Information Technology for Mobile Perimeter Security Systems Creation

Nadiia Lobanchykova[1], Svetlana Kredentsar[2], Ihor Pilkevych[3,] and Mykhailo Medvediev[4]

[1]Faculty of Information and Computer Technology, Zhytomyr Polytechnic State University, Zhytomyr, Ukraine
[2] Department of Aeronavigation Systems National Aviation University, Kyiv, Ukraine
[3]Department of computer information technologies, S. P. Korolyov Zhytomyr Military Institute, Zhytomyr, Ukraine
[4]School of Information Technologies and Engineering, ADA University, Baku, Azerbaijan

Corresponding author: lobanchikovanadia@gmail.com

Abstract. The main aim of this research is the creation of information technology for mobile (of rapid deployment) security systems of the area perimeter. This system appears to be a complex of models and methods, information, software, and hardware mean that have interacted with users during decision-making and control of implementation for management solutions. The proposed information technology aimed at improving the protection level for security departments by automating the process of danger detection for perimeters and decision-making for alarm. The structural model of the system, the model of the system's components interaction, and the model of identifying the subjects of emergency threats have been proposed. A method for identifying unauthorized access to the perimeter of the secure facilities, using the production model of knowledge representation, was created. It is a set of linguistic expressions (such as "IF-THEN") and the knowledge matrix. The method of ranking for objects, which are threats of unauthorized access to the perimeter for secure facilities, has been proposed. The practical value of work consists of the possibility of the use of this information technology by perimeter's security systems of various objects. Proposed models are complete and suitable for hardware and software implementation.

1. Introduction

Analysis of criminal situation shows an increasing number of thefts, vandalism, attempts of unauthorized access to the territory of the secure facilities. The issue of protection of the perimeter for static secure facilities has been already solved. But the problem of protection for mobile (moving) secure facilities is still very complicated.

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 mobile perimeter security systems is impossible without using modern information technologies and achievements of science. The main tasks of the perimeter security system are the early detection of unauthorized access and security notification.

2. Theoretical background

The research works of professionals as O. Yudin, O. Korchenko, O. Konahovych [7], O. Kuznetsov [1], are the most notable among the others concerning methodology and methods of creating modern perimeter security and information security systems. Mobile perimeter security systems are built using sensor networks and wireless data transmission systems. The relevance of the problem is emphasized by the authors in articles [2, 4]. Partially, the results of the authors' research are presented in [3, 5, 6]. However, there is no methodology for the creation of mobile security systems. So, this article aims to create information technology for the mobile perimeter security system.

The main tasks are the creation of information system model of ranking for objects, which are threats of unauthorized access to the perimeter for the protected area; creation of a model for interaction for information systems components; creation of a model for identifying subjects of threats; describe 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 the protected area.

3. Results.

The experience of conducting an anti-terrorist operation in the east of our country, the participation of Ukrainian Armed Forces units in peacekeeping operations and armed conflicts, analysis of activities of extremist organizations against military objects showed that early detection of the intruder (on approaches to the secure facilities) can save lives and the health of staff, can provide the proper protection of ammunition and military equipment. Automation of the process of detecting the intruder on approaches to secure facilities is an urgent problem. It determines the effectiveness of the training of troops (forces).

The equipment of radio-electronic equipment of protection of long-range approaches to positions of checkpoints, mechanized units, areas of concentration, and location of military equipment, warehouses will allow guards, patrols, guard posts securely protect military objects [10]. An analysis of recent research [10-12] found that the Armed Forces of Ukraine paid low attention to the improvement of defense systems of approaches to military objects, including temporarily located objects, in comparison with similar systems of the armed forces of the most developed countries of the world.

Notice that in NATO (the first of all in the US Mature Force) such systems have been created since the 1970s. So, in 1972, there was an initiative to implement radio-electronic technologies and the BISS (Base and Installations Security System) system for all kinds of Armed forces. That initiative included the creation means to protect all buildings and rooms that store all types of weapons. As well as there was a separate program to create an autonomous and remote-controlled alarm system for battlefields [10-11].

