International Journal of Innovative Technology and Exploring Engineering (IJITEE)
ISSN: 2278-3075 (Online), Volume-9 Issue-4, February 2020

The Model of Localization Precision for Detection of Hidden Transmitters

Savchenko Vitalii, Syrotenko Anatolii, Shchypanskyi Pavlo, Matsko Oleksander, Laptiev Oleksander

Abstract*: The article deals with the problem of remote search for hidden transmitters in a large office. Such a search should be performed inconspicuously for office visitors so that an attacker could not turn off the transmitter during the search. The complexity of the inconspicuous manual search for bugs is shown and the necessity of using a remote automated search for illegal transmitters is substantiated. The decision on the use of remote search can be made on the basis of a priori knowledge of the localization precision of a hidden transmitter. To calculate the precision of localization, a mathematical model is proposed on the basis of measuring the distances from the receiving antennas to the alleged hidden transmitter. The range and the precision of the distance from the transmitter to the receiving antenna can be calculated by knowing the attenuation of the signal during its propagation under certain conditions. The more heterogeneous the wave propagation environment, the greater the error in determining the range. The localization precision of the hidden transmitter is calculated using the Least Squares Method. The main parameter of localization precision is the Mean Square Error of its location. It is shown that the values of the Mean Square Error of localization depend both on the precision of the range measurement and on the position of the receiving antennas relative to the transmitter. The capabilities of the developed model for determining the required number of receiving antennas at a given localization precision are also shown. The simulation of a multi-storey office building was carried out and the parameters of localization precision were estimated for a different number of receiving antennas. The possibility of increasing the precision of localization with an increase in the number of antennas has been confirmed. The article concludes that it is advisable to use such a model when building scanners to search for illegal bugs and transmitters.

***Keywords*: hidden transmitter, Least Squares Method, localization precision, pseudorange.**

Revised Manuscript Received on February 28, 2020.

***** Correspondence Author

Savchenko Vitalii*, Doctor of Technical Science, Professor, Director of the Institute of Information Protection, State University of Telecommunications, Kyiv, Ukraine. Email: savitan@ukr.net +38067-5046012.

Syrotenko Anatolii, Doctor of Military Science, Head of Ivan Cherniakhovskyi National Defense University of Ukraine, Kyiv, Ukraine. Email: info@nuou.org.ua

Shchypanskyi Pavlo, PhD, Professor, Deputy Head of Ivan Cherniakhovskyi National Defense University of Ukraine, Kyiv, Ukraine. Email: info@nuou.org.ua

Matsko Oleksander, PhD, Professor, Head of Logistic and IT institute, Ivan Cherniakhovskyi National Defense University of Ukraine, Kyiv, Ukraine. Email: macko2006@ukr.net

Laptiev Oleksander, PhD, Senior Researcher, Institute of Information Protection, State University of Telecommunications, Kyiv, Ukraine. Email: alaptev64@ukr.net

I. INTRODUCTION

Information is one of the most valuable assets of most modern companies. With the value of information increase, the number of those who wish to obtain this information also increases for use in their own interests or for the purposes of third parties. One way to obtain important information is to record it using audio or video bugs, followed by transmission through hidden transmitters [1]. The search and definition of such transmitters is quite complicated as the task is complicated by many factors.

First, developers of hidden transmitters use increasingly sophisticated methods and algorithms to hide the transmission of these devices.

Secondly, the use of radio broadcasting for communication, data transmission and control commands is on the increase, and now almost all radio frequency spectrums are involved in the operation of legal radio transmitters. This complicates and makes it particularly difficult to search for hidden transmitters.

