K.V. Kolisnyk, A.V. Kipensky, E.I. Sokol
(*National Technical University «Kharkov Polytechnic Institute»,*
21 Frunze Str., Kharkov, 61002, Ukraine. e-mail: kolesniknet@ukr.net, kavkpi@ ukr.net)

The use of radiolocation control methods to protect the perimeters of large objects

Annotation – To detect an intruder for the perimeter security of a large object it is proposed to use radiolocation sensors. The sensors are chosen with taking into account the use conditions, which are inhomogeneous along the object perimeter. The way to simplify a synthesis of the security system is to use a space imaging data.

Key words – radiolocation control systems, perimeters protection control, electronic devises, quality assurance.

In today's conditions, when terrorism becomes a planetary problem, the issue of ensuring security of various objects has become one of the most topical both for organizations and enterprises and in general for the state. Need to settle security problems caused rapid development of technology in this area, the development of an extensive range of products and systems for security purposes, the establishment and modernization of methods of providing security for objects perimeter [1-3]. However, the security of *large objects* (airports, oil depots, power electrical installations, etc.) with limited access requires solving a number of additional challenges determined by the great length of the perimeters with the various terms of use for methods and systems to ensure security.

The purpose of this paper is to show the effectiveness of using different radiolocation methods and tools for perimeter security of large objects, where characteristics of these tools may compensate various environmental influences on each particular part of secured perimeter.

The large object is some organizational and industrial structure located over a large area (with a different topography, vegetation, level of electromagnetic fields, etc.) and composed of buildings and structures with common perimeter (Fig. 1). To prevent unauthorized access to the object the monitoring tools are placed along the inner side of its perimeter composed into a united security system.

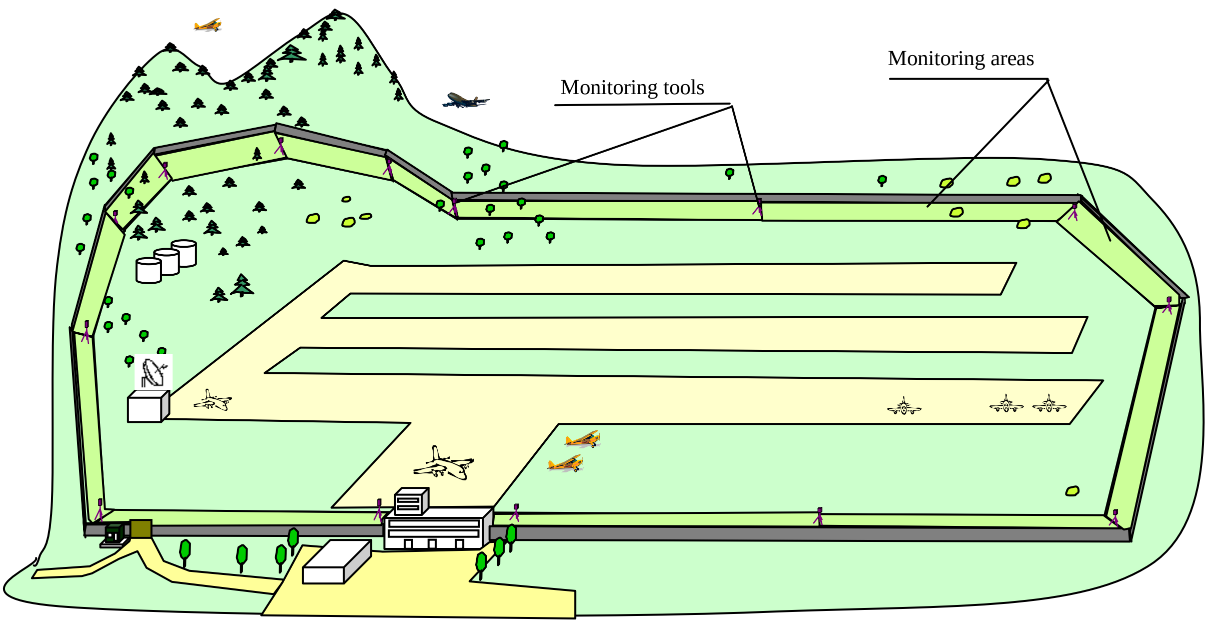


Fig. 1. Example of location of perimeter security system of a large object

To localize the region of violation as well as compensate the influence of environment on the effectiveness of the monitoring system, the entire secured perimeter is divided into a number of control zones. Within each of these zones, one or more tools are set to monitor the presence of an intruder. From a technical point of view, a security system of the perimeter of a large object can be considered as telemetry system, with functions of collecting, processing and presentation of information about the state of the object [4-7]. In general, case the block diagram of a security system of the perimeter of large objects can have the structure shown in Fig. 2.