Since the 1980s, the Soviet Union has been creating radio-electronic equipment to protect approaches to secure facilities. But in 1985 that initiative had been stopped. Since 1985, the TASS (Tactical Autonomous Security) system implementation program has been started [10-12].

For the construction of mobile perimeter security systems US Armed Forces most widely used portable radar systems radar AN / PPS-5 and -15 different modifications. Such systems were temporary parking of aircraft, military equipment, vehicles, as well as individual buildings and other small objects.

For the construction of mobile perimeter security systems US Armed Forces most widely used portable radar systems radar AN / PPS-5 and -15 different modifications. Such systems were temporary parking of aircraft, military equipment, vehicles, as well as individual buildings and other small objects.

For the proper organization of protection of temporarily located objects, it is necessary to use a combination of active (burglar-alarm security systems) and passive (intelligence-alarm systems) technical means of security. Burglar alarm systems are aimed at detecting the intruder due to its interaction with a specially formed electromagnetic field.

The use of such systems requires an increased power supply for the formation of the electromagnetic field and can be detected by special monitoring systems due to the lack of radio masking. The advantage of such systems is the ability to control large areas at near and far approaches and automatic alert notification. Intelligence-alarm systems - identify the intruder by changing the existing physical field (magnetic, vibration, thermal).

These systems are characterized by radio and visual masking. But the decision to identify the event (intruder/obstacle) is made by the operator located near the main or portable control panel. Data transmission is performed using ultra-short wave (VHF) radio channels (700-900 MHz).

Multiple portable controls and indicators are recommended to increase the tactical flexibility of terrain deployment and redundancy (destruction). The system health check is carried out by direct radio call and periodic self-monitoring.

Typically, sensors are point-to-point with a sectorial or circular detection area within a radius of 300 m. Usually, sensors are masked on the background of objects that surround them. The detection is based on known physical principles such as using radar, television (TV), infrared (IR), thermal imaging (TPV), photoelectric, laser, magnetic, electromagnetic, seismic, vibration detection principles. Also electronic and optic devices are widely used. Different combinations of those devices are used for radar detection and surveillance [16].

Detection range, the accuracy of detection, interference protection of forward and reverse channels, retrieval time, range and speed of transmission, mass and size indicators, cost, reliability, efficiency, hiding, cryptography protection against unauthorized access in the radio channel, power consumption are main technical characteristics of the equipment [16].

The sources of false alarms in the technical means for security can be animals, strong wind combined with close vegetation, lightning in thunderstorms, etc. All means except infrared can be used for all types of weather, but there are restrictions on their use, such as in high snow, grass, shrubs, trees, mountain passes, and settlements.

The main task of technical means for security is fast and reliable alarm security of areas, boundaries, arsenals of weapons, etc. The boundaries of which are covered should be closed. But that is very difficult to organize fully closed perimeter for areas with the various landscapes, with forests and gullies. Therefore usually that requirement is provided partly.

Therefore, in such areas, it is additionally necessary to use a mobile radar station and radar reconnaissance system ground targets, in hiding places near forest paths, and in ravines, mountain passes should be laid remotely controlled electronic (optical) detection means. Such radio-electronic systems of technical means of protection will allow us to detect, count, classify and determine the direction of movement of manpower and self-propelled equipment, to transfer data to the portable control panel and an indication of on a radio channel. Transmission of information (detection signals) from such technical means of protection to the portable control panel and indication (10… 20 km away) should be carried out on noise-protected ultra short waves radio channels.

The electronic equipment of technical means of protection should be powered by various power sources, mainly from autonomous power supply: batteries, accumulators, and solar batteries. Such batteries must recharge the batteries, provide batteries with 30… 50 W of power, which is sufficient for the operation of technical equipment. At the same time, the power supply from the external power supply and electrical equipment of cars should be provided.

The joint use of technical means of rapid response protection and means of detecting a mobile radar station allows solving several tasks: to carry out inconspicuous temporary alarm scanning (blocking) of the perimeter of the object, to detect violators crossing the border; to conduct covert engineering and technical reconnaissance in the uncontrolled territory (including during hostilities) in places of probable movement of armed people, transport, military equipment, signaling their appearance, number, and direction of movement.

