Visnyk NTUU KPI Seriia – Radiotekhnika Radioaparatobuduvannia, 2025, Iss. 102, pp. 5–14

UDC 621.396.6

Mathematical Model of a Radiobeam Detection System Signal

Storozh V. H., Fabirovskyy S. Ye., Prudyus I. N., Matiieshyn Yu. M., Oborzhytskyy V. I., Hurmach R. M.

Lviv Polytechnic National University, Lviv, Ukraine

E-mail: *fabirovskii@gmail.com*

This paper presents the development of a mathematical model of the information signal of a radiobeam detection system for studying the factors influencing its parameters. The model is based on the Huygens–Fresnel principle. The intruder is represented by an equivalent rectangle, which sequentially occludes certain regions of the wave phase front during movement. The information signal is defined as the normalized difference between the field strength in the absence of the intruder model and the field strength in its presence and motion. The mathematical model of the information signal was verified by physical simulation at a frequency of 9.3 GHz using a R2-61 panoramic VSWR meter, standard horn antennas, and metal plates of various sizes that were moved across the detection zone. The model demonstrated good agreement with experimental data, allowing its application for predicting the waveform of information signals. A series of computational experiments was performed for frequencies of 10.5 GHz, 5.8 GHz, 2.5 GHz, and 1.0 GHz for a 50 m security perimeter. Three intruder movement scenarios were analyzed: upright, bent over, and crawling. It was shown that at higher frequencies (10.5 GHz), the signal during crawling exhibits a positive increment, creating a risk of undetected intruder crossing in systems configured to trigger on negative increments. Lowering the frequency to 5.8 GHz and 2.5 GHz provides more stable negative increments at slightly reduced signal amplitude. At 1.0 GHz, a significant reduction in the signal level is observed. The proposed mathematical model of the information signal accounts for the operating frequency, antenna spacing, intruder geometry, its position, and movement method. This makes it possible to create a database of signals for a specific security perimeter, enabling the use of correlation-based signal processing methods. The obtained results allow selecting the optimal frequency range for a given security perimeter, reducing the volume of experimental testing on a security perimeter, and improving information signal processing algorithms, which will enhance detection reliability and reduce the number of false alarms.

Keywords: detection; radiobeam; perimeter security means; mathematical model

DOI: 10.64915/RADAP.2025.102.5-14

Introduction

When designing security systems for critical facilities, both military and civilian, priority is given to measures that prevent potential intruders from entering the facility's premises. These measures can be classified as engineering, organizational, and technical [1–3].

Through engineering measures, a reliable barrier is implemented that prevents intruder penetration or significantly slows down their progress, and actions are taken to minimize the number of areas within the territory where an intruder could remain undetected. Through organizational measures, an access control system is implemented, and preventive work is carried out with the facility personnel. Technical measures involve the installation of specialized devices for security purposes, which comprise a combination of an alarm system and a warning signal transmission system. These devices are designed to detect unauthorized intruder access to a protected facility and to generate an alarm signal for transmission to the central security console. The key element in this context is the technical detection equipment.

Technical detection equipment is based on various physical principles, but all share the common feature of converting the intruder's physical actions – such as movement, pressure on the ground or on a barrier, and other interactions – into an electrical signal, referred to as the information signal. Upon generation of the information signal by the detection device, the signal is amplified, processed, and analysed according to a specific algorithm, enabling automatic generation of an alarm notification if the signal parameters meet pre-established criteria.

In addition to large stationary facilities, where the principles of security system design are well-established, there exist small, localized objects that operate autonomously in relatively unpopulated areas, such as mobile network operator relay towers, various aerial surveillance devices and systems, and similar

installations. For such sites, it is necessary that the security system be simple to install and operate, and, if required, capable of being camouflaged to blend with the surrounding landscape and exterior structures.

Among a wide range of technical detection devices, radiobeam systems, also known as bistatic radars, are among the most effective and reliable. In the simplest configuration, a radiobeam detection system consists of two antennas — a transmitting antenna and a receiving antenna. When an intruder enters the area between the transmitting and receiving antennas, the signal level at the receiver output changes, providing information about the intrusion, i.e., the information signal. Such systems do not require prior specialized engineering preparation of the terrain. They can be deployed both in facilities with perimeter fencing and in open areas. If necessary, the linear components of these systems can be camouflaged as exterior objects. A wide range of such devices is available on the market [4,5] and others designed for different frequency ranges and security perimeter lengths. At the same time, a considerable number of researchers are engaged in the study and improvement of such detection systems.

In particular, in [6, 7] the optimal deployment of such detection systems for intrusion detection is being studied, with an emphasis on the coverage of a network of bistatic radars, consisting of multiple transmitters and receivers, where any transmitter–receiver pair can form a bistatic radar. Operational algorithms for these systems are proposed.

The study [8] examines measures to reduce the impact of destabilizing factors, such as weather conditions, vegetation, and animals, on the operation of the detection system. It has been established that the increase in the information signal level, which ensures a reduction in false alarms, is simultaneously influenced by the operating frequency, antenna design, and the employed digital signal processing methods. Several patents are also dedicated to this topic. For example, in [9] a bistatic radar is considered in which passive reflectors are used to implement a closed security perimeter, significantly reducing the overall cost of the security system. And in [10] a bidirectional bistatic radar is analysed, in which the use of transceiver modules at each end enables the formation of two information signals from the intruder, thereby significantly enhancing detection performance.

However, a drawback of radiobeam detection devices is the presence of “dead zones” and the necessity to provide a considerable “exclusion zone”. Therefore, the study of the principles of information signal formation, depending on the intruder’s method of crossing the security perimeter, and the determination of the detection zone dimensions remains a relevant and important task.

1 Development and verification of a mathematical model of the information signal of a radiobeam detection device

The operating principle of the radiobeam detection device described above is illustrated in Fig. 1.

