Risk-informed Security System. The Use of Surveillance Cameras for the Particularly Hazardous Facilities Safety

M.A. Berberova[1,2], A.S.Oboimov[1], A.Kh.Khakimova[2], O.V.Zolotarev[3]
maria.berberova@gmail.com | anton.oboimov@gmail.com | aida_khatif@mail.ru | ol-zolot@yandex.ru
[1]International Nuclear Safety Center, Moscow, Russia
[2]ANO «Scientific and Research Center for Information in Physics and Technique», Nizhny Novgorod, Russia
[3]ANO «Russian New University», Moscow, Russia

In the context of a difficult criminal situation in the world, taking into account the globalization of world development processes, international political and economic relations, which pose new risks for the development of the individual, society and the state. In the Russian Federation, as well as throughout the world, threats to the safety of industrial facilities are steadily increasing.

Moreover, in connection with the improvement of organization and the expansion of the technical equipment of potential violators (terrorists, extremists, etc.), the improvement of methods and methods of illegal actions, issues related to the rationalization of technologies aimed at protecting vital interests and resources of enterprises.

One of such technologies includes the creation of an effective automated security system and counteraction against unauthorized entry of individuals - a physical protection system, technically based on a set of engineering and technical means.

The process of designing a set of engineering and technical means of a physical protection system for industrial facilities includes two main stages: conceptual and detailed design, and the optimality of design and engineering solutions in general depends on the successful implementation of work at the conceptual design stage.

The assessment of the scale of the intruder's invasion is characterized by the time spent by the intruders in the control zone by television cameras, their tactics of overcoming this zone, time of day, illumination, etc.

In this work, we use the analysis of images obtained from surveillance cameras.

Keywords*: risk, security system, physical protection system, risk-informed security system.*

1. Introduction

The physical protection system (PPS) model consists of several components: the intruder model, the object model. An intruder model is a combination of an intruder’s action strategy and skill matrices: a probability matrix P_{11} and times matrix T_{12}.

$$P = \begin{pmatrix} p_{1,1} & p_{1,2} & \cdots & p_{1,n} \\ p_{2,1} & p_{2,2} & \cdots & p_{2,n} \\ \cdots & \cdots & \cdots & \cdots \\ p_{m,1} & p_{m,2} & \cdots & p_{m,n} \end{pmatrix} \quad (1)$$

The element of the times matrix $T_{i,j}$ is the time of overcoming the i^{th} type PPS element, using the j^{th} skill from the violator's skill set.

$$T = \begin{pmatrix} T_{1,1} & T_{1,2} & \cdots & T_{1,n} \\ T_{2,1} & T_{2,2} & \cdots & T_{2,n} \\ \cdots & \cdots & \cdots & \cdots \\ T_{m,1} & T_{m,2} & \cdots & T_{m,n} \end{pmatrix} \quad (2)$$

In modern conditions, the physical security culture of nuclear facilities attracts increased attention. Among other benefits, an effective safety culture requires staff to take action and innovative approaches in situations where threats and risks are too numerous for even the most forward-looking leaders to predict [1].

In 2007, the U.S. public was shocked by the news that several professional guards were found sleeping at their posts while serving at the Peach Bottom NPP (Fig. 1, 2) [2]. Around the same time, four armed intruders broke into the Pelindaba nuclear installation in South Africa, where hundreds of kilograms of weapons-grade uranium were stored. The criminals managed to disable several levels of physical protection of the object, but they were not detected by the guard, because no one was watching surveillance cameras. After the collapse of the Soviet Union, hundreds of radioactive sources that pose a serious danger to the population and contain radioisotopes that can be used to create dirty bombs were thrown into the territory of a number of newly formed states. Such sources harmful to human health and the environment are still annually removed from remote areas of Georgia. These and other, seemingly random and unrelated incidents, nevertheless have one common critical feature - the «failure» of the human factor.

Fig. 1. The Peach Bottom NPP

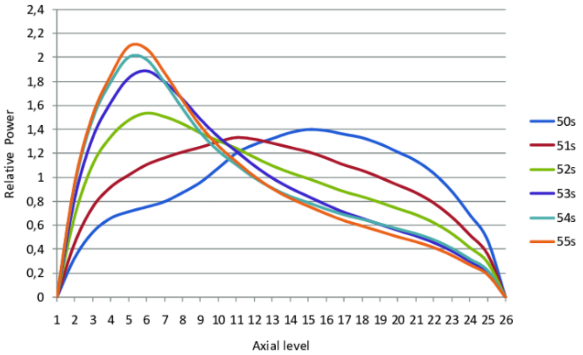


Fig. 2. Axial relative power profile evolution in the Peach Bottom NPP

Italian psychologists say that of all employees in any company, 25% are honest people, 25% expect an opportunity to divulge secrets, and 50% will act depending on the circumstances (Fig. 3) [3].