Technical means of protection, which are designed to protect temporarily located objects, can also be used in the systems of protection of stationary objects and large premises (hangars, warehouses). It is also advisable to use electronic means of protection when performing tasks on state border protection by units of the State Border Guard Service, services of the Ministry of Emergencies in summer in hard-to-reach areas of most probable forest fires, monitoring poachers on rivers and lakes (especially at night).

To protect the military facilities of the Armed Forces of Ukraine, it is necessary to develop and use unified, block-modular security systems with advanced security functions that solve the problems of intelligence, detection, signaling, and classification of violations (violators). They should be integrated security systems with extensive capabilities (remote control, field positioning, GSM, satellite, digital data transmission, etc.).

Additional use of computer capabilities on a portable control panel and indication will allow a three-dimensional display of the area from a given location of the observer or a virtual flight of the area with the environment, which is applied taking into account signals (information) automatically transmitting security devices. This allows the main portable control panel and displays to make decisions on adequate response to the situation.

Let's create the information system model of ranking for objects, which are threats of unauthorized access to the perimeter for the protected area. 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 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 protected area (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 the protected area due to the actions of a person, is shown in Figure 1. The main functions of Module 1 (M1) are the identification of staff at the protected object; positioning of staff at the protected object; identification of staff that is coming to protected object perimeter.

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

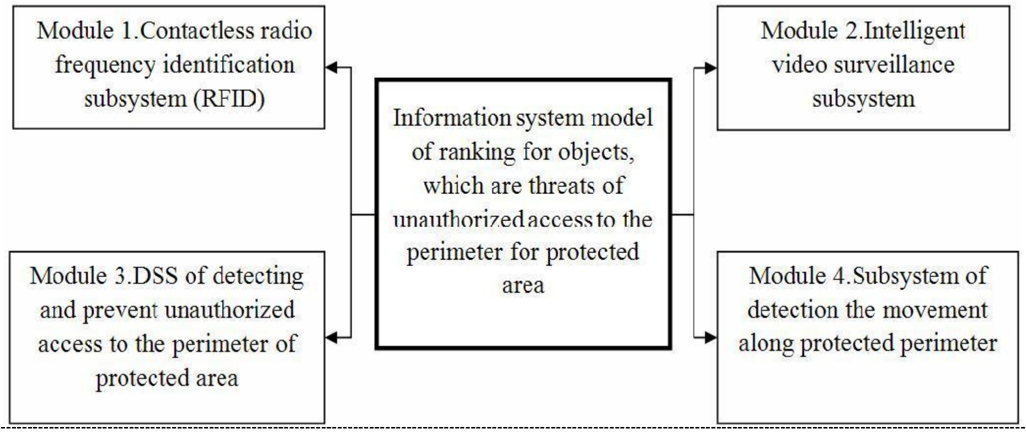
Module 1.Contactless radio frequency identification subsystem (RFID)
Module 2.Intelligent video surveillance subsystem
Information system model of ranking for objects, which are threats of unauthorized access to the perimeter for protected area
Module 3.DSS of detecting and prevent unauthorized access to the perimeter of protected area
Module 4.Subsystem of detection the movement along protected perimeter

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

The 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 the user about violators of the perimeter for the protected object; video transmission for the user about unauthorized access for real-time decision-making.

The main functions of Module 3 are the automation of management decision-making by the operator for the identification of dangerous situations, classification of dangerous situations, and determining the class of danger. The main function of Module 4 (M4) is to identify the invasion at the perimeter of the protected area. The interaction model of information system components is shown in Fig. 2.

