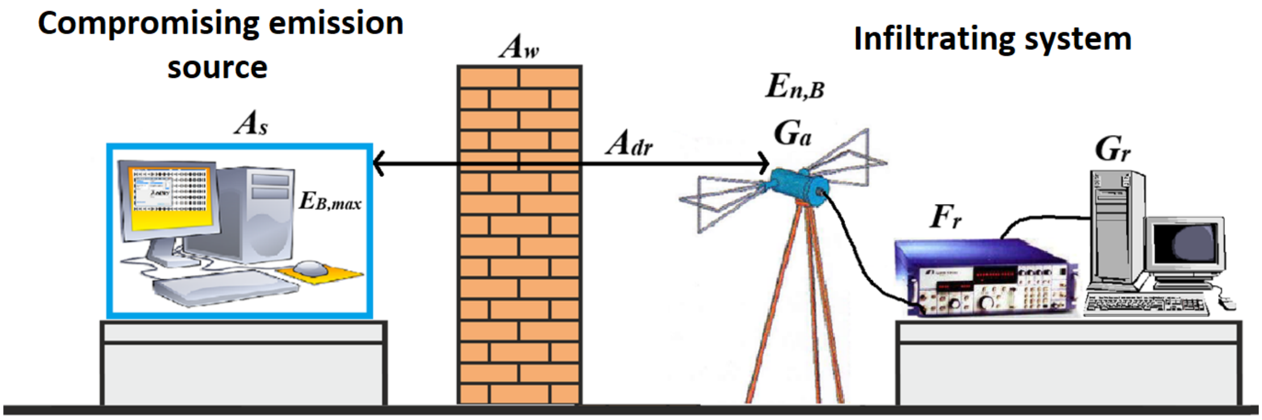

Fig. 1. The energy budget of the link between the secured IT equipment and the potential infiltrating system.

The energy budget described in relation (1) is shown in Fig. 1.

One of the components of the relationship is attenuation A_{dr} brought by the propagation of the signal between the compromising emission source and the infiltrating system's antenna. Upon performing the necessary transformations of the relationships (1) we obtain a relationship defining the value of A_{dr}, which takes the form of

$$A_{dr} = E_{B,max} + G_a + G_r - \frac{S}{N} - A_s - E_{n,B} - F_r \, . \quad (2)$$

In order to determine the relationship to the A_{dr}, value, above which the ratio of the radiated compromising emission level to the environmental interference level S/N is smaller than or equal to 0 dB, a value of $S/N = 0$ dB must be inserted into the formula.

$$A_{dr} = E_{B,max} + G_a + G_r - A_s - E_{n,B} - F_r \, . \quad (3)$$

Using the relationship above, it is possible to estimate the value of the A_{dr} parameter, above which the ratio value of the S/N relationship is smaller than or equal to 0 dB at the input of the infiltrating receiver, which greatly hinders any attempts at electromagnetic infiltration.

The attenuation value A_{dr}, derived from the signal propagation path between the source of compromising emissions and the antenna of the infiltrating system, depends on the location of the secured IT equipment in relation to the location of the potential infiltrating system. In practice, in most common scenarios, associated with the greatest risk of electromagnetic infiltration, secured IT equipment is located inside the building (in an office environment), while the potential infiltrating system is masked and located near the secured IT equipment. Possible scenario configurations, which meet the above assumptions, include:

– Scenario 1: IT equipment and the infiltrating system are located on the same floor of the building (Fig. 2),
– Scenario 2: IT equipment is located inside the building, on its lowest floor, and is separated from the infiltrating system by a single external wall of the building (with the infiltrating system positioned outside of the building) (Fig. 2),
– Scenario 3: IT equipment and infiltrating system are separated by a single internal partition, i.e. the floor or ceiling in a building (Fig. 2).

A graphical representation of the aforementioned scenarios is represented on Fig. 2. It should be noted that the aforementioned scenarios are most common for hostile electromagnetic infiltration, as they ensure minimized attenuation A_{dr} of the radiated compromising emission caused by the propagation path, and at the same time take into account the best masking locations for the infiltrating system.