A considerable number of publications are devoted to the protection of information, search and localization of hidden transmitters. Thus, [2] describes the search and localization of hidden transmitters by means of search complexes and auxiliaries. The classification of hidden transmitters and the characteristic features of the detection of radio transmitters are given. However, the location of the transmitter is mainly based on the principle of detection with the help of additional search equipment, so manual search, which takes a very long time. The approach described in [3] is based on the "acoustic binding" method. For its implementation, it is necessary to use both search equipment (field indicator, universal search system, etc.) and a low-frequency amplifier with an acoustic speaker. This allows you to implement the method of searching bugs / transmitters using acoustic communication. In this case, the disadvantages of frequency modulation (FM) are used, which leads to the appearance of spurious amplitude modulation (AM). The acoustic signal is amplified by the amplifier and sent to the loudspeaker. After that, it is picked up by the bug's microphone and a positive acoustic connection is formed. When the speaker approaches the bug at close range, a low-frequency amplifier self-excitation mode appears, similar to the self-excitation mode in conventional sound amplification systems when the microphone is brought close to the speakers. In this case, a specific acoustic signal, similar to a whistle, informs the operator about the presence of an acoustic bug near the speaker.

The distance from the speaker to the bug depends on the speaker volume level. The higher the volume, the greater the distance from the bug to the speaker. The disadvantage of this approach is the large amount of manual labor and time spent. In addition, for modern digital technology, such a technology can already be considered as a rarity.

[4] Describes methods for finding and locating hidden transmitters using search equipment (manual methods), and search complexes – a semi-automatic method of using a radiometer rangefinder (hyperbolic method). It does not completely accomplish the task of locating digital hidden transmitters.

[5] and [6] describe methods of locating transmitters. After finding an unknown radio signal in a controlled area, it searches for hidden transmitters. A method of detecting the location of a radio bug when used in conjunction with a radio receiver measuring devices (hyperbolic method) is used. For example: when detecting the radiation of a radio bug with amplitude (AM) or frequency (FM, NFM, WFM) signal modulation, such a device is connected to the line output or output of the receiver's main phones. (In hardware, software systems to the linear output of the laptop).

It is assumed [7] that test acoustic pulsed signals are generated in the devices, which are transmitted through the loudspeaker (the speaker can be built-in or remote). A hidden bug receives such an acoustic signal, converts it into an electrical signal and transfers it to the transmitter modulator. As a result, the bug's radio signal will be modulated by the test signal. The scanner receiver receives the radio signal transmitted by the bug, after which a test acoustic signal will be heard in the receiver's speaker. The received signal is sent to the software package, where it is compared with the test signal. Also, the distance is measured by the delay time of the pulse from the detector of the receiver with respect to the emitted test pulse. The measurement of the distance in time of arrival of the pulse is based on the fact that an acoustic signal propagates in air at the speed of sound, and radio signals propagate at the speed of light, that is, significantly higher than the speed of sound. , Sometimes the propagation of a radio signal from a bug to a receiver is not taken into account. This method is very similar to the "acoustic binding" method described above in [3]. The disadvantage of this method is the inability to identify them in the case of complex digital signals disguised as legal transmitters. The transmitter localization procedure is also complicated, because single-point technology is used to distribute the test signal and receive its response.

To determine the location of the bugs, a room diagram is compiled and two or three speaker locations are selected [8]. The sound column is sequentially placed at selected points and the distance to the radio bug is measured. The chart draws circles centered at the measurement points and a radius corresponding to the measured range. The circuit defines the intersection of circles. Corrections will be correct if the circles in the diagram intersect at one point in all dimensions.

The error in measuring the distance to the radio transmitter will be determined by the shape of the test pulse (steepness of the leading edge) and the principle of construction (operation) of the comparison unit. To increase the precision of range measurement, pulses with a complex type of modulation (for example, linear frequency modulation) and special processing devices that provide compression of the pulse after processing are used.

In modern instruments for measuring the distance to the bug, the measurement error is from 10 to 20 cm. [9]. This principle works great when searching for and detecting errors in analogue radio that work continuously. For localization of digital bugs, especially when pulsed transmission of information (radio bugs with accumulated information and transmission in pulsed mode), this principle does not work, since the localization time exceeds the transmission time. In addition, most manual search methods for a large office are also not applicable, since they show the attacker the search process itself and lead to the shutdown of hidden transmitters for the verification period. Based on the above solution to the problem of localization of radio bugs, the problem of inconspicuous localization of a hidden transmitter remains very relevant. But the decision to use remote localization can be made only on the basis of knowledge of the precision of localization and the number of means (antennas) involved. The aim of this work is to develop a mathematical model of the precision characteristics of determining hidden transmitters, in particular, based on the range measurement method, which would take into account the topology of the entire search system.

