Simulation of the effectiveness evaluation process of security systems

A V Godovykh[1], B P Stepanov[1], A A Sheveleva[1], K R Sharafieva[2]

[1] Tomsk Polytechnic University, 634050 Russia, Tomsk, Lenin Avenue, 30
[2] Tomsk State University, 634050 Russia, Tomsk, Lenin Avenue, 36

e-mail: aas@yandex.ru, ruf_84@mail.ru

Abstract. The paper is devoted to issues of creation of cross-functional analytical complex for simulation of the process of operation of the security system elements. Basic objectives, a design concept and an interrelation of main elements of the complex are described. The proposed conception of the analytical complex provides an opportunity to simulate processes for evaluating the effectiveness of physical protection system of a nuclear facility. The complex uses models, that take into account features of the object, parameters of technical means and tactics of adversaries. Recommendations were made for applying of this conception for training specialists in the field of physical protection of nuclear materials.

1. Introduction

Smooth functioning of the security system is one of the essential parts of the operation of a nuclear facility. The effective security system combines an activity of staff, administrative measures and correctly functioning set of engineering-technical means [1]. Management of the security system is carried out by an automated system that presupposes the presence of people. In this case, competent and prompt actions of the security staff define the system capabilities to resist to threats with regard to an object of defense.

Training of the security staff is an effective way to increase the protection level of an object. However, training of security staff on management of the technical equipment and response forces is impossible on an active security system. Depending on area of activity of the staff, different approaches to training can be implemented. It can be consideration of technical and legal documentation, usage of specialized stands with technical equipment of security systems. This methodological approach allows to simulate the operation of the security system to the maximum extent possible. Nowadays are widely used integrated electronic training devices that based on modern modelling technologies. These training simulators are usually implemented as specialized computer workstations. Its features are only limited by assigned tasks.

2. Design of the analytical complex

The cross-functional analytical complex is considered as an automated workstation that has a wide range of features to simulate an interaction between adversary and security system of the object. The automated workplace provides training opportunities to perform specified functions of security systems.

Main goals of the analytical complex are:

- performance of the analytical work on the effectiveness evaluation of the security system of an object;
- simulation of the interaction “adversary - security system”;
- skills training of the operators of control center;
- formation of capabilities to sensing and analyzing of the information by the security system staff;
- learning the decision-making methods caused by unauthorized activity.

The main element of the developing analytical complex is dedicated software. It stores and archives a data, executes algorithms, organizes a connection between units and fundamental mathematical model, visualizes the processes.

The software configuration is divided to target blocks - units, which are allocated according to set tasks [2]. The units, in turn, operate data, that represented by embedded or customer databases. In general, databases are considered as systematized and categorized data. Its purpose is information support of the organization of the simulation process.