Considering that in the above scenarios, the IT equipment constituting a potential source of compromising emissions is most commonly found inside multi-storey office buildings, in order to determine the attenuation A_{dr}, the author used a propagation model, which takes into account the specificity of electromagnetic wave propagation typical for this type of building. Technical literature [2][3][4] contains examples of many propagation models, which could be used to calculate propagation attenuation in an indoor environment. Of all available models, the propagation model recommended by the ITU-R document [2] was used due to the accuracy of the obtained calculations, and the simplicity they provide in the calculation of attenuation A_{dr} brought by the propagation path of the compromising emission signal in an indoor environment.

The propagation model recommended by ITU-R is an empirical model, which takes three factors into account, all of which have a decisive influence on the value of attenuation A_{dr} determined by signal propagation path:

– length of the propagation path d_r,
– frequency of propagating wave f,
– attenuation of the signal passing through walls and ceilings of the building A_{fl}.

The first two components are included in most propagation models and their presence is natural. The last factor is related to the propagation specificity of a multi-storey building divided by walls. Attenuation A_{dr} brought by signal propagation path is determined by the following equation [2]:

$$A_{dr} = 20 \cdot log(f) + N_l \cdot log(d_r) + A_{fl} \cdot (f_l) - 28 , (4)$$

where:

f – frequency of propagating wave [MHz],

d_r – length of the propagation path [m],

N_l – the distance attenuation factor, for which the recommended values are given in literature [2],

A_{fl} – the ceiling attenuation factor, for which the recommended values are given in literature [2],

f_l – the number of floors between IT equipment being a potential source of compromising emissions and an infiltrating system.

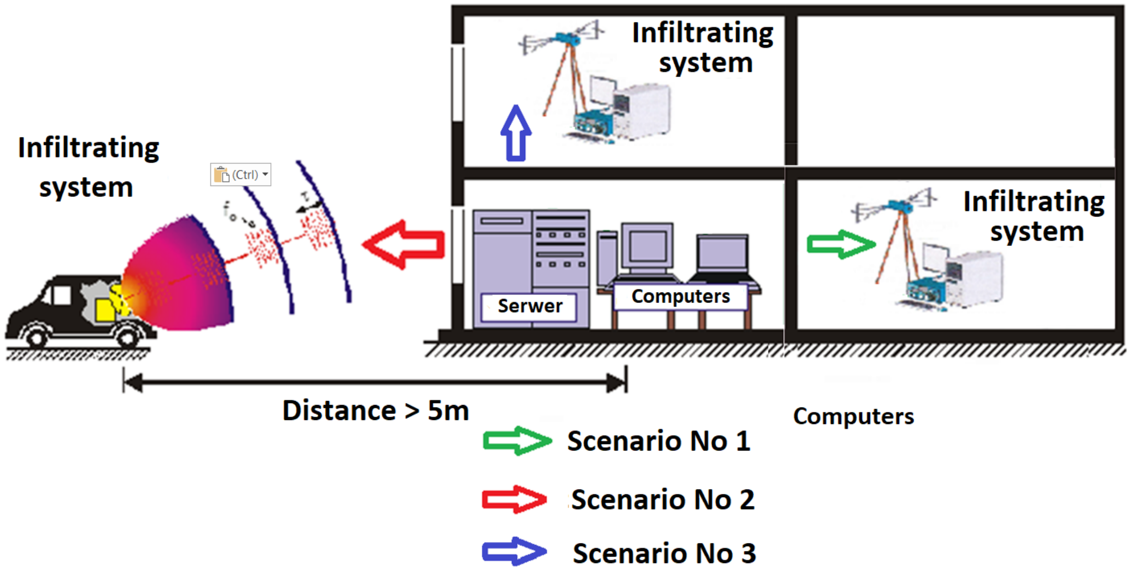

Fig. 2. Graphical representation of IT equipment and infiltrating system location scenarios.

Due to the fact that the propagation model recommended by ITU-R is used solely to calculate the attenuation of propagation inside buildings in order to use the relationship (4) to calculate attenuation of the propagation path between the IT equipment and the infiltrating system located outside the building, it is necessary to additionally consider the attenuation A_w brought by the external (load-bearing) wall of the building. Recommended attenuation A_w values can be found in reference material [3]. Therefore, the general relationship of attenuation of the signal propagation path between the IT equipment being the source of the compromising emission signal and the infiltrating system takes the following form.

$$A_{dr} = 20 \cdot log(f) + N_l \cdot log(d_r) + A_{fl} \cdot (f_l) - 28 + A_w, (5)$$