II. THE MODEL OF LOCALIZATION PRECISION

A. The basic approach to the model of localization precision

As the main measurement parameter in the model, it is advisable to use pseudorange (PR) from the receiving antenna to the hidden transmitter [5]. DOP – Dilution of Precision is used to estimate the precision of the transmitter localization to determine the precision of the range parameter. The DOP shows in how many times the transmitter localization error – Mean Square Error (MSE) is greater than the pseudorange MSE. It is advisable to use gradient analysis methods to form a DOP model for receiving antennas of the search complex. To do this, it is necessary to linearize the navigation function by decomposing into a Taylor series the degrees of correction δ_j (j = 1,2,3,4) with the retention of the first members of the decomposition:

$$D_i - D_{0i} = \frac{\partial D_i}{\partial x_0}\delta_x + \frac{\partial D_i}{\partial y_0}\delta_y + \frac{\partial D_i}{\partial z_0}\delta_z + \frac{\partial D_i}{\partial w_0}\delta_w \ , \ i = 1,...,N \quad (1)$$

where D_i – measured pseudorange from *i*-antenna to hidden transmitter;

D_{0i} – countable pseudorange from *i*-antenna to hidden transmitter;

x_0, y_0, z_0 – rectangular coordinates of the transmitter in the geocentric coordinate system (GCS);

w_0 – correction for discrepancy of time scales expressed for clarity in units of length;

N – is the number of receiving antennas.

The partial derivatives included in system (1) make up the matrix of partial derivatives at the point of the hidden transmitter with coordinates (x_0, y_0, z_0), which is the basis for further calculation of the estimations of the transmitter localization errors:

$$\mathbf{C} = \begin{Vmatrix} \frac{\partial D_1}{\partial x} & \frac{\partial D_1}{\partial y} & \frac{\partial D_1}{\partial z} & \frac{\partial D_1}{\partial w} \\ \dots & \dots & \dots & \dots \\ \frac{\partial D_N}{\partial x} & \frac{\partial D_N}{\partial y} & \frac{\partial D_N}{\partial z} & \frac{\partial D_N}{\partial w} \end{Vmatrix}^{N\times 4}. \quad (2)$$

In our case, differentiating a function by the variables x, y, z, w gives the following matrix of partial derivatives:

$$\mathbf{C} = \begin{Vmatrix} \cos\alpha_1 & \cos\beta_1 & \cos\gamma_1 & 1 \\ \dots & \dots & \dots & \dots \\ \cos\alpha_N & \cos\beta_N & \cos\gamma_N & 1 \end{Vmatrix}^{N\times 4}. \quad (3)$$

The elements of the matrix (3) are the directing cosines of vectors directed from the transmitter to the receiving antennas in the geocentric coordinate system [10]. If you enter the column matrix **R** of the difference between the measured and the calculated pseudorange values $\mathbf{R} = \|D_i - D_{0i}\|^{N\times 1} = \|r_i\|^{N\times 1}$ and to correct the amendments $\delta_i \, (i = 1,2,3,4)$ in the form of a column matrix $\Delta^{\mathrm{T}} = \|\delta_1 \quad \delta_2 \quad \delta_3 \quad \delta_4\|$, then system (1) can be written

$$\mathbf{C\Delta = R}. \quad (4)$$

To make system (4) dimensionless, both of its parts must be multiplied by a weights matrix [11]:

$$\mathbf{P_0} = \begin{Vmatrix} p_1 & 0 & . & 0 \\ 0 & p_2 & . & 0 \\ . & . & . & . \\ 0 & 0 & . & p_N \end{Vmatrix}^{N\times N}, \; p_i = \frac{1}{\sigma_{Di}}, \quad (5)$$

where σ_{Di} – pseudorange MSE to the *i*-th antenna.