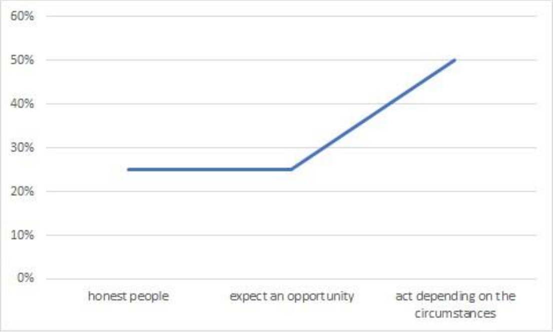


Fig. 3. The results of a study by Italian psychologists

In 1994, three reporters of the London Sunday Times conducted an experiment. Posing as businessmen, they went to twenty deputies of the British Parliament with a proposal to send a request to the government in which they are interested and receive a thousand pounds in cash or by check. 20 out of 27 immediately refused, three agreed. Similar experiments were carried out by the FBI in the early 80s: FBI agents under the guise of Arab sheikhs appealed to members of the American Congress, offering them rewards of tens of thousands of dollars for all sorts of concessions to be arranged for the «sheikhs» [3].

From this it follows that the likelihood of a «refusal» of the guard or the dispatcher on the remote control as a result of bribery is quite high. But there are also possible scenarios with the elimination of the protection of the checkpoint as a result of a military collision or an error of the dispatcher.

No less problematic is predicting the actions of people in an extreme situation similar to an attack on the object of violators. Even despite scrupulously designed instructions and a natural logic of behavior, a person in extreme conditions quite often behaves completely unpredictably, sometimes even reducing the effectiveness of the entire system to zero [1].

Violation of the instructions sometimes costs much more than the failure of an expensive video camera or computer. According to statistics, the largest fires begin with a fire, to which the on-duty shifts of specialists do not respond. Most robberies of collectors occur when they violate simple service instructions. Guarded offices, restaurants, shops "hand over" to the criminals psychologically unprepared security guards. More than half of the confidential information is distributed by their own employees, pushed by personal dissatisfaction and simple tricks of interested parties. There are many more such examples. And if we are talking about objects of increased technological risk, and in particular, nuclear power facilities, then the issue of the reliability of personnel in general and physical protection personnel in particular becomes critical.

For tasks related to physical counteraction in conflict situations, this problem is extremely relevant. It is impossible to assume the absence of criminal threats to protected objects, the results of the PPS analysis contradict this, the very fact of the creation of the PPS contradicts this. Of course, the head of the security service assures the management or owner of the facility and must be sure that the security officer will strictly comply with the approved service instructions and in the conditions of criminal or terrorist threats will ensure security without violating the laws and obligations assumed by the security. This is especially important when using weapons. However, for most security leaders, the guard’s behavior in an emergency situation remains a mystery. So, for example, two teenagers who went into the boutique with an air pistol screamed heartily on the floor of a hefty security guard, whose appearance alone assumed guaranteed protection against a thug's platoon. Adolescents strolling among showcases demanded and received a ring from the guard's hand. In the course of the trial, the reason for what happened remained unclear, the security company lost the facility, the guard quit, the management changed. However, guarantees that such an inexplicable phenomenon does not happen again are given after the third «cup of tea» and are inexpensive. And again, if we are talking about nuclear facilities, there can be no «sweat» either for security personnel or for its management.

There is no doubt that the professional readiness of security structures depends on maintaining and maintaining the appropriate psychological state of their employees. Specialists from police structures claim that only 25% of employees retain the ability to reasonably act in extreme conditions; 75% temporarily lose it; 10-12% lose it for a long time. According to psychologists, every fifth employee is doomed to professional psychological trauma. Psychological unpreparedness is the reason for the inability to assemble in extreme conditions (73%). Only about 30% of the employees of the structures under consideration are able to independently overcome crisis events, while maintaining the integrity of the personality and internal balance, are able to withstand the so-called phenomenon of professional personality deformation [1].