In order to calculate the lowest attenuation A_{dr} values, which can be practically achieved in the electromagnetic infiltration process, brought by the propagation of the compromising emission signal, additional assumptions were made for all the aforementioned IT equipment location scenarios in relation to the location of the infiltrating system. The above assumptions and their justification are presented in Table I. In order to estimate the attenuation of A_{dr} brought by the signal propagation path corresponding to Scenario 1 for the selected building parameters, in which the secured IT equipment was located, as a value of distance attenuation coefficient N_l, attenuation coefficient A_{fl} and attenuation brought by the external (load-bearing) wall of the building A_w , which are part of the relationship (5), the following values taken from the literature position [2] and [3] were adopted:

– N_l = 33 dB (f < 1GHz), N_l = 30 dB (1 GHz < f < 2 GHz), N_l = 25.5 dB (2 GHz < f < 3 GHz), N_l = 27 dB (3 GHz < f < 4 GHz), N_l = 28 dB (4 GHz < f < 5 GHz), N_l = 24 dB (5 GHz < f < 6 GHz) ,
– A_{fl} = 0.0 dB,
– A_w = 0.0 dB.

Obtained minimum values of A_{dr} attenuation brought by signal propagation path for Scenario 1 are shown in Fig. 3 (green curve).

In order to estimate the attenuation of A_{dr} brought by the signal propagation path corresponding to Scenario 2 for the selected building parameters, in which the secured IT equipment was located, as a value of distance attenuation coefficient N_l, attenuation coefficient A_{fl} and attenuation brought by the external (load-bearing) wall of the building A_w , which are part of the relationship (5), the following values taken from the literature position [2] and [3] were adopted:

– N_l = 33 dB (f < 1GHz), N_l = 30 dB (1 GHz < f < 2 GHz), N_l = 25.5 dB (2 GHz < f < 3 GHz), N_l = 27 dB (3 GHz < f < 4 GHz), N_l = 28 dB (4 GHz < f < 5 GHz), N_l = 24 dB (5 GHz < f < 6 GHz),
– A_{fl} = 0.0 dB,
– A_w = 5.0 dB.

Obtained minimum values of A_{dr} attenuation brought by signal propagation path for Scenario 2 are shown in Fig. 3 (red curve).

TABLE I
ASSUMPTIONS FOR INDIVIDUAL LOCATION SCENARIOS FOR THE IT EQUIPMENT AND LOCATION OF AN INFILTRATING SYSTEM

No.	Assumption	Assumption justification	IT equipment location scenario		
			No. 1	No. 2	No. 3
1.	The compromising emission signal is propagated inside an office building environment.	This is typically the most common location for IT equipment being a potential source of compromising emission.	x	x	x
2.	The IT equipment is located in an old office building (external walls of the building are made of light concrete, are 10 cm thick, and are furnished with single pane windows embedded in wooden frames).	Old office buildings are characterized by the lowest attenuation A_w of the (load-bearing) external wall.	–	x	–
3.	The distance between the systems is not less than 5 m.	A distance of 5 m is the shortest practical distance possible between IT equipment and the infiltrating system, if such equipment is located on the same or on adjacent floors of a building. The shortest distance value ensures that the minimum A_{dr} attenuation value of the propagation path of the compromising emission signal is achieved. The above distance also ensures that the location of the infiltrating system is masked.	x	x	x

In order to estimate the attenuation of A_{dr} brought by the signal propagation path corresponding to Scenario 3 for the selected building parameters, in which the secured IT equipment was located, as a value of distance attenuation coefficient N_l, attenuation coefficient A_{fl} and attenuation brought by the external (load-bearing) wall of the building A_w , which are part of the relationship (5), the following values taken from the literature position [2] and [3] were adopted:

– $N_l = 33$ dB ($f < 1$GHz), $N_l = 30$ dB (1 GHz $< f < 2$ GHz), $N_l = 25.5$ dB (2 GHz $< f < 3$ GHz), $N_l = 27$ dB (3 GHz $< f < 4$ GHz), $N_l = 28$ dB (4 GHz $< f < 5$ GHz), $N_l = 24$ dB (5 GHz $< f < 6$ GHz),
– $A_{fl} = 9$ dB ($f < 1$GHz), $A_{fl} = 15$ dB (1 GHz $< f < 2$ GHz), $A_{fl} = 14$ dB (2 GHz $< f < 3$ GHz), $A_{fl} = 18$ dB (3 GHz $< f < 4$ GHz), $A_{fl} = 16$ dB (4 GHz $< f < 5$ GHz), $A_{fl} = 22$ dB (5 GHz $< f < 6$ GHz),
– $A_w = 0.0$ dB.

