УДК 004.056(043.2)

Lobanchykova N.**, **PhD, Associate Professor
Zhytomyr Polytechnic State University,
Kredentsar S.**, **PhD, Associate Professor
National Aviation University

METHODOLOGY FOR PERIMETER SECURITY SYSTEMS CREATION

The most often problem is the protection of the area from unauthorized in the short-term. This task is factual during anti-terrorist operations, exploration activity, transportation of cargo and other objects that are needed for short-term protection.

Many conditions, such as the absence of connection to the electricity, relief features for system allocation, system disguising, limited deployment time and amount of personnel, resistance to different weather phenomena (snow, rain, frost, heat, the influence of electromagnetic radiation) create peculiarities for the usage of specialized systems.

Construction of perimeter security systems is impossible without using modern information technologies and achievements of science. The main tasks are the creation of information system model of ranking for objects, which are threats of unauthorized access to the perimeter for secure facilities; creation of a model for interaction for information systems components; creation of a model for identifying subjects of threats; description the process of determining the danger level for threats subjects; creation of decision-making block; generating the array of dangers; creation of a method of detecting unauthorized access to the perimeter for secure facilities.

This system is a computer-aided system intended to increase the security level of objects by using automation for the process of identifying violators of the perimeter and process of decision-making for generating alarms for the security units. It consists of mathematical models and methods, information, software and technical means that are interrelated and interacting with users during the making and monitoring of administrative decisions.

The goal is achieved by the synthesis of integrated units. These units are contactless radio frequency identification subsystem (RFID) (Module 1), intelligent video surveillance subsystem (Module 2), DSS of detecting and prevent unauthorized access to the perimeter of secure facilities (Module 3); subsystem of detection the movement along the protected perimeter (Module 4).

The block-scheme of an information system model of ranking for objects, which are threats of unauthorized access to the perimeter for secure facilities due to the actions of a person, is shown in Fig. 1. The main functions of

Module 1 (M1) are the identification of staff at the secure facilities; positioning of staff at the secure facilities; identification of staff that is coming to secure facilities perimeter.

The initial data of this module is a combination of a digital ID, which is input flow to Module 3.

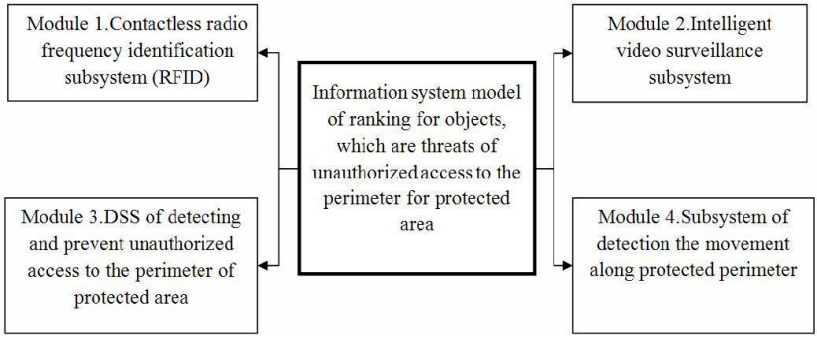

Fig.1. Block-scheme of information system model of ranking for objects, which are threats of unauthorized access to the perimeter for protected area

Main functions of Module 2 (M2) are: surveillance for the staff at the area of the protected object; surveillance around the perimeter of the protected object; providing information for user about violators of the perimeter for protected object; video transmission for user about unauthorized access for real-time decision-making.

The main functions of Module 3 are automation of management decision-making by operator for identification of danger situations, classification of dangers situations and determining the class of danger. The main function of Module 4 (M4) is to identify the invasion at the perimeter of protected area.

To construct the information system model of ranking for objects, which are threats of unauthorized access to the perimeter for protected area, it is needed to develop some other models, such as: the model for identifying subjects of threats at the protected area, the model of process of the level threats determination, and block for management decision-making.

This technology makes be automated processes of violator detection and decision-making for alarm generation.