Then the system (4) will take the form

$$\mathbf{P_0 C\Delta = P_0 R}. \quad (6)$$

Using the least-squares method [12], minimizing the square of the discrepancy between the left and right parts of the system of conditional equations (6), we obtain the system of normal equations in the form

$$\mathbf{C^T P_0^T P_0 C\Delta = C^T P_0^T P_0 R}. \quad (7)$$

The product $\mathbf{P_0^T P_0}$ gives a diagonal matrix **P**, which elements are squares of elements of the matrix $\mathbf{P_0}$ and it is possible to write down

$$\mathbf{C^T PC\Delta = C^T PR}. \quad (8)$$

If we represent in (8) $\mathbf{C^T PC = A}$ and $\mathbf{C^T PR = B}$ then the system of equations can be written in the form

$$\mathbf{A\Delta = B}. \quad (9)$$

By multiplying the right and left sides of system (9) by the inverted matrix $\mathbf{A}^{-1}$, we can get a solution for corrections

$$\mathbf{\Delta = A^{-1}B}.$$

B. The localization precision parameter

The matrix $\mathbf{P}^{-1}$ that is part of the matrix $\mathbf{A}^{-1} = \mathbf{C}^{-1}\mathbf{P}^{-1}\left(\mathbf{C}^{-1}\right)^{\mathbf{T}}$ is a variance of the pseudorange measurements. The matrix $\mathbf{A}^{-1}$ itself has the content of the errors correlation matrix of the required parameters. The resulting location error can be expressed by the trace of the correlation matrix $\sigma_q = \left(Tr\left(\mathbf{K}_q\right)\right)^{\frac{1}{2}}$. In general terms, the expression for MS can be written as a relation $GDOP = \frac{\sigma_q}{\sigma_D}$, where *GDOP* – global dilution of precision, σ_D – MSE of pseudorange to the hidden transmitter; σ_q – MSE of the hidden transmitter localization.

So, MSE $\sigma_q = \left(Tr\left(\mathbf{K}_q\right)\right)^{\frac{1}{2}}$ can be taken as the main precision parameter for hidden transmitters localization. This indicator will indicate the precision of the localization of the transmitters on the basis of which both the number and the location of the receiving antennas can be determined.

C. Algorithm for calculating the precision field

Calculation of the precision field for determining the hidden transmitter can be done according to the following algorithm.

1. The installation coordinates of the receiving antennas $x_{A_i}, y_{A_i}, z_{A_i}$ are fixed.
2. The territory and levels within which the calculations will be made are determined. In the case of a multi-storey office, these may be separate floors of the building.
3. The entire territory for each floor is distributed on separate grid points in each of which the calculation of the Mean Square Error σ_q will be performed.
4. A single grid point is selected.
5. The distances D_i from each antenna to the grid point are calculated, which will make it possible to form a matrix of cosines (3).

6. The Mean Square Error of the measurement range from the antenna to the intended transmitter σ_{Di} is set or calculated. The matrix (5) is formed.

7. For a given grid point, using the formulas (8) - (9), the value of the Mean Square Error $\sigma_q = \left(Tr\left(\mathbf{K}_q\right)\right)^{\frac{1}{2}}$ of localization of the hidden transmitter is calculated.

8. Return to item 4.

After calculation for all grid points, the transition to the next floor is carried out. Similarly, a precision field should be built for each floor.

The constructed precision fields reflect the general picture of how accurately localization of a hidden transmitter is possible in a particular room or on the floor.

The lower the value of the Mean Square Error in the grid node, the better the localization precision of the hidden transmitter and the faster it can be found.

If the localization precision for the entire building is unsatisfactory, then the topology of the receiving antennas can be reviewed and all calculations repeated again.

III. SIMULATION RESULTS AND DISCUSSION

To analyze the precision field of the monitoring system with receiving antennas located in different parts of the building we will consider a typical office of 3 floors with basement and technical rooms on the 4-th floor, such as in Fig. 1.