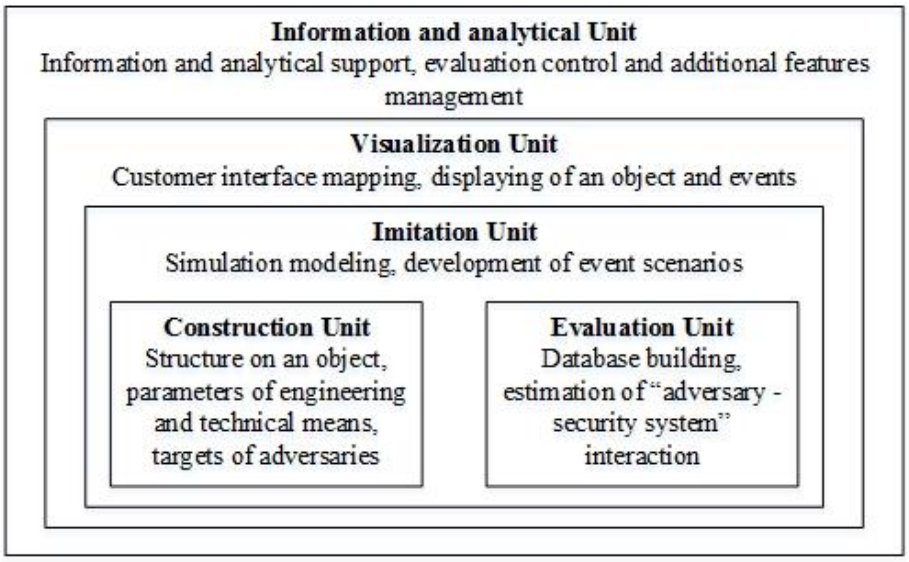

Figure 1. Main units of analytical complex

Constructive, evaluation and interface units are the basis of the analytical complex. The first two is responsible for the imitation of the first level model – “static” model. At this level, basic characteristics and infrastructure of the object are described: features of surrounding area, properties of engineering and technical means of physical protection system (PPS) etc. In addition, general presumptions are defined: number of response forces and adversaries, its “tactic” etc. Sufficiency and correctness of source data are verified for further PPS effectiveness evaluation based on incorporated mathematical model.

The imitation unit is responsible for the second level of the simulation. This level is determined by dynamic parameters of the model. It forms model's extended functions. 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 adversaries; influence of intruder; simulation modeling within emergency; PPS effectiveness calculation algorithm etc.

The visual unit presents the third level of the simulation. Its function is to display the prototype object and events in a form that is convenient and realistic for user. Another purpose is to visualize a graphical user interface. Along with the interface unit, the visual unit maintains connection between user and resources of analytical complex.

The information-analytical unit is responsible for an informational support of the analytical complex. It is reference-methodical maintenance and legislative and regulatory framework related to physical protection of nuclear materials. Extra tools for work represent analytical functions with evaluation unit. This unit also allows to choose the modes of operation of the analytical complex depending on the demands in training of several types of the staff of the security systems.

The interface unit (it is not pictured in the figure) administrates software interaction between databases and units. It is also responsible for linking organization of hardware, which is combined into automatized workplace.

Table 1. Primary data sources

Name and short description	Supported units	Content
"Attacker" – characteristics of outside adversary	Construction Imitation Evaluation Information and analysis	- number; - type; - probability of conspiracy; - qualification; - equipment etc.
"Guard" – characteristics of response forces		- number; - type; - qualification; - equipment etc.
"Barriers" – parameters of engineering means of physical protection		- type; - time of delay; - location; - way to bypass; - strength and durability etc.
"Sensors" – parameters of technical means of physical protection		- type; - location; - triggering probability; - false triggering probability; - strength and durability etc.
"Library" – legislative and regulatory framework, supporting assistance	Imitation Information and analysis Visualization	- information support; - fragmentary and full text documents; - visual material etc.
"Facility" – description and features of secure facility for simulation purposes	Imitation Information and analysis Visualization	- characteristics of standard objects; - targets (object of defense); - threats; - operation mode; - site area parameters; - others features: climate, political and geographical parameters etc.
"Media" – video, sound data, graphical primitives	Construction Information and analysis Visualization	- primitives and elements of graphical maintenance; - video elements; - graphical objects; - acoustic elements; - dynamic elements etc.

The databases are a resource base for simulation of the object. They are represented as numerical characteristics, independent or combined parameters and as graphical and other elements of visualization. One or few units can use the elements of the databases.

All the databases used by the analytical complex are shown in Table 1.

The minimal configuration of the analytical complex can be presented as a personal device. It is enough for training of the operator of security systems. The automatized workstation is organized with simultaneous operation of the server and client parts of the complex. But this case only locally pledged situations can be processed through running of specialized software complex. Also parallel analysis of operator actions in a simulated situation is significantly reduced.

An expert mode allows a synchronous organization up to four roles. Active Members are "operator of the security system", “intruder” and “response forces”. Passive participants are “observer experts”. The number of participants of the “training” determines the maximum number of personal devices.

The local configuration of each of the personal devices includes specialized software, the subunits of the security staff and the adversary, the data on engineering and technical means. 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 operator is implemented through the appropriate interfaces. Considered configuration suggests the possibility of a separate and independent work in training.

