Information Technology for Mobile Perimeter Security System Creation

Mazin Al Hadidi, Jamil S. Al-Azzeh, Lobanchikova N., Kredentsar S., Odarchenko R., Opirskyy I., Seilova N.,

[1]Computer Engineering Department. Faculty of Engineering Technology
[2]Al-Balqa' Applied University, Jordan
[3]Computer Engineering Department. Faculty of Engineering Technology
[4]Al-Balqa' Applied University, Jordan
[5]PhD, Associate Professor, Zhytomyr State Technological University (Zhytomyr, Ukraine)
[6]PhD, Associate Professor, National Aviation University (Kyiv, Ukraine)
[7]PhD, Associate Professor, National Aviation University (Kyiv, Ukraine)
[8]PhD, Associate Professor, Lviv Polytechnic National University (Lviv, Ukraine)
[9]PhD, Associate Professor, Kazakh National Research Technical University (Almaty, Kazakhstan)

Abstract
This paper is about information technology of creation of 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 means that are 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 dangers detection for perimeters and decision-making for alarm. The structural model of the system, the model of system's components interaction and the model of identifying the subjects of emergencies threats have been proposed. A method for identifying unauthorized access to the perimeter of the protected object, using the production model of knowledge representation, was created. It is a set of linguistic expressions (such as "IF-THEN") and knowledge matrix. The method of ranking for objects, which are threats of unauthorized access to the perimeter for protected area, has been proposed. Practical value of work consists in the possibility of the use this information technology by perimeter's security systems of various objects. Proposed models are complete and suitable for the hardware and software implementation.

Keywords:
perimeter, security, information technology, information security system

1. Introduction

The most often problem is a protection of the area from unauthorized in the short-term. This task is factual during antiterrorist operations, exploration activity, transportation of cargo and other objects that are needed for short-term protection. Many conditions, such as: 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, influence of electromagnetic radiation) create peculiarities for 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 areearly detection of unauthorized access and security notification. The research works of professionals as O. Yudin, O. Korchenko, O. Konahovych, O. Kuznetsov, M. Grayvoronsky, O. Novikov, S. Kavun, V. Zavgorodny, E. Belov, and A. Malyuk are the most notable among the others concerning methodology and methods of creating modern perimeter security and information security systems. These expert's researches deal with the construction of information security systems, fixed perimeter security systems, complex information security systems and technical security means creation. However, there is no methodology for creation of mobile security systems. So, the aim of this article is to create the information technology for mobile perimeter security system. The main tasks are: creation of information system model of ranking for objects, which are threats of unauthorized access to the perimeter for protected area; creation of model for interaction for information systems components; creation of 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 method of detecting unauthorized access to the perimeter for protected area.

Manuscript received October 5, 2024
Manuscript revised October 20, 2024
https://doi.org/10.22937/IJCSNS.2024.24.10.7

2. Main Part

Let's create the information system model of ranking for objects, which are threats of unauthorized access to the perimeter for protected area. This system is computer-aided system intended to increase the security level of object by using automation for the process of identifying violators of the perimeter and process of decision-makingfor generating alarms for security unit.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 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 protected perimeter (Module 4).

The block-scheme of information system model of ranking for objects, which are threats of unauthorized access to the perimeter for protected area due to the actions of a person, is shown in Fig. 1. Main functions of Module 1 (M1) are: 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 the Module 3.