The size of building is 90 m long, 45 m wide and 15 m tall as it is shown in Fig. 2. We select the zero level of the basement at the reference height.

Three receiving antennas in Fig. 2. have coordinates (length, width, height) with the beginning in the left down corner of the building as: (90,0,1)m; (0,45,1)m; (10,15,15)m. MSE of pseudorange measurements is 0.5 m.

The color map in fig. 3 shows that in some places the MSE value can be at a level of 1 to 3 m, which is quite acceptable with such a number and topology of receiving antennas. At the same time, part of the building (diagonally) is covered by very poor (15 m or more) MSE values. Which indicates the poor location of the receiving antennas: poor DOP.

For the next simulation (Fig. 4) we will take 4 receiving antennas with coordinates (90,0,1)m; (0,45,1)m; (10,15,15)m; (0,0,1)m.

The simulation results in Fig. 5 show that in the case of 4 receiving antennas, the MSE values throughout the territory remain at a level of 1 to 2 m without bursts of errors, which were in the presence of only 3 antennas. This is a significant improvement in localization precision.

Fig. 1. Typical office building

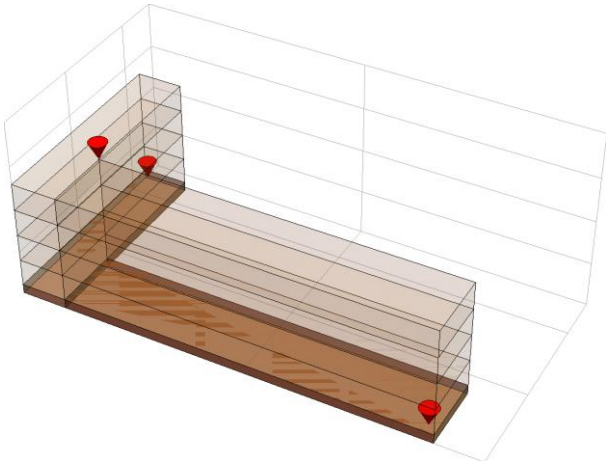
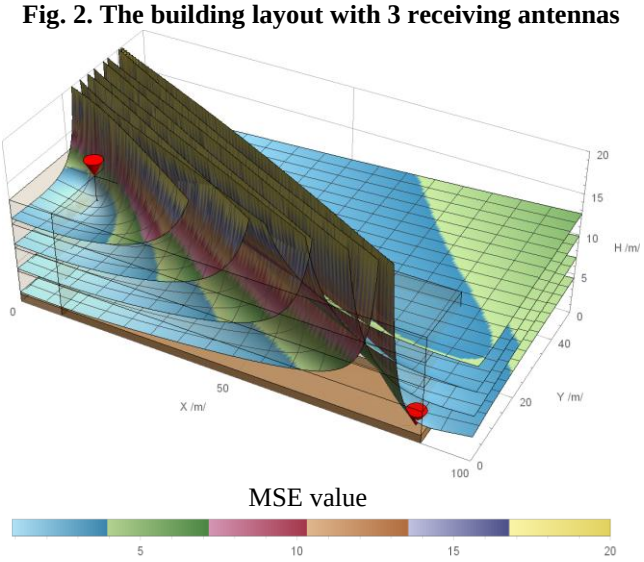


Fig. 2. The building layout with 3 receiving antennas



MSE value

Fig. 3. The field of localization precision in the case of 3 receiving antennas

The reason for this is the better mutual positioning of the receiving antennas and the intended covert transmitter. As in the previous case, the MSE value of the pseudorange measurement remains the same 0.5 m.

The exact simulation results are summarized in Table I. It can be seen that the minimum values of the Mean Square Error for 3 receiving antennas are about 0.91 m, and for 4 antennas about 0.75 m. Thus, it is obvious that an increase in the number of receiving antennas leads to an increase in localization precision.