3. Effectiveness evaluation

The effectiveness evaluation is one of the core tasks when creating of security system. Estimation of this criterion is executed within the assigned target, method of threat response and selected criteria of efficiency (probability to interrupt of adversary). Depending on the criteria, efficiency of the security system can be estimated based on different methods [3]. It can be experimental evaluation or analytical estimation in terms of specialized software. In addition, security system effectiveness can be estimated during different stages of its development.

There are psychophysical problems that occur during operation of the security staff. Among these are a monotony of the work, an operator's fatigue, a necessity to analyze a lot of displayed data. However, efficiency of the security system depends much on operator's quality of work. Nevertheless, efficiency of the security system depends much on operator's quality of work, his quick reaction capability, adaptability and flexibility to changing of situation. Identification of alarm at the appropriate time, detection of malfunctions of sensors and defined response – are the confirmations of operator's preparedness to control and management of security system.

Methods of security system effectiveness evaluation were considered within the proposed conception of analytical complex. It was highlighted, that generalized criterion of the efficiency of security system is a decision-making time by an operator of the system. In these terms, the response time divides into length of the main stages.

In this case the main stages of security system staff activity are the detection of an intruder, the decision-making time (which includes time of alarm communications and time of an assessment), the time of preparation of the response forces and their further time of interruption of adversary. The travel time of intruder divides into parts that correspond to the real adversary’s tasks. The whole action sequence of adversary includes overcoming of barriers, travel on territory of an object, access to building and travel within it, room access, and access to the defense object. All stages of actions of adversary and response forces are pictured on the figure 2.

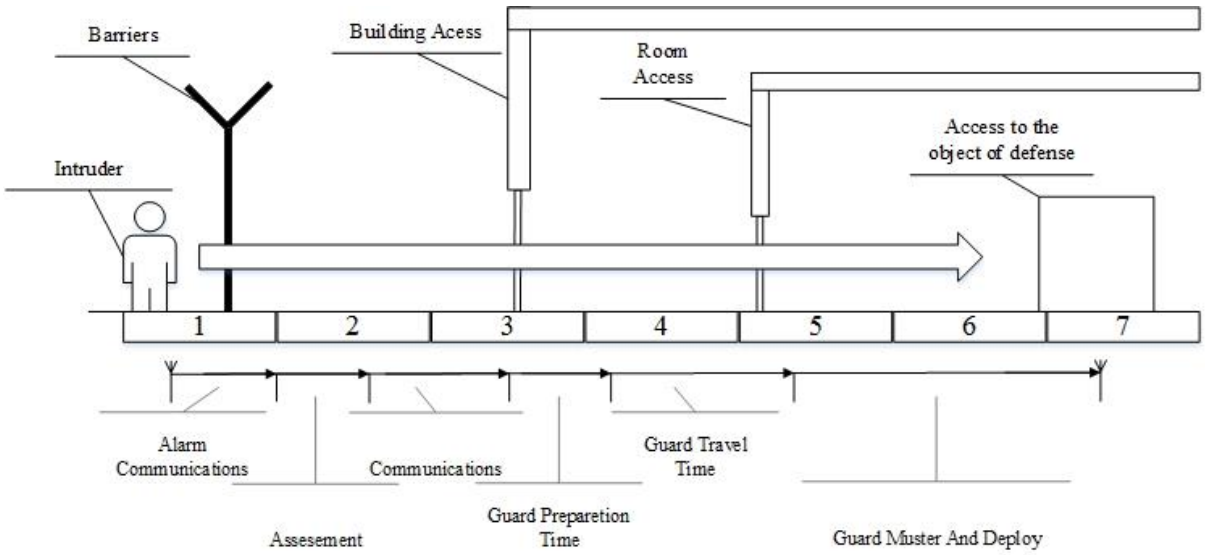

Figure 2. Stages of actions of adversary and response forces within the protected object

The total time of the intruders' action on each stage is formed based on parameters of used engineering and technical means as well as characteristics of adversary and response forces. As a result of interaction a diagrammatic model is constructed, on which the time of adversary and response forces are recorded. The classic methods based on timeline represents a quantitative approach to the effectiveness evaluation [3,4]. The result of these methods is a determination the probability of interruption the adversary's actions [5]. This probability depends on the strategies of intruders and response forces, level of an equipment of the object by engineering and technical means of the security system.