People in the extreme conditions characteristic of security activities often cannot act competently, and this is a general pattern. It is rather difficult to find «ideal men»; you need to be able to work with representatives of most homo sapience, forming professionals from them. This problem can be effectively solved only with the organization of psychological support.

However, in this paper it is not a question of psychological preparation, but it is proposed to approach the issue of increasing the level of security on the other hand. At the stage of analyzing the effectiveness of the PPS of an object, using tools of a risk-informed approach, fundamentally possible violators, tactics and scenarios of their actions were described, both invasion scenarios and counter-action scenarios to neutralize the intruder were modeled.

The task of keeping in memory all the instructions for all cases of attackers' actions, and, more importantly, the task of timely detection and recognition of unauthorized, hostile actions, these tasks are very difficult for operators or security personnel on duty of any more or less large object, this also explains the high psychological load on the operator. And this task can be greatly simplified by providing information support to the operator, issuing accurate data on the current state of affairs, helping to detect possible attacks at an early stage, issuing clear instructions on what to do in a particular case.

2. Prototype risk-informed security system

As part of this work, a prototype risk-informed security system was developed.

A video surveillance system was chosen as the main system supplying information for processing. Modern video analytics has impressive capabilities, including recognizing people, tracking (tracking) people, including in multi-camera systems, recognizing prominent, suspicious behavior, such as running, loitering, and much more [4].

However, these capabilities are largely used idle, to the maximum, including recording to detect moving objects and signaling the operator about it. The whole burden of further analysis and decision-making rests solely with the operator. However, firstly, as already indicated, the operator’s efficiency depends strongly on the time of day, the total load, and many other factors and is insufficient for many cases. And secondly, as practice shows, often operators ignore what is happening on video cameras out of habit, for example, after several false positives or after a long period of absence of any attempts to violate the security of the protected object.

The developed prototype shows the principle of the entire system on the example of one room in a building.

To demonstrate the principle of operation of the entire system, one room is considered - a corridor, Figures 4-6 show screenshots of a working program. The entrance to the premises is guarded by an employee of the facility's security service, in addition, the entrance to the premises is blocked by a lock, such as a combination lock. The premises are supposed to have a certain «forbidden» zone in which any object of physical protection is located - the target of the offender. The camera monitors what is happening in the room in automatic mode, without operator intervention. Data from the camcorder is processed by the program. In the event that anyone appears in the room, the program starts tracking detected people, tracking all their actions and movements, while analyzing them.

A tree of events and a tree of failures are constructed for the premises, corresponding to the penetration of the intruder into the restricted area. Initial probabilities of events and failures are given. The probabilities of possible final events and failures are calculated in accordance with logical operations, tree gates.

If any of the events detected in the event tree is detected, the program automatically marks the event as occurring (its probability becomes equal to one), recounts the entire tree and signals an increase in the level of risk (and, therefore, an increase in the level of security threat), if any . All detected events, as well as their corresponding failures, are recorded in the system, which will subsequently, if necessary, trace the development of events, analyze the actions of the violator and PPS personnel, and develop proposals for improving the PPS and increasing efficiency.

The event tree in this program displays the following key events:

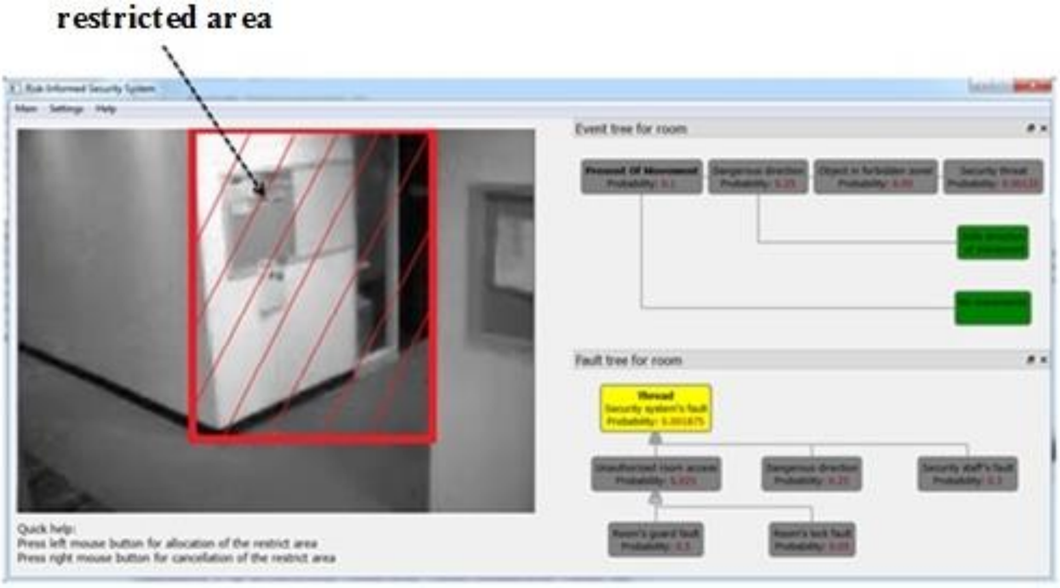
- The presence of movement (Fig. 4). The camera recorded the presence of movement in the room. First of all, this means that the detected attacker somehow got into the room, which means that the lock on the door or the security guard at the entrance to the room failed (either the guard is neutralized or he is in collusion with the intruder).
- Movement to the restricted area (Fig. 5). The presence of a person moving to a dangerous zone does not automatically mean that he is moving in the direction of the «restricted area», however, if the movement is directed in this direction, this further increases the risk.
- Penetration into the restricted area (Fig. 6). While the potential intruder has not yet entered the zone, it is likely that he will not penetrate there either: he will not be in time and will be delayed by the response group, or he will bypass it, or suddenly turn around and leave, for example, if he realizes that he will be caught and must be leave. However, if he entered this zone, this automatically means the failure of the response group, which did not have time or was unable for some reason to detain the attacker, the refusal of the lock or any access control system to the «restricted» zone, if any, well as well as the failure of the entire protection system, which allowed the intruder to enter the restricted area.

The event tree functions:

- Shows current recognized events that somehow affect the level of safety and risk and can lead to a negative outcome.;
- Shows further possible ways and scenarios of events in an explicit form on the operator's monitor;
- Provides a numerical estimate of the probability of the outcome of certain events.

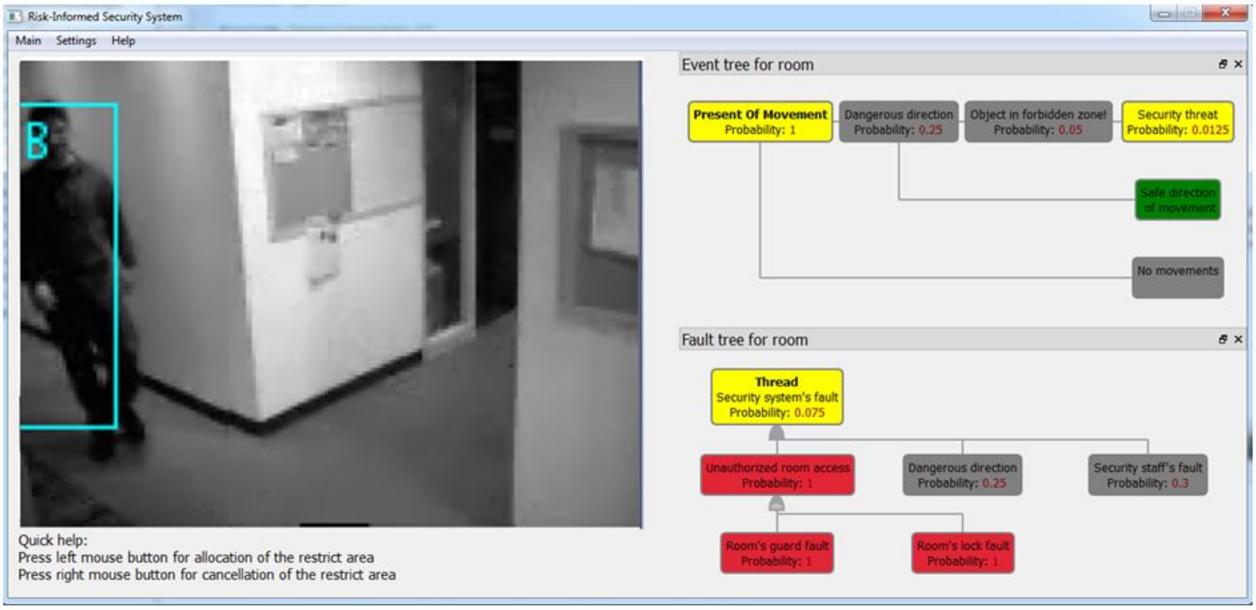
The fault tree in this case performs the following functions:

- shows the failure of which particular elements led to the fact that the offender was in a particular place, overcame this or that safety line;
- shows the impact of the failure on the entire system as a whole, explicitly shows the consequences, both possible and occurred. The fact is that modern protection systems were built on the principle of a single failure - it was assumed that if one of the system components failed, the entire system was able to provide the required level of security. However, this is far from always the case, in complex systems the failure of some elements can explicitly or implicitly affect the work of others, increasing the likelihood of their failure, and hence the current level of risk. This program clearly shows this on the operator's monitor, giving a sound notification;
- if there are appropriate instructions, it gives a warning about the need to turn on reserve PPS elements, send a response team to check the situation and, if necessary, detain the intruder, predicts possible failures of elements that depend in some way on already failed ones, etc.



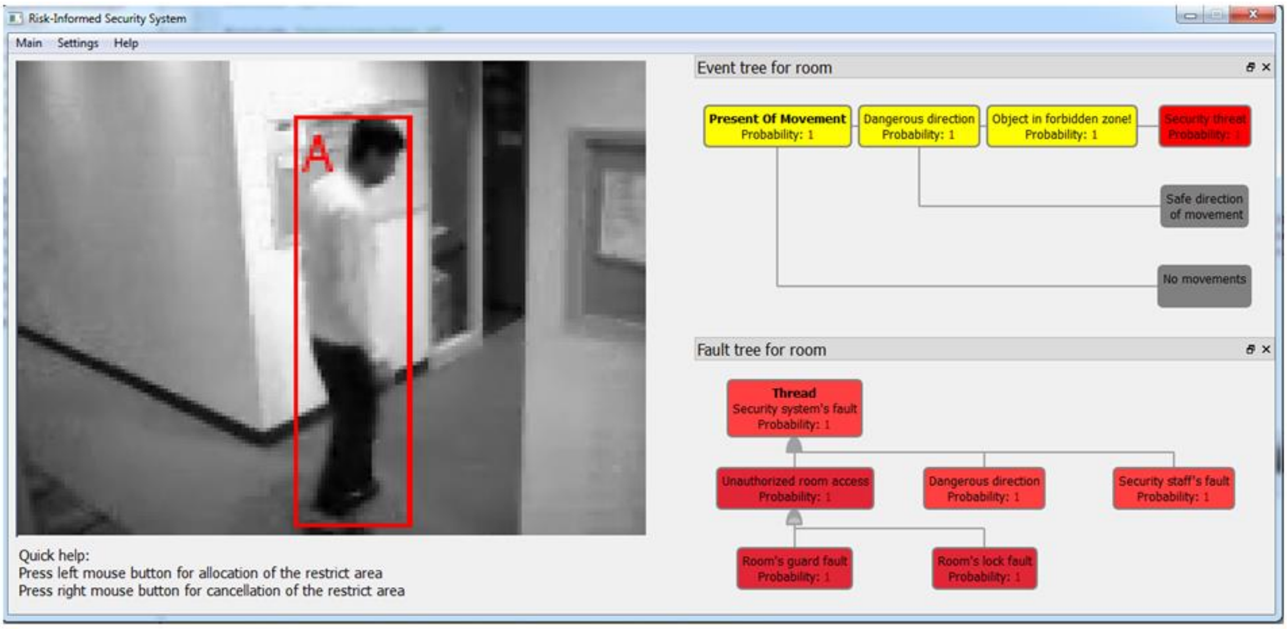
Quick help:
Press left mouse button for allocation of the restrict area
Press right mouse button for cancellation of the restrict area

Fig. 4. Program window. The room (real-time picture from the video camera), the «restricted» area in the room, the event tree (top) and the fault tree (bottom)


Risk-Informed Security System
Main Settings Help
B
Event tree for room
Present Of Movement Probability: 1
Dangerous direction Probability: 0.25
Object in forbidden zone! Probability: 0.05
Security threat Probability: 0.0125
Safe direction of movement
No movements
Fault tree for room
Thread Security system's fault Probability: 0.075
Unauthorized room access Probability: 1
Dangerous direction Probability: 0.25
Security staff's fault Probability: 0.3
Room's guard fault Probability: 1
Room's lock fault Probability: 1

Quick help:
Press left mouse button for allocation of the restrict area
Press right mouse button for cancellation of the restrict area