It is also seen that on different floors the precision does not change significantly. This is because the antennas are located at the edges of the building and everything that is in the middle of the building can be localized with the same precision. That is, the wider the localization base, the larger the area of equal precision. This can be useful in the case of localization of hidden transmitters not in one building but in a group of buildings. At the same time, the proposed system topology does not allow achieving the minimum GDOP value, which for 4 antennas should be 1.41 [5]. With such a GDOP value, the minimum achievable precision value could be equal to 0.705 m, but the poor topology of the receiving and transmitting antennas does not allow achieving this result.

Thus, the need to use more receiving antennas to improve localization precision is once again confirmed.

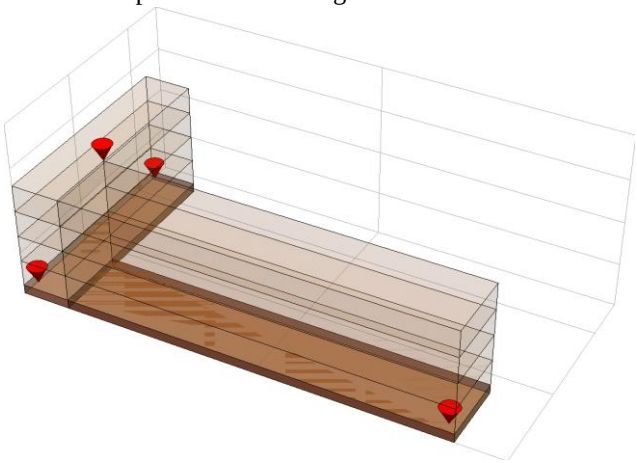


Fig. 4. The building layout with 4 receiving antennas

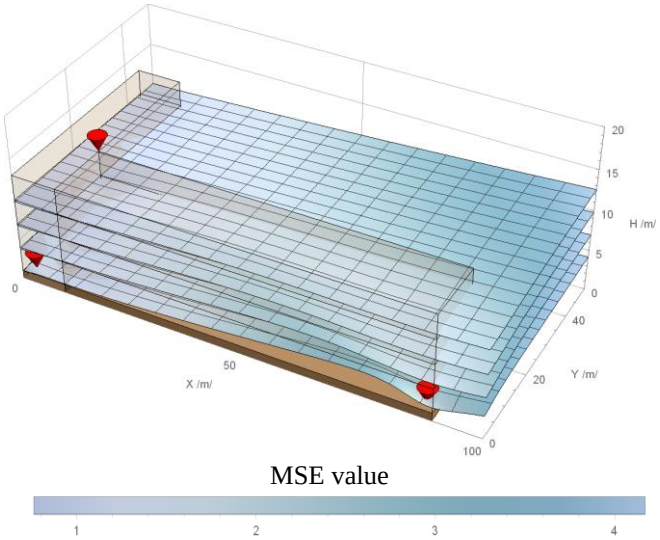


Fig. 5. The field of localization precision in the case of 4 receiving antennas

Thus, the proposed method for the precision of localization of hidden transmitters allows us to evaluate the precision of the location of the transmitter and, on the other hand, to determine the optimal location of the receiving antennas.

Table- I: Modelling Results

System variant: number of receiving antennas	Area	Mean Square Error of localization, m	
		Min	***Max***
3 antennas	Attic	0.913	413.80
	2	0.914	1119.06
	1	0.918	421.54
	Ground Flor	0.925	460.18
4 antennas	Attic	0.752	3.59
	2	0.753	3.79
	1	0.758	3.98
	Ground Flor	0.763	4.17

The minimum number of receiving antennas is 2. This is due to the need to solve the corresponding system of equations. At the same time, with only 2 antennas, the DOP will be the worst, since in this case it is impossible to provide a solution of the system of equations with sufficient precision, in particular due to a serious deterioration in the vertical DOP. The case with two antennas can only be used on a plane when there is no need to take into account the vertical coordinate (for example, in one-story buildings).

The algorithm of the method is designed so that with an increase in the number of receiving antennas, the localization precision of the hidden transmitter also increases. But this leads to a significant increase in the cost of the system and a decrease in its security, as visitors to the office may notice that radio control is being carried out. In this case, the attacker can disable the transmitter for the period of control.