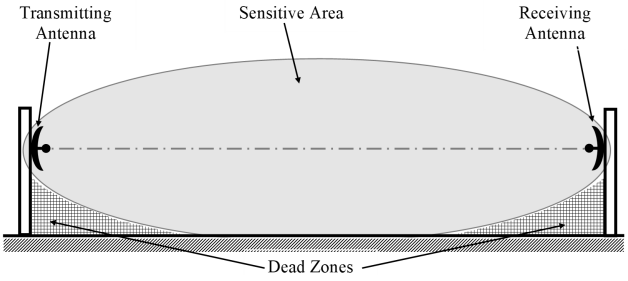

Fig. 1. Principle of construction of a radiobeam detection device

It consists of a spatially separated microwave transmitter and receiver, each equipped with a corresponding transmitting and receiving antenna. Ideally, a sensitive area is formed between the antennas in the shape of a rotational ellipsoid. Its transverse dimensions depend on the distance between the antennas and the operating frequency [11]. The higher the operating frequency, the narrower the detection zone width for the same distance, and vice versa. When an intruder appears and moves within the sensitive zone between the antennas, the amplitude of the microwave signal at the output of the receiving antenna changes. This amplitude variation, after detection and amplification, serves as the information signal. Following its amplification and processing according to a predefined algorithm, a conclusion is made regarding the presence or absence of an intruder.

Since the sensitive area has the shape of an ellipsoid, it is evident that so-called “dead zones” will exist in the immediate vicinity of the antennas, where the level of the information signal will be minimal. These regions are shaded in Fig. 1. The amplitude and shape of the information signal will also be influenced by the manner of movement: standing upright, crouching, or crawling.

Experimental study and investigation of the amplitude and waveform of the information signal, as well as the influence of “dead zones” on its parameters as a function of operating frequency, antenna spacing, and manner of movement, require considerable resources and labour efforts. Therefore, it is necessary to develop a mathematical model of the information signal of a radiobeam detection device, which will make it possible to determine the influence of the relative positioning of the transmitting and receiving antennas, operating frequency, intruder dimensions, and manner of movement on the parameters of the information signal.

As is well known, the field at the reception point can conveniently be determined based on the Huygens–Fresnel principle [11–13]. In this approach, each point of the wave front is considered a secondary source of a spherical wave, or, equivalently, a Huygens element. A Huygens element is an elementary patch of the wave front. Each side of this patch is significantly smaller than the wavelength at the specified operating frequency. The radiation pattern, whose cross-section in the $z0y$ plane is shown by a dashed line in Fig. 2, is described by a function known as a cardioid.

$$f(\Theta) = \frac{\cos(\Theta) + 1}{2}, \tag{1}$$

where the angle Θ is measured from the normal to the plane of the Huygens element (Fig. 2).

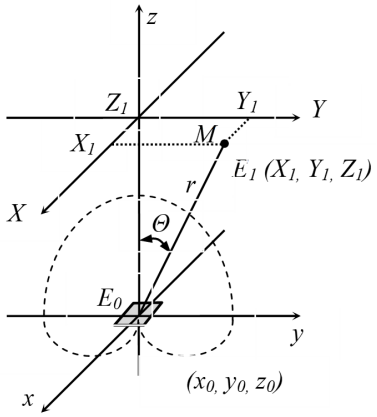

Fig. 2. For the calculation of the radiation field of a Huygens element

To determine the electric field intensity E_1 at the observation point M, it is necessary to know the electric field intensity E_0 of the Huygens element, the distance r between them, and the angle Θ between the z axis and the direction toward the observation point [11,13]:

$$E_1 = E_0 \frac{e^{-j\beta \cdot r}}{r} \cdot \frac{\cos(\Theta) + 1}{2}, \tag{2}$$

where $\beta = \frac{2\pi}{\lambda}$ – phase coefficient (phase constant).

Given the coordinates of the Huygens element (x_0, y_0, z_0) and the observation point (X_1, Y_1, Z_1), the distance r and the cosine of the angle Θ can be determined from the geometric construction (Fig. 2). The distance r:

$$r = \sqrt{(X_1 - x_0)^2 + (Y_1 - y_0)^2 + (Z_1 - z_0)^2}, \tag{3}$$

and cosine of the angle Θ:

$$\cos(\Theta) = \frac{(Z_1 - z_0)}{\sqrt{(X_1 - x_0)^2 + (Y_1 - y_0)^2 + (Z_1 - z_0)^2}}. \tag{4}$$

Omitting the intermediate steps, and based on expressions (2), (3), and (4), we obtain:

$$E_1 = E_0 \cdot e^{-j\beta \cdot \sqrt{(X_1 - x_0)^2 + (Y_1 - y_0)^2 + (Z_1 - z_0)^2}} \times \times \frac{\left((Z_1 - z_0) + \sqrt{(X_1 - x_0)^2 + (Y_1 - y_0)^2 + (Z_1 - z_0)^2}\right)}{2 \cdot \left((X_1 - x_0)^2 + (Y_1 - y_0)^2 + (Z_1 - z_0)^2\right)}. \tag{5}$$

In radiobeam detection devices, the width of the detection zone is significantly smaller than its length. Therefore, the angle $\Theta \to 0$, $\cos(\Theta) \to 1$, and thus expression (1) also approaches unity. Consequently, for this case, the influence of the directional properties of the Huygens element can be neglected, which considerably simplifies the expression for calculating the field from a single element:

$$E_1 = E_0 \frac{e^{-j\beta \cdot \sqrt{(X_1 - x_0)^2 + (Y_1 - y_0)^2 + (Z_1 - z_0)^2}}}{\sqrt{(X_1 - x_0)^2 + (Y_1 - y_0)^2 + (Z_1 - z_0)^2}}. \tag{6}$$

At the location of the receiving antenna, the field is determined as the superposition of the fields from all Huygens' elements into which the wave phase front is conventionally divided. As a result, a certain field strength level is established at the receiving point, and corresponding signal amplitude is formed at the receiver output. When an intruder crosses the security perimeter, they sequentially obscure certain portions of the wave phase front corresponding to different Fresnel zones.

To reduce the complexity of the expressions and facilitate subsequent calculations, several new notations are introduced, as shown in Fig. 3.