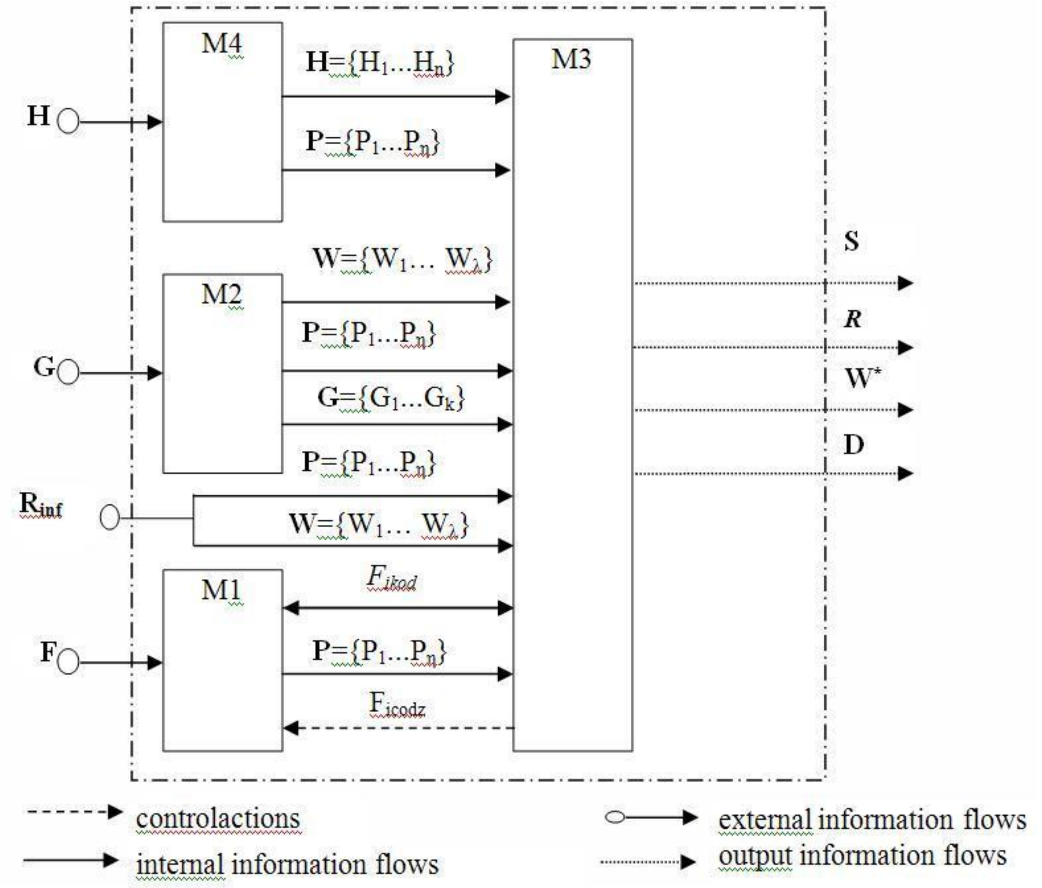

Figure 2. The interaction model of information system components.

Input system data are $\mathbf{F} = \{F_1, \dots, F_i\}$– a set of signals RFID-signs that are received by RFID-scanners; $\mathbf{G} = \{G_1, \dots, G_k\}$ – video data flow coming from cameras; $\mathbf{R_{inf}} = \{R_{inf1}, \dots, R_{inf\rho}\}$– information flow coming from protected area resources of the military base; $\mathbf{H} = \{H_1, \dots, H_y\}$ – a set of signals received by motion detectors.

Information flows using for system interaction consists of $\mathbf{F_{icod}}$– digital code (ID) received from RFID-sign of *i*-employee, $i = \overline{1...n}$; $\mathbf{G_{v1}} = \{G_{v1}, \dots, G_{vn}\}$ – a set of digitized frames in a form of images in BMP format coming from cameras; $P_1, \dots, P_{()}$ – detected dangerous subjects; $W_1, \dots, W_{()}$ – a set of parameters that are controlled and analyzed to determine the danger class.

The control influences are $\mathbf{F_{icodz}}$– ID of worker *i*. Input system parameter is informative vector $\mathbf{W^*} = \{W_i\}$, $i = \overline{1 \dots (}$, that is transmitted by channels as an electronic message from day duty to the security unit and in a case of necessity to the external law enforcement agency; informative vector

$\mathbf{D} = \{D_l\}$, $l = \overline{1 \dots \varepsilon}$, is generated automatically by the system and is addressed to the person on duty and is transmitted in a case of necessity to the external law enforcement agency; **R** – the decision of DSS as to dangerous subjects classification; **S** – the decision of DSS as to the detection of unauthorized access inside the protected area.