The proposed method for determining precision based on range measurement can be applied not only to one building, but also to a group of buildings, thereby increasing stealth and reducing the cost and visibility of all control measures. The boundaries of the application of the method will be determined by the sensitivity of the receiving antennas.

Further research on the detection of hidden transmitters is the recognition of certain signal sources against the background of legally operating transmitters (mobile phones, access points, etc.), e.g. as shown in [13].

IV. CONCLUSION

The problem of remote search for hidden transmitters is becoming increasingly important. The decision to use a remote scanner can be made with an a priori knowledge of the localization precision of a hidden transmitter. Existing methods for constructing automated hidden transmitter search complexes do not evaluate the precision of their localization.

The proposed model of localization precision based on the Least Squares Method calculates the precision of the location of the hidden transmitter using the ranges and the precision of measuring distances from the transmitter to the receiving antennas. The resulting parameter of the model is the Mean Square Error of localization of the hidden transmitter. This approach is quite simple to implement in an automated complex of remote scanning and allows to localize the installation location of a hidden transmitter remotely.

In addition, it is possible to determine the required number and topology of receiving antennas of the search complex.

The simulation results confirm the possibility of using a remote localization scheme. By simulating a different number of receiving antennas and their location, it is possible to achieve a continuous localization field for hidden transmitters with high precision parameters.

REFERENCES

1. Dinesh Sathyamoorthy, Mohd Jalis Md Jelas & Shalini Shafii, “Wireless Spy Devices: a Review of Technologies and Detection Methods”, in *Defence S and T Technical Bulletin* 7(2): November 2014, p.130-139.
2. I. Svistun, “Detection and localization of radio microphone embedded devices using the Square M radio monitoring system”. Available: https://cyberleninka.ru/article/v/obnaruzhenie-i-lokalizatsiya-radiomikrofonnyh-zakladnyh-ustroystv-s-ispolzovaniem-kompleksa-radiovontroadrat

3. A. Horev, “Information leakage protection through technical channels”. Moscow: Russian State Guest Committee, 1998. 320 p.
4. A. Laptev, O. Barabash, Vi. Savchenko, Va. Savchenko, V. Sobchuk, “The method of searching for digital means of illegal reception of information in information systems in the working range of Wi-Fi” in *International Journal of Advanced Research in Science, Engineering and Technology*. Vol. 6, Issue 7, July 2019, pp. 10101-10105.
5. V. Savchenko, A. Vorobyov, R. Mykolaychuk, A. Mykolaychuk, T. Kursietov, “The Model of Accuracy of a Local Radio Navigation System Considering Unstable Performance of Individual Elements” in *Eastern European Journal of Advanced Technologies*, T.3, № 9 (81), 2016, p. 4-10.
6. A. Laptev, “The methodology of the recognition of the silent information capture by a potential offender”, *Science and Education a New Dimension. Natural and Technical Sciences*, VII (24), Issue: 200, 2019 July. Available: www.seanewdim.com p.27-31.
7. A.A. Laptev, V.A. Savchenko, O.V. Barabash, V.V. Savchenko, A.I. Matsko, “The method of searching for digital bugs of illegal information retrieval on the basis of cluster analysis”, *Magyar Tudományos Journal* Budapest, Hungary, No. 31, (2019), p. 33-37.
8. Ankit Jain. Detection on HF radio transmitters using passive geolocation techniques. Signal and Image processing. *Ecole nationale supérieure Mines-Télécom Atlantique*, 2019.
9. X. Li, J. Wang, C. Liu, L. Zhang, Z. Li, “Integrated WiFi/PDR/smartphone using an adaptive system noise extended Kalman filter algorithm for indoor localization”. *ISPRS Int. J. Geo-Inf.* 2016, p. 5-8.
10. Bonan Jin, Xiaosu Xu and Tao Zhang, “Robust Time-Difference-of-Arrival (TDOA) Localization Using Weighted Least Squares with Cone Tangent Plane Constraint”. *Sensors*, 2018, 18, p. 778-794.
11. Paula Tarrıo, Ana M. Bernardos and Jose R. Casar, “Weighted Least Squares Techniques for Improved Received Signal Strength Based Localization” *in Sensors* 11(9, · December 2011. P. 8569-8592.
12. C. Wang, Y. Chiou, S. Yeh, “A Location Algorithm Based on Radio Propagation Modeling for Indoor Wireless Local Area Networks”. *In Proceedings of 2005 IEEE 61st Vehicular Technology Conference*, VTC 2005-Spring, Stockholm, Sweden, 30 May–1 June 2005; Volume 5, pp. 2830–2834.
13. O. Laptiev, G. Shuklin, V. Savchenko, O. Barabash, A. Musienko, H. Haidur, “The Method of Hidden Transmitters Detection based on the Differential Transformation Model”, *International Journal of Advanced Trends in Computer Science and Engineering*, 2019, No.6, p. 2840-2846.

