Computer simulation of functioning of elements of security systems

A V Godovykh, B P Stepanov, A A Sheveleva

Tomsk Polytechnic University, 634050 Russia, Tomsk, Lenin Avenue, 30

e-mail: aas@yandex.ru

Abstract. The article is devoted to issues of development of the informational complex for simulation of functioning of the security system elements. The complex is described from the point of view of main objectives, a design concept and an interrelation of main elements. The proposed conception of the computer simulation provides an opportunity to simulate processes of security system work for training security staff during normal and emergency operation.

1. Introduction

Safe functioning of the industrial facility cannot be possible without creation of a security system. Usually, an automated systems execute the management of the security system. Such systems presuppose the presence of people [1, 2]. In this case, the security staff should perform competent and prompt actions, because it defines the capabilities of the system to resist threats.

Objectives of the security staff are: to observe the operation of facility, to react to alarm signals, to manage the response forces for capture of adversary. Training of the security staff is necessary to increase the protection level of an object [3]. However, such kind of trainings on the basis of the real security system are impossible. Depending on the field of activity of the staff, different training methods can be implemented. It can be consideration of technical and legal documentation, operation of specialized stands with technical equipment. But, the best complex training can be implemented using integrated electronic training devices that are based on modern modelling technologies. These training simulators can be formed as specialized computer workstations [4]. Its features are only limited by assigned tasks.

2. Basic elements of the analytical complex

The informational complex is considered as a computer-based workstation that simulates an interaction between an attacker and a security system of the object, where both sides are controlled by the users. The automated workplace simulates functions of security systems to provide training opportunities for a training staff.

Main objectives of the complex are:

- training of skills of the operators of the control center;
- formation of abilities to observe and analyze the information by the security system staff;
- learning the decision-making methods caused by an unauthorized activity.

Work of the complex is based on the simulation of interaction "attacker - security system" with regards of characteristics of both [5]. The main functions of the complex are performed by a special

software. It stores and archives data, executes algorithms, makes a connection between units and a fundamental mathematical model, visualizes the processes.

The software configuration is designed in the form of target blocks - units, which are allocated according to the performing tasks [6]. The units operate data that are represented by embedded or customer databases. Core units are presented in Table 1.

Table 1. Basic units of the analytical complex

	Function		**Name of unit**
1	First level	"Static" model	Construction Unit Evaluation Unit
	Description of basic characteristics of the object and the attacker		
2	Second level	"Dynamic" model	Imitation Unit
	Performing of interaction algorithms		
3	Third Level	Visualization	Visual Unit Interface Unit
	Displaying of the object, events and interface		
4	Support	Service	Information-analytical unit
	Legislative and methodical maintenance		

Constructive, evaluation and imitation units are the basis blocks of the complex. The first two are responsible for the imitation of the first level model – a "static" model. At this level, a user describes basic characteristics and the infrastructure of the object, for example: features of an object, properties of engineering and technical means of a security system etc. In addition, a user defines the general characteristics of both sides: the number of response forces and attackers, their "tactics" etc.

The imitation unit is responsible for the second level of the simulation. This level is determined by dynamic parameters of the model. At this stage, interaction algorithms of elements of the first level model are defined. Examples are the implementation of different "tactics" and versions of scenarios for response forces and attackers; the influence of an intruder; simulation modeling within an emergency situation etc.

The visual unit presents the third level of the simulation. Its function is to display the prototype of an object and events in a form that is convenient and realistic for a user. Another purpose is to visualize a graphical user interface. Along with the interface unit, the visual unit maintains a connection between a user and resources of the analytical complex [7]. The interface unit administrates a software interaction between databases and units. It is also responsible for linking organization of hardware, which is combined into an automatized workplace.

Visualization of security systems pursues a number of objectives. In turn, the computer simulation gives the ability to display the object of research as a combination of elements and their properties. In forming the initial requirements to the model of an object with considering the possibility of subsequent visualization, it is logical to determine the levels of detailing and connections of the visualization and computational parts of the model.

Imaging techniques in varying degrees are based on source data of the model. When forming the functional part of the security system model, its visualization is possible through the following options. The option one is when two separate units: visual and evaluation, are connected only at the logical level and their purpose is demonstration. An alternative option is a more "dense" interaction of the model elements and connections, up to the use of additional methods and visualization techniques.

In case of simulation of security systems, the "interactive environment' is in the spotlight. It is focused on computational models of physical and technical parameters of the technical means, response forces and variants of their complex interaction. Related tools provide construction activity at the information and documentary level that extends the functionality of such an environment. And the

presence of a well-prepared graphical database converts this model in the framework of the environment at a significantly different level.