Obtained minimum attenuation A_{dr} values brought by signal propagation path for Scenario 3 are shown in Fig. 3 (blue curve).

The mathematical relationships presented in the article and the calculated attenuation A_{dr} values presented in Fig. 3 relate to polarization of infiltrating antenna presented in Fig. 1 (horizontal polarization). In order to calculate the attenuation A_{dr} value for vertical polarization of infiltrating antenna we must use another value of antenna gain G_a in mathematical relationships presented in the article.

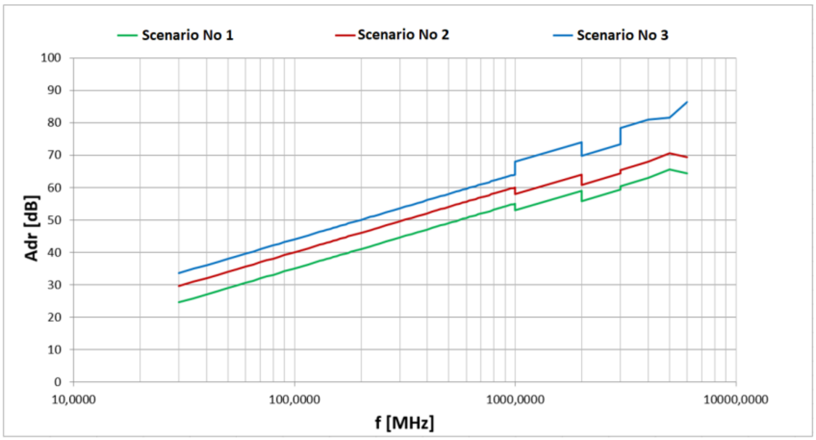

Fig. 3. Attenuation A_{dr} introduced by signal propagation path for particular scenarios of IT equipment location in relation to the location of the infiltrating system.

III. PRACTICAL APPLICATIONS FOR SOLUTIONS PROTECTING IT EQUIPMENT AGAINST ELECTROMAGNETIC COMPROMISING EMANATIONS

In practice, there are very often situations when the construction of buildings and rooms in which IT devices are used and the maximum possible propagation path attenuation A_{dr} between IT devices and the potential location of the infiltration system do not ensure suppression of the compromising emission level to the value for which the compromising emanation signal level up to the level of environmental interference S/N < 0. In such cases, one of the possibilities of suppressing of the compromising emanation signal level is the use of shielding housings with the appropriate value of shielding efficiency A_s. The authors evaluated the required suitable values for parameters A_s, which would enable efficient shielding of IT equipment enclosures, and therefore reduce the risk of electromagnetic information emanations, as presented in reference [5].

A number of shielding cabinets and enclosures integrated with protected IT equipment are available commercially. In articles [6][9][10], one can find examples of protective solutions for IT equipment in the form of a shielding enclosure, a shielding cabinet, and an enclosure integrated with the protected equipment and fitted with a power filter capable of satisfying requirements for shielding effectiveness A_s, as well the requirements regarding attenuation introduced by the power supply filters. Design solutions for protections presented therein were appropriated for use in scenarios with single and several items of IT equipment.

The following is one of the possible solutions for the shielding enclosure for protection against compromising emanations from a single item of IT equipment. In order to protect a single item of IT equipment, such as a portable computer or a small-form-factor (SFF) CPU against electromagnetic emanation of compromising information, the shielding enclosure can be used built-in power supply filters and wires, which are used to supply power to the protected IT equipment and enable its communication with external accessories. In case of the shielding enclosure solution discussed herein, it is necessary to ensure that the PC being protected can communicate with the following peripherals: keyboard, mouse, monitor and 9 V DC and 12 V DC power supply.

In order to satisfy the aforementioned requirements, the following components were installed within the enclosure:

- power supply filters,
- signal line filters.

As the protected IT equipment emits a considerable volume of heat during operation, it must be cooled – in this case, by removing hot air out of the shielding enclosure. For this purpose, two 15 cm x 15 cm Tecknit ventilation panels were used. Cold air is sucked into the chamber through one of these panels, while the hot air evacuates out the chamber through the other.