To construct the information system model of ranking for objects, which are threats of unauthorized access to the perimeter for a 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 the process of the level threats determination, and block for management decision-making.

Let us create the model for identifying subjects of threats at the protected area. Ones of the dangerous subjects (**P**) can be mentally ill persons (P_1), spies (P_2),regional terrorist organizations (P_3), international terrorist organizations (P_4), lone extremists or a group of extremists (P_5), and sabotage and reconnaissance groups (P_6). It is possible to represent them as open dangerous subjects\` classification (a set of subjects\` classification) that may be supplemented or adapted. The model for identifying subjects of threats at the protected area is shown in figure 3. Therefore, we obtain open classification groups:

$\mathbf{N} = \bigcup_j N_j$ – a set of staff under danger attack as a result of unauthorized access;

$\mathbf{X} = \bigcup_a X_a$ – a set of hitting objects.

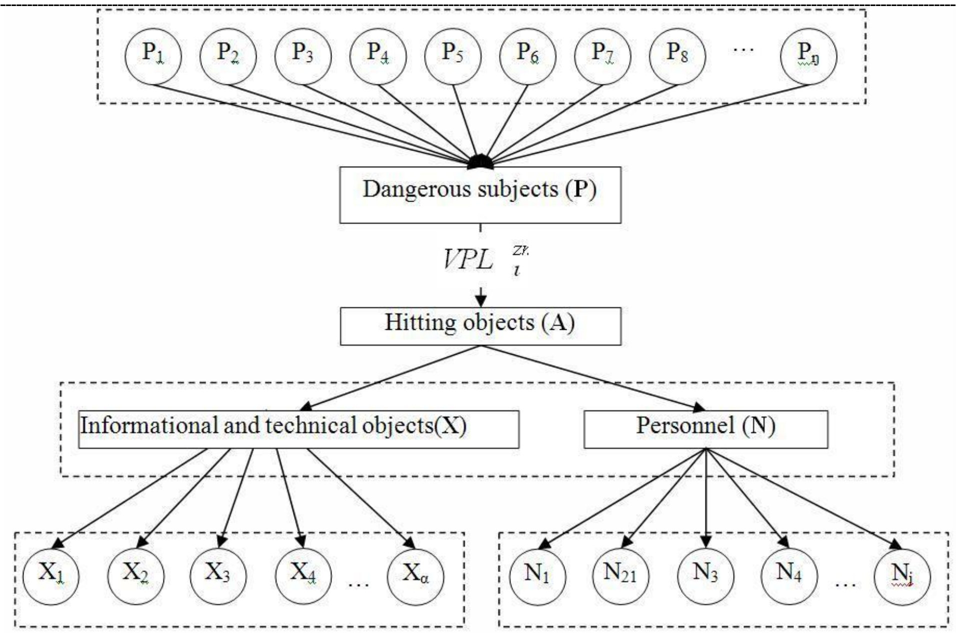

Figure 3. The model for identifying subjects of threats at the protected area.

Therefore, we have the open classification grouping of hitting objects in the form of a union of sets of potential goals of unauthorized access, (1):

$$\mathbf{A} = \mathbf{N} \bigcup \mathbf{X} = (N \setminus X) \vee (X \setminus N) \vee (X \wedge N) \tag{1}$$

Thus, we determined the threat sources in the form of a set of dangerous subjects (**P**) that may attack VPL^{zn} the position of the subdivision on duty to destroy or to invade informational and technical objects (**X**) or/and personnel (**N**).

During the analysis of the functioning of the subdivision on duty the objects with the maximum impact zone were discovered: radio-electronic means(X_1^p), reconnaissance information (X_2^p), subdivision's equipment (X_3^p), signal center (X_4^p), subdivision's weapon (X_5^p), and food supply (X_6^p).

Staff in potential danger include: chief of the position (N_1^l), worker on duty (N_2^l), post operator (N_3^l), signalman (N_4^l), doctor (N_5^l), sentry (N_6^l).