AUTHORS PROFILE

Savchenko Vitalii, Doctor of Technical Science, Professor, Director of the Institute of Information Protection, State University of Telecommunications, Kyiv, Ukraine.
In 1990 graduated from the Military Aviation Engineering School and served in the Air Force of Ukraine in the meteorological service. In 2000 began to engage in science. In 2005 received a PhD in Navigation and in 2012 got a Doctors degree in Information Technology. In 2017 resigned from the Armed Forces. Retired Colonel. Field of Interest: navigation, information technology, cybersecurity. The author of 5 computer models for teaching students and the author of more than 150 scientific publications. Teaches disciplines on protecting objects from unauthorized access, searching for hidden bugs, methods of counteracting technical radio intelligence.

Syrotenko Anatolii, Lieutenant General, Doctor of Military Science, Head of Ivan Cherniakhovskyi National Defense University of Ukraine, Kyiv, Ukraine.
In 1981 graduated from the Kharkiv Tank Command School. Was a commander of a tank platoon, a company, a battalion chief of staff, a battalion commander, a deputy regiment commander. In 2004 received the rank of Major General. Since August 2017 has been Head of Ivan Cherniakhovskyi National Defense University of Ukraine. In 2018 got a Doctors degree in Military Science. Scientific interests: military management, strategic operations, counteraction to foreign intelligence, technical facilities of security. The author of more than 50 scientific publications.

Shchypanskyi Pavlo, Major General, PhD, Professor, Deputy Head of Ivan Cherniakhovskyi National Defense University of Ukraine, Kyiv, Ukraine.
Graduated from the Military School of Air Defense. Served in the Air Force and Air Defense of Ukraine. Has a considerable practical experience in military service. Many times participated in combat firing of air defense systems. Began to study science in 1998. Was a lecturer at the Military Academy and head of the Air and Air Defense Institute. In 2002 received Ph.D. in military sciences. The author of 80 scientific publications on military topics and has 15 patents for inventions.

Matsko Oleksander, Colonel, PhD, Professor, Head of Logistic and IT institute, Ivan Cherniakhovskyi National Defense University of Ukraine, Kyiv, Ukraine.
Graduated from the Military Engineering School of the Land Forces. Has served in the military units as an engineer and the chief of the engineering service. Has a considerable combat experience. Started as a researcher in 2002. Areas of interest: application of units of engineering troops, electronic warfare, counteraction to radio intelligence, security of information systems, cyber security. Has more than 70 scientific publications, monographs and patents for invention. Teaches Combat operations support and the Information technologies applications at the University of Defense.

Laptiev Oleksander, PhD, Senior Researcher, Institute of Information Protection, State University of Telecommunications, Kyiv, Ukraine.
Graduated from the radio faculty of the Military Aviation Engineering College in 1986. Served in the Air Force units and the Air Force Research Center. In 1994 got Ph.D. in radio technology. Retired Colonel. After resignation from the Armed Forces has worked as an information security engineer and information security expert at various enterprises. Has an extensive practical experience in finding hidden bugs and transmitters. Areas of interest: information security, hidden transmitter search, radio intelligence. Author of more than 40 scientific publications on information security.