To facilitate installation of protected IT equipment, the chamber is fitted with removable doors with EMI gaskets, mounted using pins. The dimensions of the chamber allow for the installation of equipment, which is no larger than (15×35×55) cm in size.

The main body of the shielding enclosure is made out galvanized steel sheets with a thickness of 1.5 mm. The sheet at the front is 5 mm thick, and made out of duralumin, with the transient panel made out of 2 mm thick brass.

A block diagram of the shielding enclosure described herein can be found in Fig. 4. Dimensions of the chamber are presented in Fig. 5, and its external view is presented in Fig. 6. An example of how such a shielding chamber can be used is discussed and presented in the reference [7]. The shielding effectiveness of the shielding chamber described herein is presented as a diagram in Fig. 7.

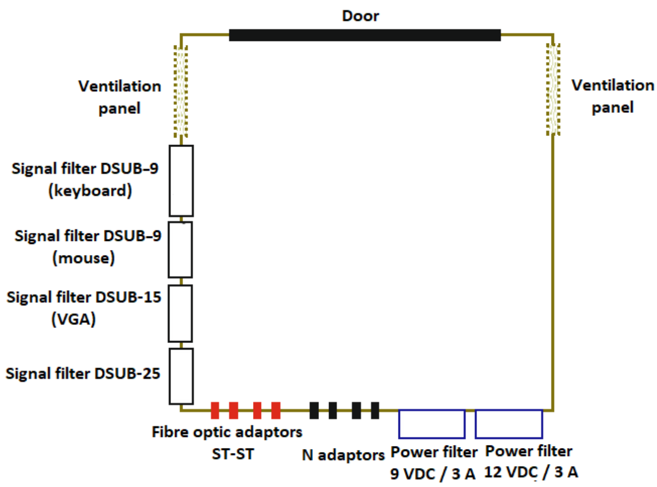

Fig. 4. Block diagram of the enclosure.

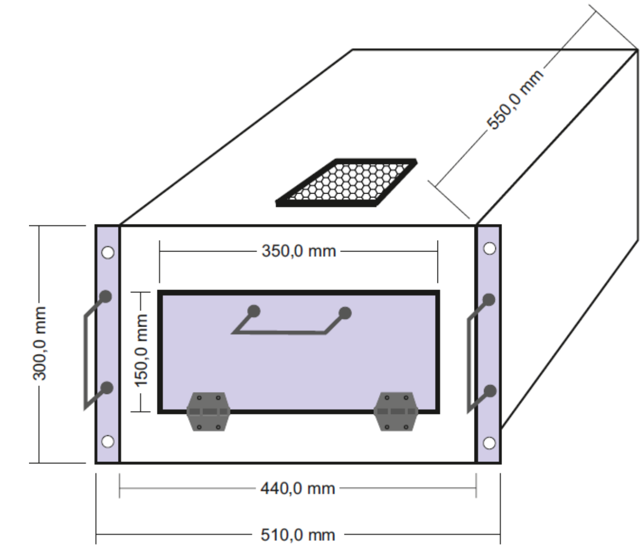

Fig. 5. Dimensions of the enclosure.

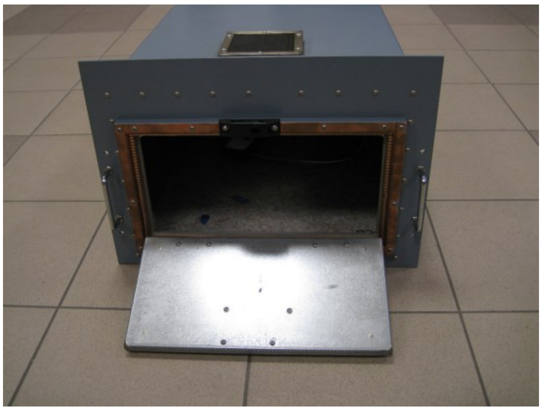

Fig. 6. External view of the front panel of the shielding enclosure.

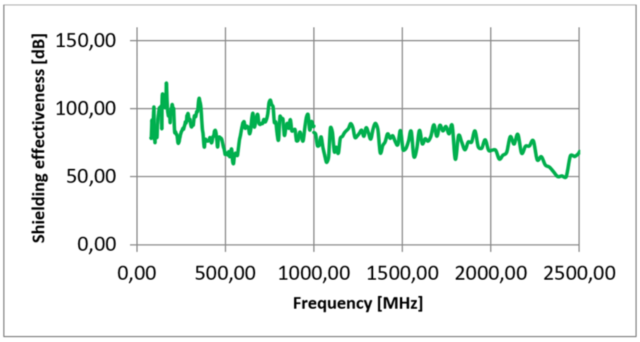

Fig. 7. Resulting A_s of the shielding enclosure.