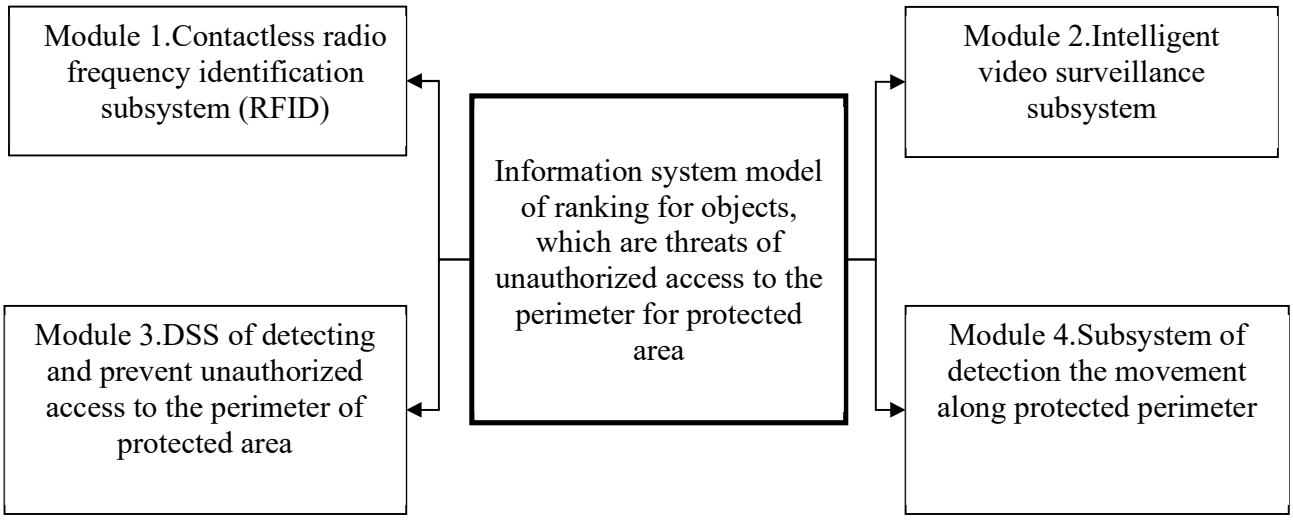

Figure1 – Block-scheme of information system model of ranking for objects, which are threats of unauthorized access to the perimeter for protected area

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 is 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. Interaction model of information system components is shown in Fig. 2.

2. The model for identifying subjects of threats

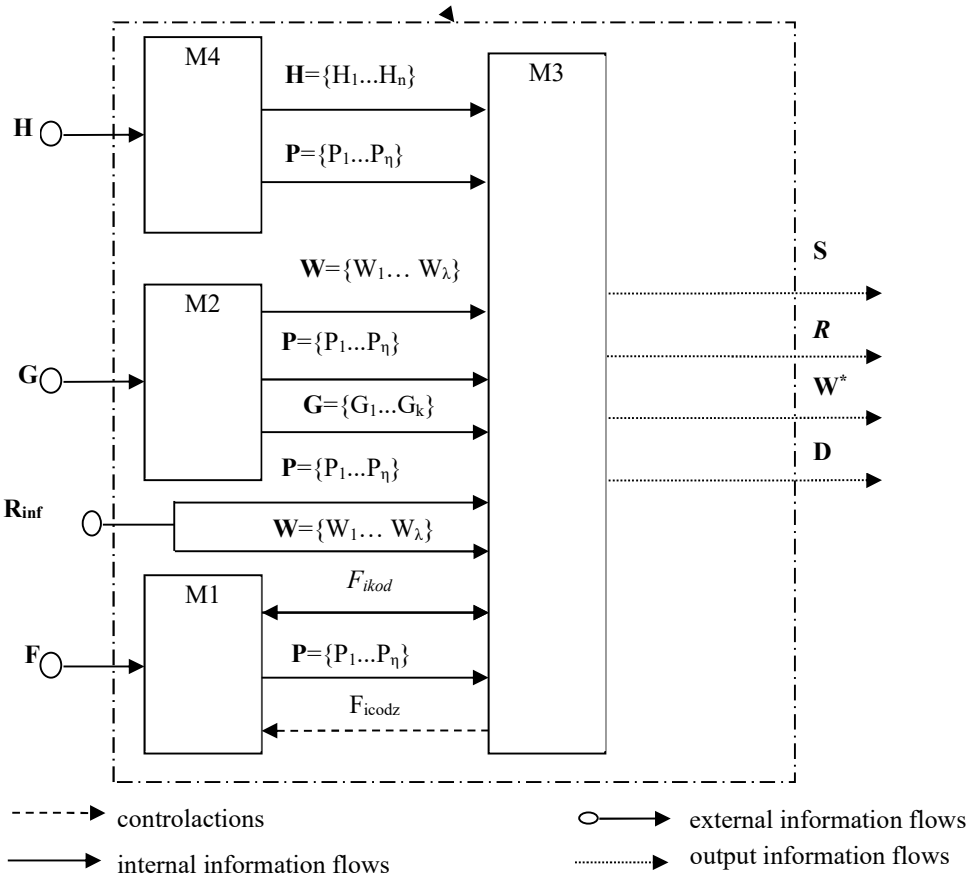

Figure 2 – Interaction model of information system components

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 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: F_{icod}– digital code (ID) received from RFID-sign of *i*-employee, $i=\overline{1\dots n}$; $\mathbf{G_v}=\{G_{v1},\dots,G_{vn}\}$ – a set of digitized framesin a form of images in BMP format coming from cameras; $\mathbf{P}=\{P_1,\dots,P_\eta\}$ – detected dangerous subjects; $\mathbf{W}=\{W_1,\dots,W_\lambda\}$ – a set of parameters that are controlled and analyzed to determine danger class.