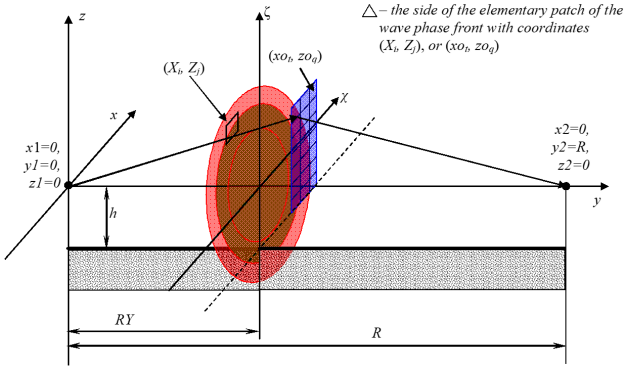

Fig. 3. Geometry of the mathematical model of the information signal

At the point with coordinates (x_1, y_1, z_1) is located the phase center of the transmitting antenna, while at a distance R from it, at the point with coordinates (x_2, y_2, z_2), is located the phase center of the receiving antenna. In the $(\chi 0\zeta)$ plane, at a distance RY from the transmitting antenna, an intruder moves, which is conventionally represented as a rectangle composed of a certain number of elementary square patches with

side Δ, much smaller than the wavelength. The coordinates of these elementary patches in the $(\chi 0\zeta)$ plane are (xo_t, zo_q). As the intruder model moves along the χ-axis, it sequentially obscures the corresponding elementary patches with coordinates (X_i, Y_j), into which the wave phase front is discretized, thereby simulating the process of information signal formation.

The sequence of the process for modeling the shape of the information signal can be presented as follows. First, the field distribution is determined in the $(\chi 0\zeta)$ plane, through which the intruder model will move (see Fig. 3).

$$E_{i,j} = E_0 \frac{e^{-j\beta\cdot\sqrt{(x_1-X_j)^2+(y_1-RY)^2+(z_1-Z_j)^2}}}{\sqrt{(x_1-X_j)^2+(y_1-RY)^2+(z_1-Z_j)^2}} \quad (7)$$

Next, by summing expression (7) over both coordinates χ and ζ, the field at the location of the receiving antenna with coordinates (x_2, y_2, z_2) is determined. This constitutes the so-called reference signal:

$$ER = \sum_{i=0}^{N}\sum_{j=0}^{M} E_{i,j} \times \times \frac{e^{-j\beta\cdot\sqrt{(x_2-X_j)^2+(y_2-RY)^2+(z_2-Z_j)^2}}}{\sqrt{(x_2-X_j)^2+(y_2-RY)^2+(z_2-Z_j)^2}}. \quad (8)$$

By performing analogous steps, the field distribution in the plane that will be obscured by the intruder model as it moves along the χ coordinate is determined:

$$EP_{t,\theta}(\chi) = E_0 \times \times \frac{e^{-j\beta\cdot\sqrt{(x_1-xo_t+\chi)^2+(y_1-RY)^2+(z_1-zo_\theta)^2}}}{\sqrt{(x_1-xo_t+\chi)^2+(y_1-RY)^2+(z_1-zo_\theta)^2}}. \quad (9)$$

As a result, the field at the location of the receiving antenna will change:

$$EOB(\chi) = \sum_{t=0}^{T}\sum_{\theta=0}^{\Theta} E_{t,\theta}(\chi) \times \times \frac{e^{-j\beta\cdot\sqrt{(x_2-xo_t+\chi)^2+(y_2-RY)^2+(z_2-zo_\theta)^2}}}{\sqrt{(x_2-xo_t+\chi)^2+(y_2-RY)^2+(z_2-zo_\theta)^2}}. \quad (10)$$

The information signal is defined as the difference between the field magnitude at the location of the receiving antenna in the absence of the intruder model, determined by expression (8), and the change in field intensity caused by its movement (10). For convenience in comparing simulation results under different conditions, this difference is suitably normalized with respect to the magnitude of the field intensity at the receiving antenna location in the absence of the intruder model:

$$S(\chi) = \frac{ER - EOB(\chi)}{|ER|}. \quad (11)$$

The developed mathematical model of the signal enables the investigation of the shape of the information signal and allows assessment of the impact of the operating frequency, the length of the security perimeter, the intruder's dimensions, and the manner of their movement relative to the antennas of the radiobeam security device on the parameters of this signal.

As noted above, when an intruder crosses the security perimeter, they sequentially obscure certain portions of the Fresnel zones, which is the cause of the information signal. However, the intruder may traverse the security perimeter in different ways [14]: standing upright, bent over, or crawling. In a first approximation, it is convenient to represent the intruder as equivalent rectangles [15, 16], which are appropriately positioned relative to the Fresnel zones (Fig. 4).

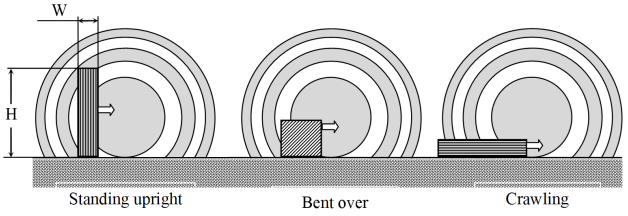

Fig. 4. Representation of an intruder crossing the security perimeter by equivalent rectangles

Thus, in each case, the signal will differ both in amplitude and in shape. Information about the parameters of the information signal is particularly important when developing the processing and analysis of information signal algorithm for any detection device, as it ensures reliable intruder detection and reduces the probability of false alarms.

The verification of the proposed mathematical model was carried out through physical simulation at a frequency of 9.3 GHz. The security perimeter was simulated using two horn antennas with a gain of 19 dBi - transmitting and receiving - placed 230 cm apart, while the intruders were represented by two metal plates measuring 125×315 mm and 222×315 mm. The measurements were carried out using a panoramic VSWR meter R2-61.

The plates were sequentially mounted between the transmitting and receiving antennas on a special mechanism that provided transverse displacement in 0.5 cm increments in the vertical orientation, thus simulating the crossing of the security perimeter. The comparison of experimental and simulation results for the 125×315 mm plate is shown in Fig. 5, and for the 222×315 mm plate in Fig. 6.