As a result of investigations, a set of threats of unauthorized access **S** was formed. Unauthorized access S_θ is determined by the set of hitting objects **A** according to the formula (2)**:**

$$S_\theta = \{A_\sigma \mid \sigma = \overline{0,(X_a + N_j)}\} \tag{2}$$

Unauthorized access determined at the hitting object S_θ may be expressed by the set of dangerous subjects **P**, the formula (3):

$$S_\theta^p = \{P_n \mid n = \overline{0, m_{sz}}\} \, , \tag{3}$$

where m_{sz} – the number of dangerous subjects.

Unauthorized access determined at the hitting object and by the set of dangerous subjects S_θ^p is obtained by the set of impacts occurred by subjects, the formula (4):

$$S_\theta^{pv} = \{VPL_\iota^{zn} \mid \iota = \overline{0,k}\} \, , \tag{4}$$

where m_{sz} – the number of possible impacts.

The set of possible acts at the hitting object is determined by the set of possible impacts and the set of dangerous subjects and is found using the expression, the formula (5):

$$T = (P \wedge VPL^{zn}) \tag{5}$$

Unauthorized access determined at the hitting object and by the set of dangerous subjects and the set of possible impacts is obtained by, the formula (6):

$$S_\theta^{pvs} = \{H_y, F_i, G_k \mid \theta = \overline{1,\mu}, y = \overline{1,\psi}, i = \overline{1,n}, k = \overline{1,\delta}\} \, , \tag{6}$$

where *n, δ, ψ* – amount of means to detect each class; μ–the number of system solutions.

Therefore, an informative vector of unauthorized access can be represented in the form of, the formula (7):

$$I_{\mu_i}^{pvs} = \{T_\upsilon, VPL_\iota^{zn}, P_n, A_\sigma \mid \upsilon = \overline{0,\xi}, \ \iota = \overline{0,c}, \ \sigma = \overline{0,(X_a + N_j)}, \ n = \overline{0, m_{sz}}\} \, . \tag{7}$$

Thus, S_θ^{pvs} is determined as an integral value $W_i^{'}$, $i = \overline{0,\mu}$, the formula (8):

$$S_\theta^{pvs} = f(H_y, F_i, G_k) \tag{8}$$

According to the formula (8) S_θ^{pvs} , the presence of unauthorized access is determined and decision about the alarm is made. To classify the rank of the violator, who committed unauthorized access to the perimeter of the object, we use a set R, which is a subset of Q and has the same parameters. The method of detection of unauthorized access threat to the protected area is constructed with the help of a productive model of knowledge representation. It is a complex of linguistic expressions "if-then". Let us consider that the scales of all expert rules equal 1.

As at the beginning formalized experts` knowledge is not enough, so it is supposed that the knowledge matrix may compete with the appearance of new knowledge about the possibility to detect unauthorized access, experimental data. It is performed by the creation of new rules that make the method of detection of unauthorized access closer to the real conditions. Thus, adaptation and settings of the knowledge matrix are supposed.

So, the threat detection of unauthorized access to the subdivision on duty may be shown as, the formula (9):

$$S_\theta^{pvs} = f_\theta(H_y,G_k,F_i) \; , \; \theta=\overline{1,\mu} \; , \; y=\overline{0,\psi} \; , \; k=\overline{0,\delta} \; , \; i=\overline{0,n} \qquad (9)$$

where H_y – a set of discrete signals coming from motion detectors; F_i – a set of discrete signals of RFID signs; G_k – a flow of data coming from cameras; $f_\theta(H_y,G_k,F_i)$ – logical expressions that determine the level of threat for unauthorized access on the safety principle S_θ^{pvs} , $\theta=\overline{1,\mu}$.

The range of changes of the motion detector's characteristics of the state $H_y \in \left\lfloor \underline{H_y},\overline{H_y} \right\rfloor$, $y=\overline{1,\psi}$, RFID signs $F_i \in \left[\underline{F_i},\overline{F_i}\right]$ $i=\overline{1,n}$, , the flow of video data $G_k \in \left[\underline{G_k},\overline{G_k}\right]$, $k=\overline{1,\delta}$ an output value of the result of situation classification (identification) is known. Here $\left\lfloor \underline{H_y},\overline{H_y} \right\rfloor$, $\left[\underline{F_i},\overline{F_i}\right]$, $\left[\underline{G_k},\overline{G_k}\right]$ are the respectively lower and upper value of motion detector's characteristics of the state, signals from RFID signs, and flow of video data that get values 0 or 1.