The control influences are: F_{icodz}– ID of worker *i*. Input system parameter is informative vector $\mathbf{W}^*=\{W_i\}$, $i=1\dots\lambda$, 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 $\mathbf{D}=\{D_l\}$, $l=1\dots\varepsilon$, 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*** – decision of DSS as to dangerous subjects classification; , **S** – decision of DSS as to 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 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.

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 (*P1*), spies (*P2*),regional terrorist organizations (*P3*), international terrorist organizations (*P4*), lone extremists or a group of extremists (*P5*), and sabotage and reconnaissance groups (*P6*). It is possible to represent them as open dangerous subjects` classification $\mathbf{P} = \bigcup_{\eta} P_{\eta}$ (a set of subjects` classification) that may be supplemented or adapted.

The model for identifying subjects of threats at the protected area is shown at the 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.

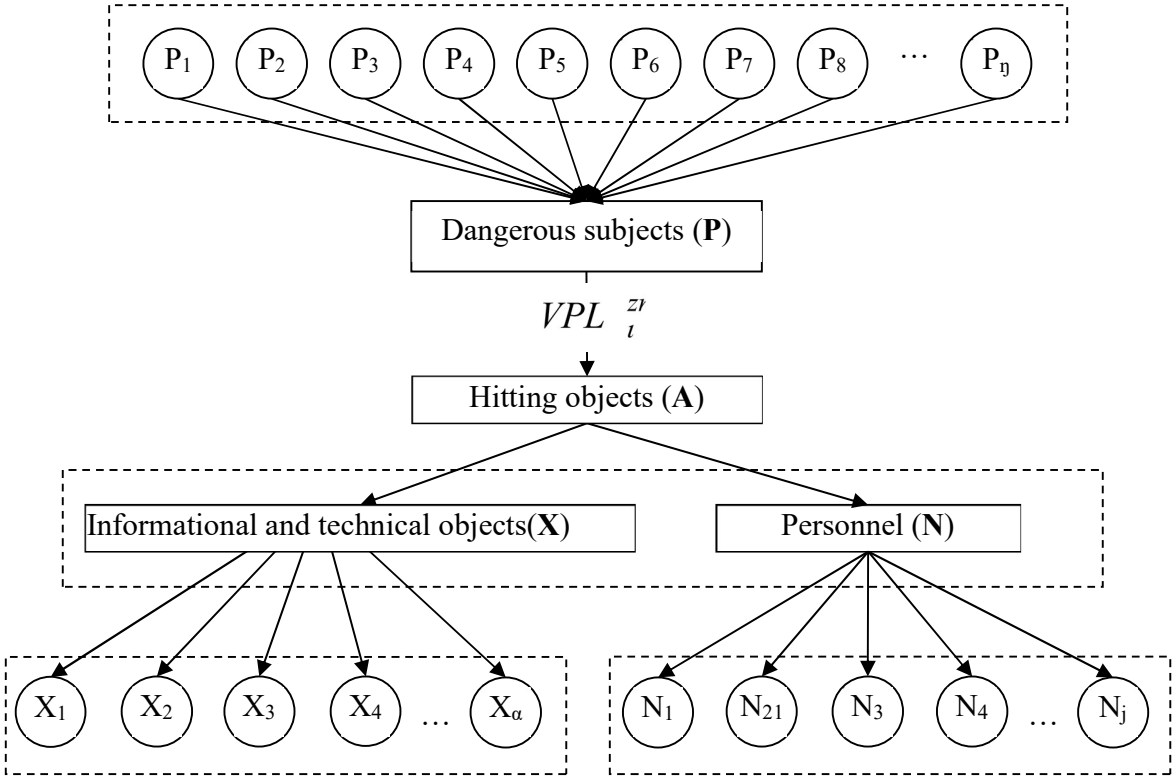

Figure 3 – The model for identifying subjects of threats at the protected area.