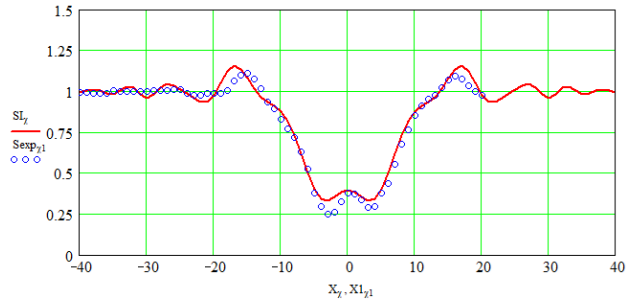

Fig. 5. Comparison of simulation results (solid line) and physical experiment (points) for the plate with dimensions 125×315 mm

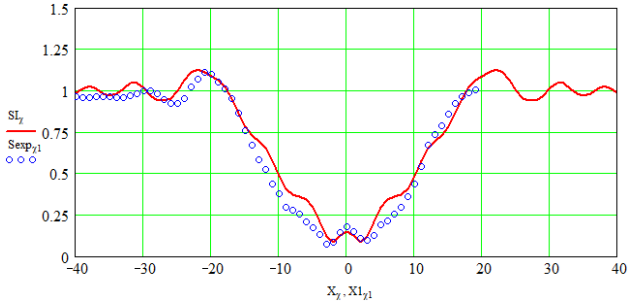

Fig. 6. Comparison of simulation results (solid line) and physical experiment (points) for the plate with dimensions 222×315 mm

In both graphs, the signal amplitude is normalized with respect to the level in the absence of any objects in the sensitive zone, and the numerical values along the x-axis correspond to centimeters. The incomplete data along the x-axis for the physical experiment is due to the limited travel range of the displacement mechanism. The verification demonstrated a sufficiently good agreement between the simulation and experimental results. Therefore, this model can be used for further studies.

2 Modeling of the information signal waveform during intruder penetration of the security perimeter

To simulate the shape of the information signal, the intruder is represented by an equivalent rectangle (see Fig. 4) with dimensions H along the ζ-axis and W along the χ-axis. For modeling an intruder walking upright, H = 1.8 m and W = 0.42 m are assumed; for a bent over, H = 0.85 m and W = 0.9 m; and for crawling, H = 0.4 m and W = 1.9 m. In all three cases, the cross-sectional area of the intruder model is approximately the same and equals $S_{off} \approx 0.76$ m^2.

For the protection of small local facilities operating autonomously in relatively unpopulated areas, the length of a single security section is relatively short and may amount to only several tens of meters. Therefore, for the purposes of signal modeling, the length of the security perimeter is limited to R = 50 m.

The installation height of the antennas of the radiobeam detection system is selected to ensure maximum overlap of the cross-sectional area of the first Fresnel zone by the intruder crossing the security perimeter. This area simultaneously depends on the operating wavelength, the length of the security perimeter, and the point of intersection. The area is largest at the midpoint of the section and narrows toward its edges. Therefore, the maximum installation height is limited in order to prevent the formation of a dead zone in the middle portion of the perimeter directly at ground level. Conversely, the minimum installation height is also constrained to reduce the influence of vegetation and snow cover during winter.

Therefore, for modeling purposes, the antenna installation height is taken as h = 0.75.

An evaluation of the magnitude and waveform of the information signal will be carried out for different modes of movement (see Fig. 4), both at the midpoint of the section and at its edge, at a distance of 5 m from the antenna, for various frequency bands.

Fig. 7 presents the results of information signal simulation at a frequency of 10.5 GHz for an intruder moving in an upright position. The section length is 50 m, and the antenna installation height is 0.75 m.

In this case, the information signal represents the variation of the field strength at the location of the receiving antenna as a function of the intruder model position along the χ-axis (see Fig. 3), relative to the field strength in its absence. Thus, this signal is a dimensionless quantity, which makes it possible to focus on its shape. Additionally, for convenience of analysis, in Fig. 7 and in all subsequent figures, conditional triggering threshold lines are indicated by points at levels 1.1 and 0.9.

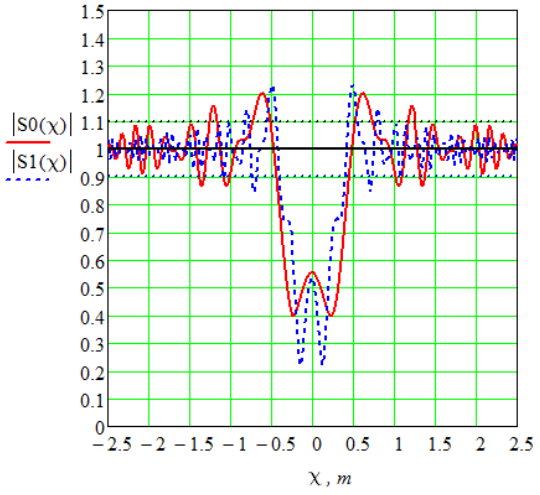

Fig. 7. Information signals during intruder crossing of the security perimeter in an upright posture for a 50 m security section at f = 10.5 GHz: solid line – at the midpoint of the section; dashed line – at a distance of 5 m from the section edge

As can be seen from Fig. 7, a significant decrease in the signal level occurs at the moment of crossing the security perimeter, which is easily detectable. By appropriately selecting the triggering threshold, it is possible to localize the detection zone directly along its axis.

Similar results were obtained when using the model of the intruder crossing the perimeter in a bent over posture, as shown in Fig. 8.