Then the solution S_θ^{pvs*} is placed as conformity to fixed states of H_y, F_i, G_k determined by fixed vectors of input parameters. Considering the abovementioned factors we obtain authorized access in the form of knowledge matrix (table 1).

Table 1. Knowledge matrix used to classify the threat of the appearance of unauthorized access.

№ input value combination	Input variables			Output variable
	Motion detector`s signals (H_y)	RFID-sign signals (F_i)	Changes of video data Stateflow (G_k)	S_θ^{pvs}
1	0	1	0	S_1
2	0	1	1	
3	1	1	0	
4	1	1	1	
5	0	0	0	S_2
6	0	0	1	
7	1	0	0	
8	1	0	1	

1. The table dimension equals (λ+1)×N, where (λ+1) – number of columns, which value equals the number of classification groups for indexes of the protected perimeter; N – the number of rows.

2. First λ columns of the matrix correspond to input variables H_y, F_i, and G_k, but (λ+1)th column corresponds to the value S_θ^{pvs} of the output variable $\mathbf{S}$, $\theta = \overline{1,\mu}$.

3. Each row of the matrix is a combination of input variable values that refers to one of the possible values of output variable **S**. Besides, first k_{θ_1} rows correspond to the output variable value S_1, but others k_{θ_2} correspond to the S_2.

4. Input variables are binary. An element of the matrix α_μ^e that is placed at the intersection of row and column corresponds to the linguistic assessment of the input data parameter and takes place in the determination of the possible value of output variable that detects unauthorized access.

Categorization of unauthorized access detection $\mathbf{S} = \bigcup_\theta S_\theta^{pvs}$ $\theta = \overline{1,5}$ consists of classification units: $S_1 = S_1^{pvs}$ – the alarm is not generated; $S_2 = S_2^{pvs}$ – the alarm is generated.

The input knowledge matrix determines the system of logical expressions "IF-THEN, ELSE" that connect values of input variables with one of the possible solutions. In this case, the system determines the presence of unauthorized access to the area of the subdivision on duty S_θ^{pvs}, $\theta = \overline{1,\mu}$, the formula:

```
  IF (F=0) AND [((H=0) AND ((G=0) OR (G=1)) OR (H=1) AND ((G=0) OR
(G=1))], THEN S=S2, ELSE, S=S1
```

If the location of the subdivision on duty is a constant place for a long time and there is a possibility to extend the protected perimeter by distribution the motion detectors, RFID signs, and cameras as far as possible (thereby to increase the time for operator's decision and realization of appropriate measures) the possibility to realize violator classification appears.

4. Conclusions.

The research yielded the following results:

1. The structures of the information system for ranking objects, which are threats of unauthorized access to the perimeter for the protected area, have been proposed. This system consists of a contactless radio frequency identification subsystem (RFID), intelligent video surveillance subsystem, DSS of detecting and prevents unauthorized access to the perimeter of the protected area, a subsystem of detection the movement along the protected perimeter. The integration and implementation of these subsystems allow automating the process of violator's detection and the process of decision-making for alarm generation.

2. The first time the model of components interaction for information systems of ranking objects, which are threats of unauthorized access to the perimeter for the protected area has been proposed. This model determines informational flows and realizes the interaction of system components. Also, it was determined as a form of transmitted vectors.

3. The model for identifying subjects of threats for unauthorized access to the protected area has been improved. It determines classification groups of dangerous subjects, staff, and informational-technical objects. This model was the base to form a classification set of potential hitting objects. Therefore, threat sources were determined in the form of dangerous subjects set that may attack the location of the subdivision on duty to destroy or to invade staff and/or informational-technical objects.

4. The method of detecting unauthorized access to the perimeter for a protected area has been proposed. It is constructed with the help of a productive model of knowledge representation, which is a set of linguistic expressions "IF-THEN". Given expressions are in the form of operations of indistinct logic and knowledge matrix, thus, there is the opportunity to automate the determination of

threats. The method of classification of dangerous subjects for unauthorized access to the protected area has been realized.