Conclusion

Electromagnetic safety of IT equipment is affected by attenuation A_{dr} brought in by the signal propagation path between the source of the compromising radiation and the antenna of infiltrating system. The article presents original analytical relationships necessary to estimate the attenuation value of the propagation path of the potential radiated compromising emanation signal, which corresponds to the most probable scenarios of locating IT equipment in relation to the location of the potential infiltrating system. The article analyzes various location scenarios for IT equipment – a potential source of compromising emanation – with a potential infiltrating system positioned within or outside the boundaries of a building, in which said IT equipment is located. It was determined that from the point of view of the location of a potential infiltrating system, the risk of infiltration, as measured by the value of attenuation brought by the propagation path of the emission signal is comparable for all analyzed scenarios.

The paper presents an example design for a solution protecting against electromagnetic compromising emanations, namely a shielding enclosure equipped with required filtering hardware, which can fit a single item of IT equipment inside.

The shielding enclosure as designed, with protected IT equipment being installed within, can be comfortably used in practice. The solution proposed does not require any interference in the internal design of the equipment being protected. The user of this solution needs only to install the equipment being protected inside the shielding enclosure.

References

[1] EN 55032:2015, "Electromagnetic compatibility of multimedia equipment - Emission Requirements".

[2] Recommendation ITU R P.1238 8 (07/2015), "Propagation data prediction methods for the planning of indoor radiocommunication systems and radio local area networks in the frequency range 300 MHz to 100 GHz", ITU, Geneva, 2015.

[3] I. Rodriguez, H. C. Nguyen, N. T. K. Jorgensen, T. B. Sorensen, P. Mogensen, "Radio Propagation into Modern Buildings: Attenuation Measurements in the Range from 800 MHz to 18 GHz", 2014 IEEE 80th Vehicular technology Conference (VTC2014-Fall), Vancouver, BC, 2014, pp. 1-5, DOI: 10.1109/VTCFall.2014.6966147.

[4] J. Łopatka, L. Nowosielski, M. Siłaczuk, "Modelling of electromagnetic wave propagation with the use of the ray-tracing method", Progress in Electromagnetics Research Symposium 2014, Conference Proceedings, Guangzhou, China, 2014, s. 2741–2745, ISSN 1559-9450.

[5] L. Nowosielski, J. Michalak, "Shielding effectiveness required for IT equipment enclosures", PIERS 2017 Conference Proceedings, Singapore.

[6] L. Nowosielski, J. Michalak, M. Nowosielski, "Applications of IT equipment protective solutions against electromagnetic compromising emanations", 2018 40th Progress in Electromagnetics Research Symposium (PIERS), Toyama, Japan, 01-04.08.2018 r.

[7] A. Kaszuba, R. Chęciński, M. Kryk, J. Łopatka, L. Nowosielski, "Electromagnetically Shielded Real-time MANET Testbed", PIERS 2014 Conference Proceedings, 25÷28.08.2014 r., Guangzhou, China,ISSN 1559-9450, Pages 2746–2750.

[8] M. G. Kuhn, "Compromising emanations: Eavesdropping risks of computer displays" Technical Report UCAM-CL-TR-577, University of Cambridge, 2003, ISSN 1476-2986.

[9] Zhou C., Gui L. "Shielding effectiveness measurement of small size metal enclosure", 2016 Asia-Pacific International Symposium on Electromagnetic Compatibility (APEMC), IEEE Xplore, Shenzhen, China, 2016, s. 417-419, DOI: 10.1109/APEMC.2016.7522755.

[10] Zhou H., Yan L., Fang M., Zhao X., Qiang Liu Q. "Shielding effectiveness prediction of metallic structures with thin slots using FDTD", 2018 IEEE International Symposium on Electromagnetic Compatibility and 2018 IEEE Asia-Pacific Symposium on Electromagnetic Compatibility (EMC/APEMC), IEEE Xplore, 2018, s. 359-362, DOI: 10.1109/ISEMC.2018.8393798.