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

$$\mathbf{A} = \mathbf{N} \cup \mathbf{X} = (N \setminus X) \vee (X \setminus N) \vee (X \wedge N) \qquad (1)$$

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

During the analysis of functioning of 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 the formula**:**

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

Unauthorized access determined at the hitting object S_θ may be expressed by the set of dangerous subjects **P**:

$$S_\theta^p = \{P_n \,|n = \overline{0, m_{sz}}\} \quad , \quad (3)$$

where m_{sz} – amount 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:

$$S_\theta^{pv} = \{VPL_\iota^{zn} \,|\iota = \overline{0,k}\}, \quad (4)$$

where m_{sz} – amount 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 expression:

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

Unauthorized access determined at the hitting object and by the set of dangerous subjects and the set of possible impacts is obtained by:

$$S_\theta^{pvs} = \{H_y, F_i, G_k \,|\, \theta = \overline{1,\mu}, y = \overline{1,\psi}, i = \overline{1,n}, k = \overline{1,\delta}\}, \quad (6)$$

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

Therefore, informative vector of unauthorized access can be represented in the form of:

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

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

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

According the formula (8) S_θ^{pvs}, the presence of unauthorized access is determined and decision about alarm is made.

To classify therank of 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 protected area is constructed with a help of 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` knowledges are not enough, so it is supposed that the knowledge matrix may compete with the appearance of new knowledges about possibility to detect an unauthorized access, experimental data. It is performed by creation of new rules that make the method of detection of unauthorized access be closer to the real conditions. Thus, adaptation and settings of knowledge matrix are supposed.

So, the threat detection of an unauthorized access to the subdivision on duty may be shown as:

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

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 level of threat for unauthorized access on the safety principle S_θ^{pvs}, $\theta = \overline{1,\mu}$.

The range of changes of motion detector`s characteristics of state $H_y \in \left[\underline{H_y}, \overline{H_y}\right]$, $y = \overline{1,\psi}$, RFID signs $F_i \in \left[\underline{F_i}, \overline{F_i}\right]$, $i = \overline{1,n}$, flow of video data $G_k \in \left[\underline{G_k}, \overline{G_k}\right]$, $k = \overline{1,\delta}$ and output value of the result of situation classification (identification) are known. Here $\left[\underline{H_y}, \overline{H_y}\right]$, $\left[\underline{F_i}, \overline{F_i}\right]$, $\left[\underline{G_k}, \overline{G_k}\right]$ are respectively lower and upper value of motion detector`s characteristics of 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 abovementioned factors we obtain an authorized access in the form of knowledge matrix.

Table 1. Knowledge matrix used to classify threat of 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	
6	0	0	1	S_2
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 amount of classification groups for indexes of protected perimeter; N – amount of rows.

2. First λ columns of matrix correspond to input variables H_y, F_i, and G_k, but $(\lambda+1)^{th}$ column corresponds to the value S_{θ}^{pvs} of 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 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}^{o} that is placed at the intersection of row and column corresponds to linguistic assessment of input data parameter and take place in the determination of possible value of output variable that detects an 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 possible solutions. In this case, the system determines the presence of unauthorized access to the area of subdivision on duty S_{θ}^{pvs}, $\theta = \overline{1,\mu}$.

IF (F=0) AND [((H=0) AND ((G=0) OR (G=1)) OR (H=1) AND ((G=0) OR (G=1))], THENS=S_2, ELSE, S=S_1 (11)

If the location of subdivision on duty is at 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 structure of information system for ranking objects, which are threats of unauthorized access to the perimeter for protected area have been proposed. This system consists of: contactless radio frequency identification subsystem (RFID), intelligent video surveillance subsystem, DSS of detecting and prevent unauthorized access to the perimeter of protected area, subsystem of detection the movement along protected perimeter. Integration and implementation of these subsystems allows to automate the process of violators detection and the process of decision-making for alarm generation.

2. The first time the model of components interaction for information system of ranking objects, which are threats of unauthorized access to the perimeter for protected area has been proposed. This model determines informational flows and realizes the interaction of system components. Also it was determined 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 subdivision on duty with the aim to destroy or to invade staff and/or informational-technical objects.

4. The method of detecting unauthorized access to the perimeter for protected area has been proposed. It is constructed with a help of productive model of knowledge representation, that 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.