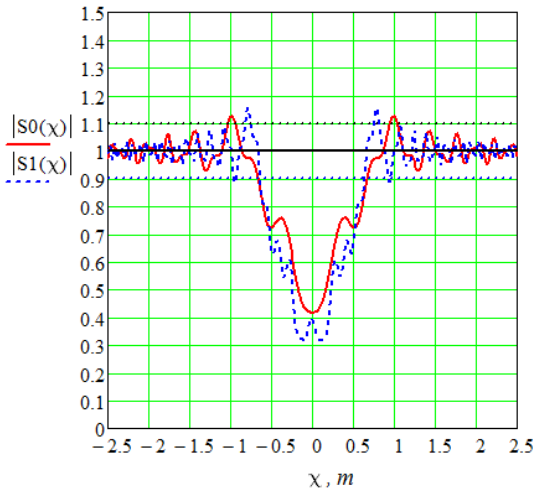

Fig. 8. Information signals during intruder crossing of the security perimeter in a bent over posture for a 50 m security section at $f = 10.5$ GHz: solid line – at the midpoint of the section; dashed line – at a distance of 5 m from the section edge

In this case, a distinct negative signal increment is observed, which also ensures detection of the perimeter crossing and clear transverse localization of the intruder. The results of signal waveform simulation for crawling across the perimeter are shown in Fig. 9.

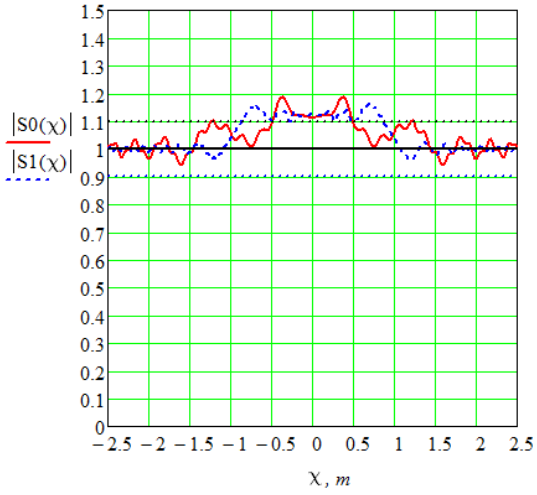

Fig. 9. Information signals during intruder crossing of the security perimeter in a crawling posture for a 50 m security section at $f = 10.5$ GHz: solid line – at the midpoint of the section; dashed line – at a distance of 5 m from the section edge

Unlike the previous cases, here a positive signal increment is observed. This is explained by the fact that, in addition to the first Fresnel zone, the signal formation is also influenced by the intruder's occlusion of higher-order Fresnel zones. As is known, occlusion of odd-numbered zones leads to a decrease in signal level, whereas occlusion of even-numbered zones results in an increase. This phenomenon is illustrated in Fig. 10, which shows the position of the intruder model relative to the concentric Fresnel zones during its movement, corresponding to Fig. 9.

In Fig. 10, all proportions correspond to the case considered above. The rectangular intruder model is rendered semi-transparent to illustrate the relationship between the areas of the Fresnel zones it occludes during movement. The figure shows that there is no occlusion of the first Fresnel zone. Therefore, the positive signal increment occurs due to partial occlusion of the second Fresnel zone, while its fluctuations are caused by the influence of higher-order zones. Consequently, the information signal processing algorithm should account for such a case, but at the same time should not trigger on positive increments that occur for other modes of movement before the intruder crosses the security perimeter (see Fig. 7).

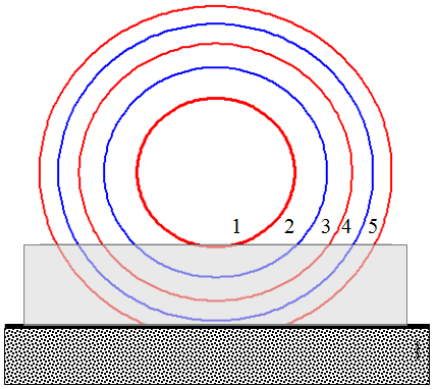

Fig. 10. Position of the intruder model during crawling movement relative to the concentric Fresnel zones at a distance of 5 m from the antenna

It is evident that reducing the operating frequency of the detection system should lead to an increase in the sizes of the Fresnel zones and ensure occlusion of the first zone. Therefore, Figs. 11, 12, 13 present analogous simulation results for the 5.8 GHz frequency band.

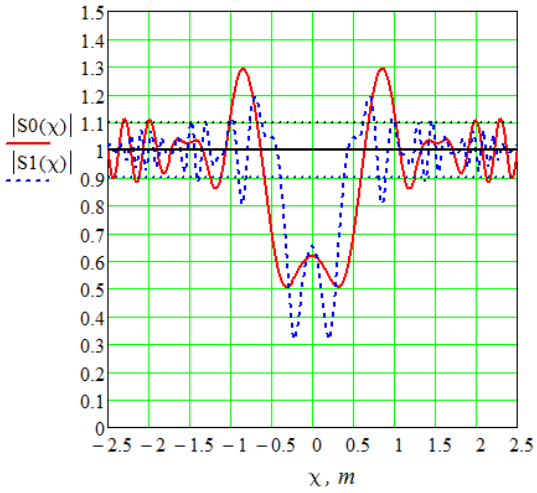

Fig. 11. Information signals during intruder crossing of the security perimeter in an upright posture for a 50 m security section at $f = 5.8$ GHz: solid line – at the midpoint of the section; dashed line – at a distance of 5 m from the section edge

As in the previous case, a distinct negative signal increment is observed, which ensures detection and recording of the perimeter crossing; however, there are significantly larger positive increments at the sides. Information signals for the intruder crossing the perimeter in a bent over posture are shown in Fig. 12.

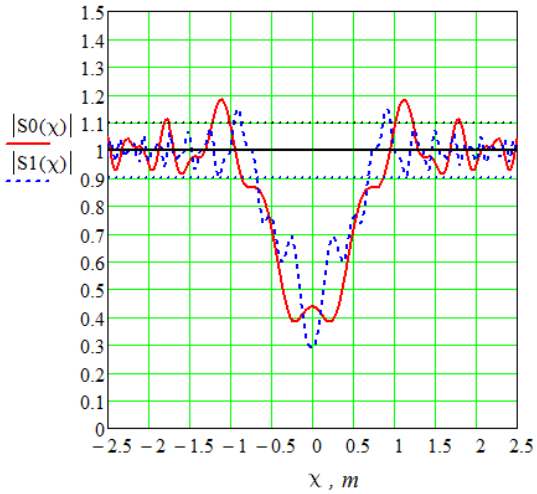

Fig. 12. Information signals during intruder crossing of the security perimeter in a bent over posture for a 50 m security section at $f = 5.8$ GHz: solid line – at the midpoint of the section; dashed line – at a distance of 5 m from the section edge

Here, a distinct signal with a reduction of positive increments at the sides is also observed. The results of information signal simulation for the intruder model crawling across the perimeter are shown in Fig. 13.