Based on the obtained data, the time of operator actions as well as probability of penetration interruption of the offender is evaluated. These results characterize the accuracy and speed of the executed operator's procedures. In setting the initial data for modeling the interaction in the system "intruder - security" for the effective working of the operator takes time and the probability of successful performance of the task for an adjustable time interval [6].

In terms of presented conception of analytical complex, the main criterion of security system effectiveness is the effectiveness of operator's work.

Within the performance of analytical complex, proposed model allows to evaluate the effectiveness of a whole security system of an object as well as effectiveness of the security system's staff work.

The effectiveness of the operator's work can be determined as the probability of the successful performance of the task for a specified time interval.

Operator error is defined as fail in performance of the task (or performance of forbidden actions), which can cause disruption of the security system [7]. There are also several factors that can be regarded as the operator errors. The operator can be committed to achieving the false target. The target cannot be reached because of the wrong actions of the operator. The operator is inactive at the moment when it is necessary to participate.

Thereby, the efficiency of the operator's work is characterized by response speed and reliability. The criterion of the response speed is the decision-making time; in other words, it is time from the response to the incoming signal until the end of control actions.

Special attention was paid to the factors that are associated with the organization of the operator's workstation. For better performance of the training functions, the imitation must correspond to the real conditions of the work.

Based on the described above suppositions and features of design of the analytical complex, the modelling capabilities of the object are represented at appropriate level according to the related goals. Basic requirements regarding the effectiveness evaluation of the operator's work are:

- Conformance of developed display mode to the real elements of the control system used by the operators;
- Sufficient authenticity and approximation of mathematical interpretation of interaction between adversary and security system;
- Appropriate level of abstraction in description of technological processes.

A number of standard actions is identified for the security staff. They must to be made when the alarm signal occurs or in case of false alarm as well as in case of disruption of a technical mean. When these situations are being simulated within the analytical complex, the response speed, the quality of conformance of actions to the standard, operator's actions are being assessed.

It is worth noting that since the adversary in this interaction is also a person, the details and specifics of the situations will be different due to the nature of each individual's personality.

4. Conclusion

As a result of a work the conception of the analytical complex to assess the effectiveness of security systems is developed. The proposed set of the core units enables to model an object security system, and then on this basis, to evaluate the effectiveness of used engineering and technical means. In addition, the complex has enough functionality to assess the effectiveness of operator's actions. This provides a comprehensive approach to the effectiveness assessment of security systems, which takes into account the individual characteristics of the personality.

This analytical complex can be used within security system operator's automatized workstation for training of “person - security system” interaction.

One of the distinctive features is function that provides maximum variability when specifying the object and editing the existing interaction mechanisms and methods of evaluation. Besides, functional capability on realization of experts' analytical work on effectiveness of security systems' assessment is provided.

References

[1] Garcia M L 2005 *Vulnerability Assessment of Physical Protection Systems* 1st ed (Butterworth-Heinemann) p 400
[2] Godovykh A, Stepanov B 2015 Development and Creation of Software and Information Environment for Simulation of Nuclear Facility *Advanced Materials Research* **1084** 652-654
[3] Lovecek T, Ristvej J, Simal L 2010 Critical Infrastructure Protection Systems Effectiveness Evaluation *J. of Homeland Security and Emergency Management* 7 p
[4] Fennelly L 2012 *Effective Physical Security* 4th ed (Butterworth-Heinemann) p 384
[5] Garcia M L 2007 *The Design and Evaluation of Physical Protection Systems* 2nd ed, (Butterworth-Heinemann) p 370
[6] 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
[7] Fischer R J, Hailibozek E P, Walters D C *Introduction to Security* 9th ed (Elsevier) p 544