A set of proposed models, methods, information, and software-hardware means that are interrelated and interacted with users during preparation, adoption, and control of management decisions, creates information technology for mobile perimeter security systems and increases the security level of guard subdivision and subdivision on duty. This technology makes be automated processes of violator detection and decision-making for alarm generation. The practical value of this article consists of the possibility to use given information technology in security systems for different objects. Proposed models are finished and able to software and hardware realization.

References

[1]. Information security and economic safety for enterprise: monograph [Text] / O.O. Kuznetsov, S.P. Evseev, S.V. Kavun, Kharkiv, KhNEU, 2008, p. 360.

[2]. Lysenko O.I., Kozelkova K.S., Novikov V.I., Pryshchepa T.O., Romaniuk A.V. 2015. Functional model of wireless sensor network management system with self-organization for monitoring of environmental parameters. *Systemy obrobky informatsii*. **10(135).** 222–225.

[3]. Lobanchykova N.M., Kotenko V.M. 2011. The method of determining the location of objects at the airport. *Problems of creation, testing, application and operation of complex information systems: a collection of scientific papers.* **Vip. 4**. (Zhytomyr: ZhVI NAU). 140–147.

[4]. Minochkin A.I. 2007. Prospects for the development of tactical sensor networks. *Collection of scientific works.***4** (K .: VITI NTUU "KPI").112-119.

[5]. Pilkevych I.A., Lobanchykova N.M. 2011. Models and methods of building a decision support system for an automated personal identification system. *Problems of construction, testing, application and operation of complex information systems*. **Vip. 5**. (Zhytomyr: Korolov Zhytomyr Military Institute NAU). 69-76.

[6]. Yudin O.K., Korchenko O.G., Konahovych G.F. 2009. *Information security in data networks*. (Kyiv, Interservis) p.719.

[7]. *Zakhyst informatsii ta ekonomichna bezpeka pidpryiemstva: monohrafiia* 2008 / O.O. Kuznetsov, S. P. Yevseiev, S. V. Kavun. (Kharkiv: Vyd. Khneu). p.360.

[8]. Hraivoronskyi M.V., Novikov O.M. 2009. *Security of information and communication systems*. (K.:Vydavnychahrupabhv).p. 608.

[9]. Pilkevych I.A. 2014. *Information security in ICS: tutorial* / I. Pilkevych, K. Molodetska, N. Lobanchykova/ (Zhytomyr, ZhSU). p.170.

[10].Kavun, S. V. Information security: a textbook. (Kharkiv: Vyd. KhNEU). p. 368.

[11].Zavhorodnyi V.Y. Comprehensive information protection in computer systems: a textbook.2001. (M. :Lohos; Pboiul). p. 264.

[12].Belov E., Los V., Meshcheriakov A. 2006 Fundamentals of information security: a textbook for universities (M. : "Studyo"). p. 356.

[13]. Maliuk A.A. 2004. *Information security: conceptual and methodological bases of information protection:* [textbook. manual for universities]. (M. :Horiachaia lynyia-Telekom), p. 280.

[14]. Zghurovskyi, M.Z, Pankratova N.D. 2007. *Fundamentals of systems analysis*: a textbook [for students. higher textbook lock]. (K: Vydavnychahrupa BHV) p. 544.

[15].Kotsiuba V.P. 2011. Improving the organization of protection of temporarily located military facilities through the introduction of modern technical means of protection. *Science and Technology of the Air Force: Scientific and Technical Journal (*Kh.:KhUPS).**1(5)**.p.164–167.

[16]. Zhukov V.I. 2010. Determining ways to counter sabotage of special operations forces / V.I.Zhukov, V.P. Kotsiuba, O.S. Titov. *Zbirnyk naukovykh prats KhUPS*. (Kh.:KhUPS). **Vyp. (4)26.** p. 10-14.

[17]. Dzeverin I.H. Kostenko I.L., Borshchevskyi O.M. 2010. Synthesis of the structure of the integrated system of protection and defense of military facilities of the Air Force. *Science and Technology of the Air Force: Scientific and Technical Journal* (Kh.:KhUPS). **Vyp. (2)4**. p. 186-190.