The information-analytical unit is responsible for informational support of the analytical complex. It is reference-methodical maintenance and a legislative and regulatory framework related to the operation and the construction of the security systems [8]. This unit presented as a database consisting of documentation related to security systems. It is an interactive documentary search engine to quickly find the desired information using a variety of filters. Besides, a user can add, remove and change the stored information. Extra tools for work represent analytical functions with the evaluation unit. This unit also allows choosing the modes of operation of the analytical complex depending on the demands in training of several types of the staff of the security systems.

3. Data sources

The databases form a resource base for describing parameters of the object and interacting elements. In general, databases are considered as systematized and categorized data. Their purpose is information support of the organization of the simulation process. Databases consists of numerical characteristics, independent or combined parameters as well as graphical and other elements of visualization. One or few units can use multiple elements of the databases.

Additional plug-resources - custom databases also can be used [9]. They give the opportunity to upload and download data for special calculations. An identical opportunity is presented for working with graphics and algorithmic resources. This greatly expands capabilities of the system as a whole.

All the data used by the informational complex are shown in Table 2 [10].

Table 2. Primary data sources

Type	Name	Description	Parameters
Active members	Attacker	characteristics of outside adversary	- number; - qualification; - type; - equipment etc.
	Guards	characteristics of response forces	
Description of the object	Object	description and features of secure object for simulation purposes	- characteristics of standard objects; - targets (object of defense); - operation mode; - threats; - operation mode; - site area parameters etc.
	Barriers And Sensors	parameters of engineering and technical means of security system	- type; - time of delay; - triggering probability; - strength and durability - location etc.
Support	Library	legislative and regulatory framework, supporting assistance	- information support; - fragmentary and full text documents; - visual material etc.
	Media	video, sound data, graphical primitives	- primitives and elements of graphical maintenance; - video elements; - acoustic elements etc.

A user can perform different types of training. He can observe and analyze data from video surveillance and sensors, performing a role of an “operator of the security system”, while the other is trying to disrupt the facility as an attacker. An expert mode allows a synchronous organization up to

four roles. Active Members are an "operator of the security system", an "attacker" and "response forces". Passive participants are "observer experts". The number of participants of the "training" determines the maximum number of personal devices.

The minimal configuration of the complex can be formed as a personal device. It is enough for training of the operator of security systems. The automatized workstation is organized with the simultaneous operation of the server and client parts of the complex.

The local configuration of each of the personal devices includes a specialized software, the subunits of the security staff and the adversary, the data on engineering and technical means [11, 12]. Thus, each workstation is a separate system and can be used independently from other workstations. The interaction between the users and subsystems of the instructor and the operator is implemented through the appropriate interfaces. The considered configuration suggests the possibility of a separate and independent work in training.

4. Conclusion

As a result of the work, the conception of the informational complex to simulate the work of security systems is developed. The proposed set of the core units enables modelling of a security system, and then, on this basis, performing the functioning of the used engineering and technical means. Thus, this allows one to simulate the interaction "attacker – security system". This development can be used for training of a security staff, effectiveness evaluation of used engineering and technical means.

5. References

[1] Garcia M L 2005 *Vulnerability Assessment of Physical Protection Systems* 1st ed (Butterworth-Heinemann) p 400
[2] Lovecek T, Ristvej J, Simal L 2010 Critical Infrastructure Protection Systems Effectiveness Evaluation *J. of Homeland Security and Emergency Management* 7 p
[3] Fischer R J, Hailibozek E P, Walters D C *Introduction to Security* 9th ed (Elsevier) p 544
[4] De Jong T, Linn M C, Zacharia Z C 2013 Physical and virtual laboratories in science and engineering education *Science* **6130** 305-308
[5] Bukovetskiy A V, Stepanov B P, Tatarnikov D A 2016 Initial Data Forming for Process Simulation in System "Intruder – Physical Protection System" *Key Engineering Materials* **685** 148-152
[6] Godovykh A, Stepanov B 2015 Development and Creation of Software and Information Environment for Simulation of Nuclear Facility *Advanced Materials Research* **1084** 652-654
[7] Darrah C 1995 Workplace Training, Workplace Learning: A Case Study *Human Organization: Spring* **54** 31-41
[8] Garcia M L 2007 *The Design and Evaluation of Physical Protection Systems* 2nd ed, (Butterworth-Heinemann) p 370
[9] O'Neil H F, Perez R S 2013 *Web-based learning: Theory, research, and practice* (Routledge) p 444
[10] Fennelly L 2012 *Effective Physical Security* 4th ed (Butterworth-Heinemann) p 384
[11] Lee W W, Owens D L 2004 *Multimedia-based instructional design: computer-based training, web-based training, distance broadcast training, performance-based solutions* 2nd ed (John Wiley & Sons) p 488
[12] Dennis J 1987 Computer Based Training *Education + Training* **29** 11 – 12