5. 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 security level of guard subdivision and subdivision on duty. This technology makes be automated processes of violator detection and decision-making for alarm generation. 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] Yudin O.K. Information security in data networks [Text]/ O.K. Yudin, O.G. Korchenko, G.F. Konahovych, Kyiv, Interservis, 2009, 719 p.
[2] Information security and economic safety for enterprise: monograph [Text] / O.O. Kuznetsov, S.P. Evseev, S.V. Kavun, Kharkiv, KhNEU, 2008, 360 p.
[3] Graivoronsky M.V. Safety information and communication systems [Text] / M.V. Graivoronsky, O.M. Novikov, Kyiv, BHV, 2009, 608 p.
[4] Pilkevych I.A. Information security in ICS: tutorial [Text] / I. Pilkevych, K. Molodetska, N. Lobanchykova, Zhytomyr, ZhSU, 2014, 170 p.
[5] Kavun S.V. Information security: manual / S. V. Kavun, Kharkiv, KhNEU, 2009, 368 p.
[6] Zavgorodny V. I. Complex protection of information in computer systems: tutorial [Text] / V. Zavgorodny, Moscow, Logos; 2001, 365 p.
[7] Belov E. Basis of information security: tutorial for higher education [Text] / Belov E., Los V., Meshcheryakov A., Moscow, Studio, 2006, 356 p.
[8] Malyuk A.A. Information security and conceptual and methodological framework for the information security: [tutorial for higher education], Moscow, Hotline-Telecom, 2004, 280 p.
[9] Zgurovsky M. Z. Basis of system analysis: manual [for higher aducation] / M. Z. Zgurovsky, N. D. Pankratova, Kyiv, BHV, 2007, 544 p.

Dr. Mazin Al Hadidi was bom in Jordan in October 1966; He earned his Ph.D in 1994, in Engineering Science (Computers. Systems and Networks). He received his M.Sc in 1990 in Engineering Science (Computer and Intellectual Systems and Networks). He is presently associate professor at the Computer Engineering Department at Al-Balqa Applied University, Jordan. Dr. Al Hadidi published many research papers in many topics such as computer networks, image processing, and Data Hiding, and many others.. .He is a reviewer for several journals and conferences. He was appointed in many conferences as keynote speaker, reviewer, track chair and track co-chair.
^

Dr. Jamil S. Al-Azzeh received his PhD Degree in Computer Engineering from Sami Petersburg State University -Russia in 2008. Since 2003. Dr. Al-Azzeh has been an associated professor in the Computer Engineering Department. Faculty of Engineering Technology, at Al-Balqa' Applied University. His research interests include image processing, computer system architecture, parallel processing FPGA. Digital systems design, network operating system, and Microprocessors.

Hussein A. Al ofeishat Associate professor at Al-Balqa Applied University / Department of Computer Engineering

I earned my Bachelor and master Degree from Department of Computer Engineering, National Technical University of Ukraine in 1992 . 2005 I got my PhD in Computer Engineering / computer network from Department of Computer Engineering, National Technical University of Ukraine (KPI). Since 2016 to present Dean of Faculty of Engineerin

Dr. Nadiia M. Lobanchykova – 2002, Zhytomyr Engineering and Technological Institute, Specialty "Control systems and automatics", Candidate of Engineering Sciences, Associate Professor at the Department of Computerized management and automation system of Zhitomir State Technological University. Scientific interests: Information technology, Cybersecurity, Sensor networks.

Dr. Svetlana M. Kredentsar – 2005, East Ukrainian National University named after Volodymyr Dahl, Severodonetsk, Specialty "Computer systems and networks", Candidate of Engineering Sciences, Associate Professor at the Air Navigation systems department, National Aviation University, Kyiv. Scientific interests: Information technology, Geoinformating systems

Dr. Roman Odarchenko: PhD, Associate Professor of Telecommunication systems academic department in NAU. M.Sc. (2010), Ph.D. (2013) from the NAU, teacher in Kyiv College of Communication. Major research interests: Network Security, Communications, Data Processing, Sensor networks, Computer networks, Education Technology.

Dr. Ivan R. Opirsky, PhD, Associate Professor of Information security academic department in National University "Lviv Polytechnic". M.Sc. (2008), Ph.D. (2012). Major research interests: Computer Network and Technical Security, State Secret Security, Mathematical Methods and Models of Information Security.

, PhD, Associate Professor, **Dr. Nurgul A. Seilova** Head of Information security academic department in Kazakh National Research Technical University. M.Sc. (2001), Ph.D. (2010). Major research interests: Computer Networks and Information Security, Data Bases, Communications, Data Processing.