Fig. 5. Intruder detected moving towards restricted area


Risk-Informed Security System
Main Settings Help
A
Event tree for room
Present Of Movement Probability: 1
Dangerous direction Probability: 1
Object in forbidden zone! Probability: 1
Security threat Probability: 1
Safe direction of movement
No movements
Fault tree for room
Thread Security system's fault Probability: 1
Unauthorized room access Probability: 1
Dangerous direction Probability: 1
Security staff's fault Probability: 1
Room's guard fault Probability: 1
Room's lock fault Probability: 1

Quick help:
Press left mouse button for allocation of the restrict area
Press right mouse button for cancellation of the restrict area

Fig. 6. The intruder entered the restricted area. PPS failure

The assessment of the scale of the invasion is characterized by the time spent by intruders in the control zone by television cameras, their tactics of overcoming this zone, time of day, light exposure, etc. Depending on these data, it is possible to select the closest of the intruder's actions available in the database, obtained at the stage of the analysis of effectiveness and modeling, and predict the most likely actions of the intruder, the most likely routes and goals, and, as a result, quickly organize adequate countermeasures.

The time spent by the intruder in the control zone is determined by the camera as the quotient of dividing the length of the controlled zone by the speed of movement:

$$\tau_{nar} = \frac{2 \cdot D \cdot tg\frac{\alpha}{2}}{V_{nar}} \qquad (3)$$

where:

D - distance from the camera to the point of intersection of the intruder's trajectory with the main optical axis of the camera (m);

α - camera viewing angle (degrees);

V_{nar} - intruder speed (m/s).

For television cameras controlling the perimeter of the object, it is assumed that the intruder moves perpendicular to the main optical axis of the camera.

Introducing into the system a module that simulates the actions of the intruder described in the previous chapter. Using this module combined with the methodology for assessing the scale of the invasion will give the operator information about the exact location of the intruder, its number, and also show further possible routes of the intruder, the most probable targets, the most optimal points for deploying the reaction forces, as well as the probability of interception at one or another point, which will allow you to plan further actions depending on the situation.

3. Results

Work with the video stream is implemented using the OpenCV open computer vision library. The program highlights moving objects against a motionless background, and tracks them (tracking an object). In addition, the program works as a motion detector, in case the object is somehow masked, and it is not possible to select it explicitly. In this case, tracking of moving parts is carried out.

This prototype shows the possibilities of using the object's video surveillance system to automate the operator's work: assessing the operational situation, monitoring the level of security and risk level, demonstrating the results of the analysis in real time on the operator's monitor, if available, displaying relevant instructions and recommendations for further actions, depending on setting.

4. Conclusions

Further development of this software product and its integration into existing physical protection systems involves connecting the following functions to the program:

- connection to the information processing system from other PPS elements: motion sensors, infrared sensors, other signal elements.
- integration with the access control and management system - including for tracking the actions of the facility's personnel and identifying an internal violator using his powers to disrupt the facility's operation.

This program also allows with a high degree of reliability (higher than that of a human operator) to estimate the scale of the invasion.

In the future, it is planned to consider the location of CCTV cameras at especially dangerous facilities and make suggestions for improving the layout and the possibility of using images received from them.

5. Acknowledgments

The study was carried out within the framework of grants 17-07-01475, 18-07-01111, 18-07-00909 and 19-07-00455.

6. References:

[1] Oboymov A.S. Safety Analysis of Physical Protection of Potentially Hazardous Objects / M.A. Berberova, R.Sh. Kalmetev, R.T.Islamov, I.A. Kirillov, S.V. Klimenko, D.V. Minaev, A.S. Oboimov, V.P. Petrov // MEDIAS-2011: proceedings of the International Scientific Conference. - Protvino-Moscow: Ed. ICPT, 2011 - p. 114-134.

[2] Bartosh O.V., Izmailov A.V., Litvinenko E.I., Turkin V.M. Methods and algorithms for the analysis of operational actions of security forces at objects such as buildings of complex configuration // Special issues of atomic science and technology. Ser. Security equipment. Scientific and technical Sat - 1978. - Vol. 1 (10). - p. 60-65.

[3] Andronova E. The weakest link in the security system. // Magazine «BDI» No. 2 (53) - 2004.

[4] Development of recommendations for conducting a risk-informed vulnerability analysis and evaluating the effectiveness of the physical protection systems of nuclear hazardous facilities: a research report on reg. No. 2142OT11 // International Nuclear Safety Center - M., 2011. - 61 p.