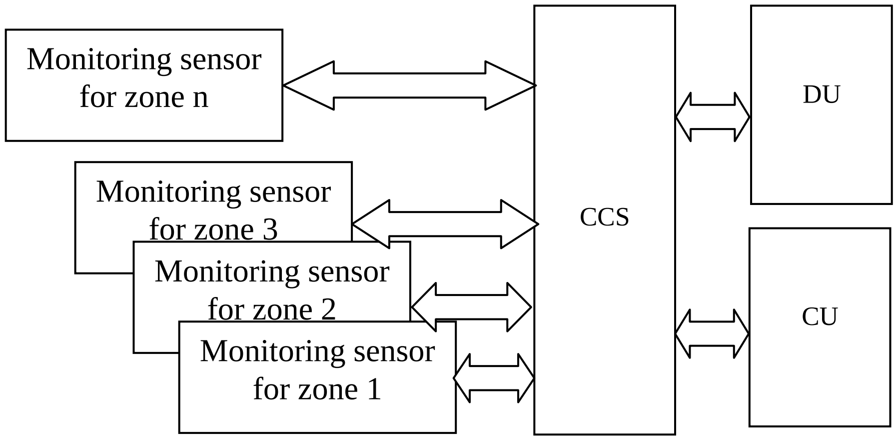


Fig. 2. The block diagram of a security system of the perimeter of a large object:
CCS – central control system for perimeter security;
DU – display unit of the system state;
CU – control unit for notifying and counteraction to intruders.

To identify a person or group of people trying to make unauthorized entry to the object the sensors of various types are used. Type of sensors is determined by the physical phenomena underlying the principles of their actions:

- the infrared radiation of biological object;
- reflection of electromagnetic waves with optical and radio-frequency spectrum;
- scattering of acoustic and electromagnetic waves;
- the change of magnetic or electrostatic fields, etc.

According to the principles of use, radar facilities are classified as: radio ray, radio wave, infrared, optical, acoustic, ultrasonic, etc. [1-3].

The efficiency of various radiolocation controls will be different under different conditions of their use. That is why the solution to the problem of identification of an intruder into the perimeter of a large secured object has a number of features [4].

First, this is work in the near zone (from several to hundreds meters) allowing to localize the place of intrusion. In addition, it is necessary to build a narrow radiation pattern without side lobes, thereby reducing the likelihood of misoperations, and thus improve the efficiency of security system.

Furthermore, it is important not to have dead space near the receiving and transmitting antennas, due to the necessity to provide a continuous field along the secured perimeter throughout the entire volume.

Moreover, there are some limitations on the power and frequency characteristics of the radiolocation tools, which are defined by their noise immunity, stability to electronic resistance, as well as the possibility of impact on staff, ensuring the security of the object.

The lower bound of radio receiving route sensitivity of security systems is usually defined such as to ensure the separation of noise from animals, birds and underlying vegetation. Also for this purpose an adaptive processing of received information is often used

Let us consider the use of radiolocation monitoring methods of an intruder presence by the example of two-position radio ray tool (Fig. 3).

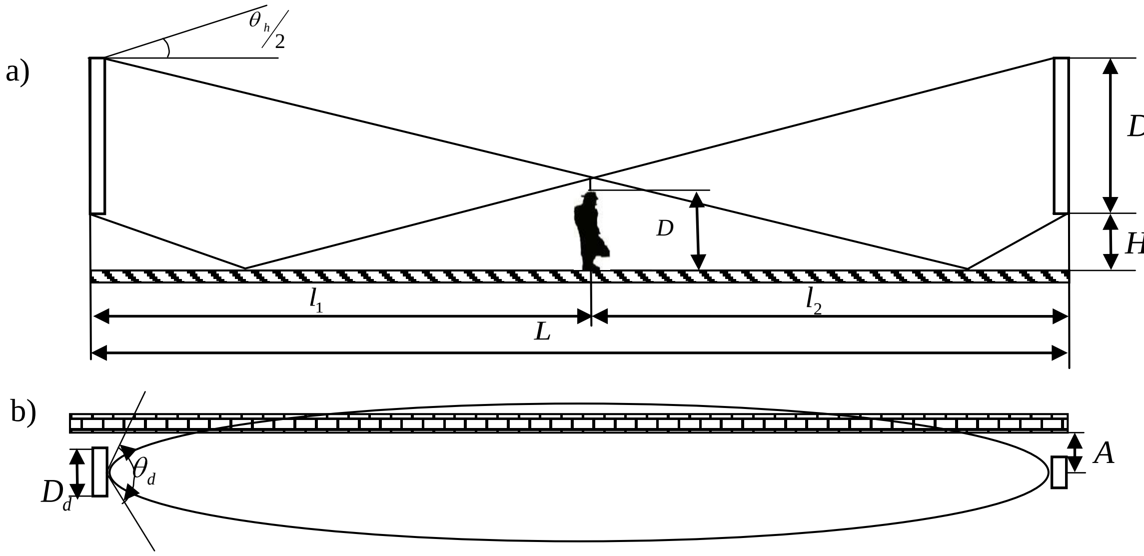


Fig. 3 Two-position radio ray tool

In the figure, we use the following notation:

L – the distance between the receiving and transmitting antennas;

l_1, l_2 – the distance from the intruder to the transmitting and receiving antennas respectively;

D – the height of the intruder;

$D_d, \theta_d, D_h, \theta_h$ – the geometric parameters of antennas;

H_A – the distance between the antennas and the ground;

A – the distance between the antennas and a vertical barrier.

Two-position radio ray tool is a set of receiving and transmitting devices that create an electromagnetic field of a given configuration, defined by the parameters of the antennas and the control area of the object, and

$$P_{REC} = P_{TR} \left(\frac{G_\lambda \lambda}{4\pi L} \right)^2 |F|, \quad (1)$$

where:

P_{REC}, P_{TR} – power at the input of the receiving antenna and at the output of the transmitting antenna respectively;

G_λ – antenna gain;

λ – the wavelength of electromagnetic radiation.

Influence of surface roughness (terrain, buildings, vegetation, etc.) of control zones to the work of the radiolocation tool is considered in an attenuation index

$$|F| = \sqrt{1 + n^2 - 2n\mathrm{Cos}\Omega}, \quad (2)$$

where:

n – the reflection coefficient of the surface;

Ω – phase of the reflected wave.

It is known that the propagation of radio waves from the transmitting antenna to the receiver forms a complex interference pattern. When $D >> \lambda$ RF-scattering region is determined by the ratio of the typical height D of the intruder to the radius R_1 of the first Fresnel zone. For the most of radiolocation control tools, the condition of Fresnel diffraction D/R_1 ~1 is true. When an intruder moves across the secured region, he consecutively closes the Fresnel zones. It causes the receiver input signal to get a particular form. This form allows identifying the presence of the intruder in the monitoring area [1].

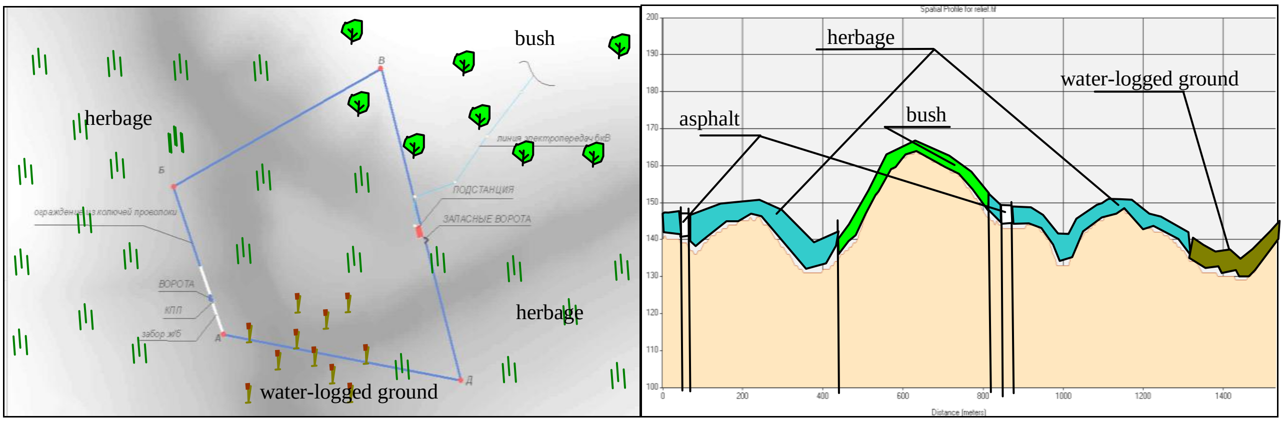
Therefore the quality of the radiolocation control tool functioning significantly depends not only on the geometrical parameters of the antennas ($D_d, \theta_d, D_h, \theta_h$) and the conditions of their placement, but also on the surface roughness of control zones.