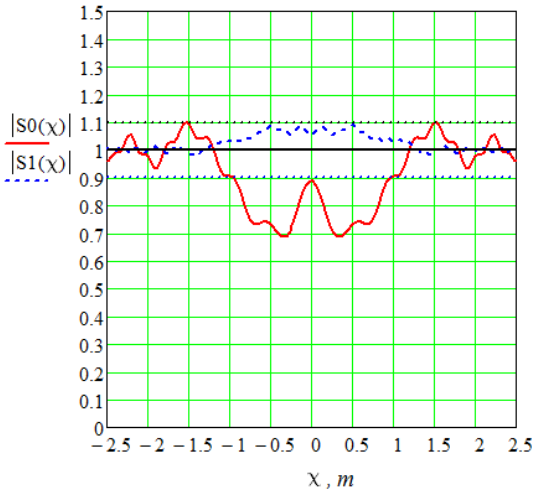

Fig. 13. Information signals during intruder crossing of the security perimeter in a crawling posture for a 50 m security section at $f = 5.8$ GHz: solid line – at the midpoint of the section; dashed line – at a distance of 5 m from the section edge

In the central part of the section, a negative information signal increment (solid line) is observed, similar to the cases of upright and bent over movement. This is explained by the fact that, at a reduced operating frequency and given the relative positions of the detection system antennas and the intruder, the latter increasingly falls within the first Fresnel zone. However, during crawling movement of the intruder model, a positive information signal increment (dashed line) is observed closer to the edge of the section. This is caused by a reduction in the mutual overlap area between the intruder model and the first Fresnel zone. Investigations at an even lower frequency, namely 2.5 GHz, yielded results presented in Figs. 14, 15, 16.

Information signals for upright movement are shown in Fig. 14.

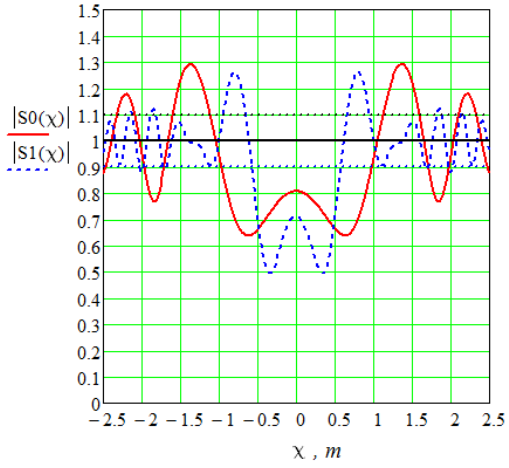

Fig. 14. Information signals during intruder crossing of the security perimeter in an upright posture for a 50 m security section at $f = 2.5$ GHz: solid line – at the midpoint of the section; dashed line – at a distance of 5 m from the section edge

Comparing this result with those obtained at other operating frequencies – 10.5 GHz in Fig. 7 and 5.8 GHz in Fig. 11 – it can be concluded that the negative signal increment caused by the intruder crossing the perimeter has slightly decreased. At the same time, the positive signal increments to the left and right of the perimeter axis, corresponding to $\chi = 0$, have increased. These positive increments are comparable in magnitude to the negative ones at deviations from $\chi = 0$ and their spatial extent has also increased. This effect is explained by the enlargement of the Fresnel zones, whose areas are proportional to the operating wavelength.

The results of information signal simulation for the intruder moving in a bent over posture are shown in Fig. 15, and for crawling movement in Fig. 16. The operating frequency of the detection system in these cases is 2.5 GHz.

In both cases, a distinct negative increment of the information signal is observed, which, however, may be double. Therefore, despite some reduction in the relative negative signal increment compared to higher operating frequencies, this decrease in frequency is justified. The study showed that all instances of the intruder crossing the perimeter are characterized by negative information signal increments, and their amplitudes are not strongly dependent on the crossing location, which allows for simplification of the signal processing algorithm.

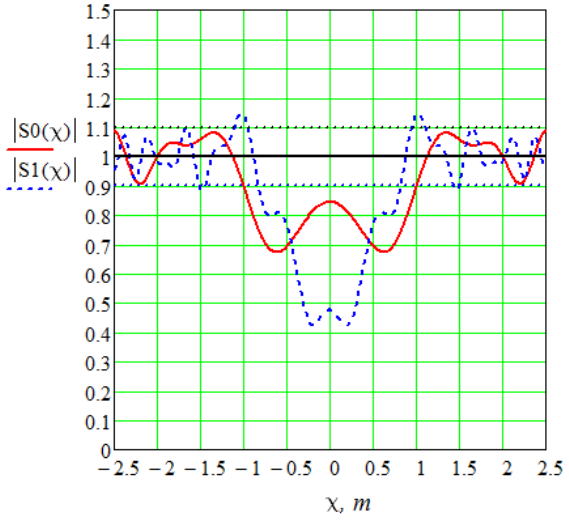

Fig. 15. Information signals during intruder crossing of the security perimeter in a bent over posture for a 50 m security section at $f = 2.5$ GHz: solid line – at the midpoint of the section; dashed line – at a distance of 5 m from the section edge

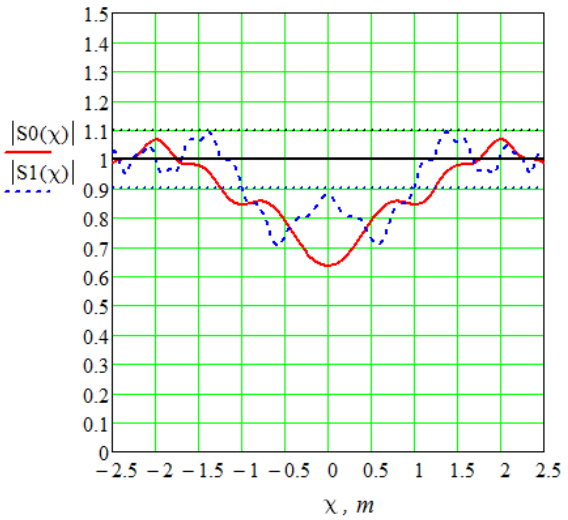

Fig. 16. Information signals during intruder crossing of the security perimeter in a crawling posture for a 50 m security section at $f = 2.5$ GHz: solid line – at the midpoint of the section; dashed line – at a distance of 5 m from the section edge

A further decrease in the operating frequency, namely to 1 GHz, and the execution of similar experiments, the results of which are presented in Figs. 17, 18, 19, demonstrated the following.