In addition, the performance of the radiolocation tools strongly depends on climatic conditions and other conditions of use:

- geological (topography, type and chemical composition of soil, water space, seismic activity);
- biological (plants, animals, birds, insects);
- climatic (wind, dust, sand, atmospheric precipitates, fog, solar radiation, temperature, thunderstorms, seasonal behaviour, etc.);
- electromagnetic fields and radiation;
- acoustic vibrations;
- level of radioactivity;
- level of illumination, etc.

Considering aforesaid, to create effective systems for perimeter security of large objects it is advisable and promising to use the technology capabilities and methods of geographic information systems (GIS) [9, 10].

GIS-technology is based on processing of space mapping information about the state of a secured object with its subsequent refinement for each control zone of the perimeter (Fig. 4).



a) b)

Fig. 4. Example of using GIS-technology for the construction of the object perimeter by coordinates (a) and its profile (b) on a digital terrain map

Knowing the secured object coordinates and using digital maps you can get information about the profile of the perimeter of the object and the characteristics of each control zone. Then, having geo-information model of a specific object and information about the capabilities of existing radiolocation tools, it is easy enough to solve the optimization problem (discrete choice of radiolocation control tools with regard to the conditions of their use) for each control zone of the secured perimeter [11, 12].

Conclusion

To effectively protect the perimeters of large objects it is advisable to use radiolocation control methods. Due to the large extent of the secured perimeter of such objects, one should consider the possibility of various conditions of use for the radiolocation tools in the different zones. In addition, for each specific zone of the perimeter one should choose such kind of control tool that is most effective for the respective conditions of use. It is possible to simplify the choice of control tools using data obtained by space mapping.

References

1. *Иванов И.В.* Охрана периметров. – Москва: Радио и связь, 1997. – 98с.
2. *Магауенов Р.Г.* Системы охранной сигнализации: основы теории и принципы построения. – М.: Горячая линия-Телеком, 2008. – 496 с.
3. *Колесник К.В., Смаглюк В.В., Чурюмов Г.И.* Концепция построения радиотехнических систем охраны периметров крупних объектов // Технология и конструирование в электронной аппаратуре. – Одесса: Политехпериодика. – 2008. – № 4 (76). – С. 19-22.
4. *Колесник К.В., Поляков Г.Е., Чурюмов Г.И.* Анализ принципов построения и оценка современного технического уровня радиотехнических систем охраны периметров объектов // Технічна електродінаміка. Тематичний вип. «Силова електроніка та енергоефективність». – Київ: ІЕД НАНУ. – Ч. 2. – 2009. – С. 104-108.
5. *Колесник К.В., Смаглюк В.В., Виноградов Г.М.* Особенности построения электронных систем охраны периметров крупных объектов // Материалы VIII МНПК «Современные информационные и электронные технологии». – Одесса: 2007. – С. 303.
6. *Колесник К.В., Смаглюк В.В., Чурюмов Г.И.* Обобщенная структурная схема радиотехнических систем охраны периметров крупных объектов // Материалы IX МНПК «Современные информационные и электронные технологии». – Одесса, 2008. – С. 223.
7. *Колесник К.В., Чурюмов Г.И.* Аналитический обзор технических средств охраны периметров крупных объектов // Технічна електродінаміка. Тематичний вип. «Силова електроніка та енергоефективність». – Київ: ІЕД НАНУ. – Ч. 5. – 2008. – С. 127-132.
8. *Колесник К.В., Чурюмов Г.И., Смаглюк В.В.* Методы контроля присутствия человека в системах охраны объектов // Технічна електродінаміка. Тематичний вип. «Силова електроніка та енергоефективність». – Київ: ІЕД НАНУ. – Ч. 5. – 2007. – С. 121-124.
9. ERDAS IMAGINE. Практическое руководство Tour Guides. 05 декабря 2005. Geospatial Imaging, LLC. Norcross. Georgia. Leica Geosystems.
10. *Колесник К.В., Мачехин Ю.П., Чурюмов Г.И.* Методы статического моделирования радиотехнических систем контроля охранных периметров объектов // Збірник наукових праць ХУПС МО України «Системи обробки інформації». – Харків: ХУПС. – 2010. – № 1(82). – С. 61-65.
11. *Колесник К.В., Кипенский А.В., Мачехин Ю.П., Чурюмов Г.И.* Методика оценки качества радиотехнических систем охраны периметров территориально-распределенных объектов // Материалы IX МНПК «Современные информационные и электронные технологии». – Одесса, 2012. – С. 175.
12. *Колесник К.В., Кипенский А.В., Мачехин Ю.П., Чурюмов Г.И.* Использование формализованных показателей для оценки качества при проектировании радиотехнических систем охраны периметров территориально-распределенных объектов // Технология и конструирование в электронной аппаратуре. – Одесса: Политехпериодика. – 2012. – № 4 (94).– С. 31-35.