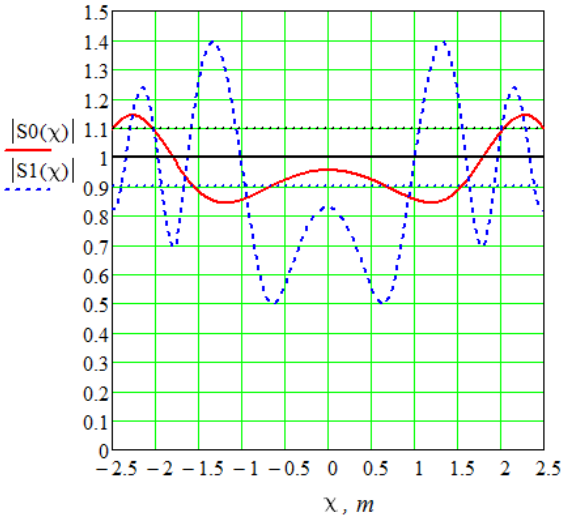

Fig. 17. Information signals during intruder crossing of the security perimeter in an upright posture for a 50 m security section at $f = 1$ GHz: solid line – at the midpoint of the section; dashed line – at a distance of 5 m from the section edge

For all modes of movement, a significant reduction in the signal level caused by the intruder is observed in the middle part of the section, shown as a solid line in Figs. 17, 18, 19. At the same time, at the edge of the section, this level is considerably higher, as indicated by the dashed line in the figures. Therefore, this frequency range is not optimal for the studied section.

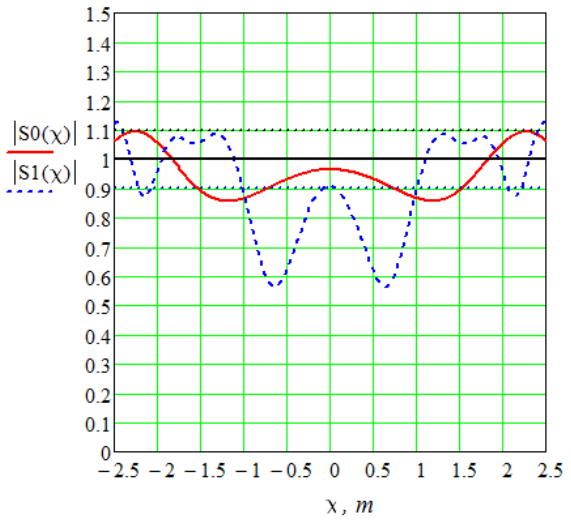

Fig. 18. Information signals during intruder crossing of the security perimeter in a bent over posture for a 50 m security section at $f = 1$ GHz: solid line – at the midpoint of the section; dashed line – at a distance of 5 m from the section edge

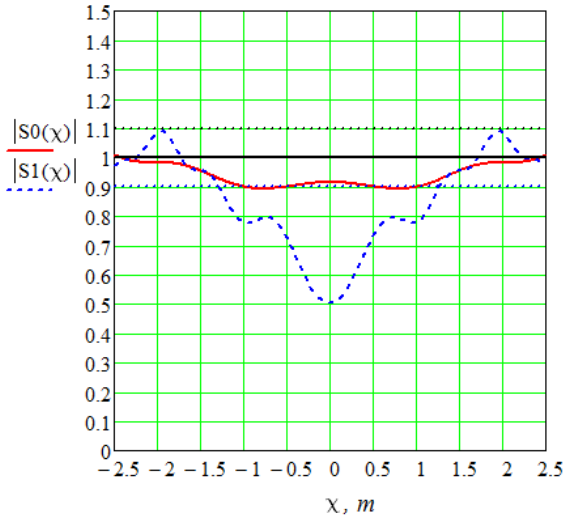

Fig. 19. Information signals during intruder crossing of the security perimeter in a crawling posture for a 50 m security section at $f = 1$ GHz: solid line – at the midpoint of the section; dashed line – at a distance of 5 m from the section edge

Conclusions

The proposed mathematical model of the information signal in a radiobeam detection system is approximate; however, it allows evaluating the influence of the length of the security perimeter, antenna installation heights, operating frequency, and the transverse dimensions of the intruder model on the information signal.

In particular, it was found that at certain operating frequencies and specific modes of intruder movement, a positive increment of the information signal occurs. Specifically, at 10.5 GHz when the intruder moves crawling, and at 5.8 GHz also during crawling, but closer to the edge of the perimeter. This may cause the intruder to be missed by systems tuned to detect interruptions in the radiobeam. Further studies conducted at 2.5 GHz and 1.0 GHz led to the conclusion that the length of the security perimeter and the optimal operating frequency of the radiobeam detection system are interrelated. The shorter the perimeter, the more advisable it is to use devices operating at lower frequencies, which, unfortunately, is not always feasible.

In this case, the proposed mathematical model can provide predictions of the information signal shape depending on the specific operating frequency, the length of the security perimeter, antenna installation height, modes of intruder traversal, and intruder dimensions. For given algorithms of information signal processing and alarm generation, the parameters of the detection zone can be forecasted. This enables pre-assessment and comparison of the effectiveness of radiobeam detection systems across different frequency bands and the selection of an optimal system, reducing the number of cumbersome and costly experimental studies.

If needed, the proposed mathematical model allows creating a database of information signals for a specific security perimeter for the application of correlation processing methods, which will undoubtedly contribute to increased detection reliability and reduced false alarm rates.

Acknowledgements

The paper is supported by the National Research Foundation of Ukraine, project number 2023.04/0116 “Modular acoustic system of airspace monitoring” from the contest Science to strengthen Ukraine’s defense capabilities.

References

[1] Yevseiev, S., Melenti, Y., Voitko, O., Hrebeniuk, V., Korchenko, A., et al. (2021). Development of a concept for building a critical infrastructure facilities security system. *Eastern-European Journal of Enterprise Technologies*, Vol. 3, No. 9(111), pp. 63–83. DOI: 10.15587/1729-4061.2021.233533.

[2] Armstrong D. and Peile C. (2005). Perimeter intruder detection systems performance standard. *Proceedings 39th Annual 2005 International Carnahan Conference on Security Technology*, pp. 33-36. DOI: 10.1109/CCST.2005.1594845.

[3] U.S. Department of Homeland Security, Science and Technology Directorate. (2025, April 10). *Perimeter intrusion detection sensors.*, date of access: 8 August 2025.

[4] 100 m Microwave Bistatic Sensor FMW-100 – Forteza. *Ornicom*, date of access: 10 August 2025.

[5] 500 m Microwave Bistatic Sensor FORTEZA-500 – Forteza. *Ornicom*, date of access: 10 August 2025.

[6] Gong, X., Zhang, J. and Cochran, D. (2012). A Coverage Theory of Bistatic Radar Networks: Worst-Case Intrusion Path and Optimal Deployment. *arXiv*, 11(19), 3080. DOI: 10.48550/arXiv.1206.1355.

[7] Xu, X., Zhao, C., Ye, T. and Gu, T. (2019). Minimum Cost Deployment of Bistatic Radar Sensor for Perimeter Barrier Coverage. *Sensors*, Vol. 19, Iss. 2, Article 225. DOI: 10.3390/s19020225.

[8] Redpath, G. (2016, May). Reducing perimeter false alarms. *SMART Security Solutions*, date of access: 12 August 2025.

[9] Blacksmith P., Poirier J. L. and Holt F. S. (1979). Radar intrusion detection system. U.S. Patent No. 4,132,988A. *U.S. Patent and Trademark Office*.

[10] Ludlow, P., Redpath, G. and Seawright, S. (2016). Bi-directional bistatic radar perimeter intrusion detection system (U.S. Patent Application No. US20160178741A1). *United States Patent and Trademark Office*.

[11] Griffiths, D. J. (2023). *Introduction to Electrodynamics* (5th ed.). Cambridge University Press, 602 p.

[12] Kakani, S. L. (2020). *Electrodynamics: Classical and Quantum*. CBS Publishers and Distributors, 944 p.

[13] Willis, N. J. (2005). *Bistatic Radar*, (2nd ed.). IET, 337 p.

[14] Tekinerdogan, B., Özcan, K., Yağız, S. and Yakın, İ. (2021). Feature-Driven Survey of Physical Protection Systems. *arXiv*. DOI: 10.48550/arXiv.2104.00949.

[15] Tripathi, D., Tripathi, A. K., Singh, L. K., Chaturvedi, A. (2022). Towards analyzing the impact of intrusion prevention and response on cyber-physical system availability: A case study of NPP. *Annals of Nuclear Energy*, Vol. 168, 108863. DOI: 10.1016/j.anucene.2021.108863.

[16] Villegas-Ch, W. and García-Ortiz, J. (2023). Authentication, access, and monitoring system for critical areas with the use of artificial intelligence integrated into perimeter security in a data center. *Frontiers in Big Data*, Vol. 6, Article 1200390. DOI: 10.3389/fdata.2023.1200390.

Математична модель інформаційного сигналу радіопроменевого засобу виявлення

Сторож В. Г., Фабіровський С. Є., Прудиус І. Н., Матієшин Ю. М., Оборжицький В. І., Гурмач Р. М.

Розроблено математичну модель інформаційного сигналу радіопроменевого засобу виявлення для дослідження факторів, які впливають на його параметри. Основою представленої моделі є принцип Гюйгенса–Френеля. Порушник моделюється еквівалентним прямокутником, який в процесі переміщення почергово екранує певні ділянки фазового фронту хвилі. Інформаційний сигнал визначається як нормована різниця між напруженістю поля при відсутності моделі порушника та напруженістю поля при її наявності і переміщенні. Математичну модель інформаційного сигналу верифіковано шляхом фізичного моделювання на частоті 9,3 ГГц за допомогою панорамного вимірювача КСХ Р2-61 із використанням стандартних рупорних антен та металевих пластин різних розмірів, що переміщувались.

Модель продемонструвала хорошу відповідність експериментальним даним, що дозволило застосувати її для прогнозування форми інформаційних сигналів. Проведено серію обчислювальних експериментів для частот 10,5 ГГц, 5,8 ГГц, 2,5 ГГц та 1,0 ГГц для рубежу охорони протяжністю 50 м. Проаналізовано три способи переміщення порушника: у повний зріст, зігнувшись і плазом. Показано, що при високих частотах (10,5 ГГц) при русі плазом, сигнал має додатній приріст, що створює ризик пропуску порушника в системах, налаштованих на спрацювання за від'ємним приростом сигналу. Зниження частоти до 5,8 ГГц та 2,5 ГГц забезпечує більш стабільні від'ємні прирости сигналу при дещо нижчій його амплітуді. Водночас при частоті 1 ГГц спостерігається суттєве зменшення рівня сигналу. Запропонована математична модель інформаційного сигналу враховує робочу частоту, відстань між антенами, геометрію порушника, його розташування та спосіб переміщення. Це дозволяє створити банк сигналів для конкретного рубежу охорони з метою застосування кореляційних методів їх оброблення. Отримані результати дозволяють обирати оптимальний частотний діапазон для конкретного рубежу охорони, скоротити обсяг експериментальних досліджень на рубежі охорони, удосконалити алгоритми оброблення інформаційних сигналів, що сприятиме підвищенню надійності виявлення та зниженню кількості хибних спрацювань.

Ключові слова: виявлення; радіопроменевий; засоби рубежу охорони; математична модель