Issues of Intruder Analytical Model Applicability for Evaluating an Efficiency of Security Systems

Anton V. Bukovetskiy[1], **Vladimir I. Boyko**[2], **Gennady N. Kolpakov**[3], **Michael V. Poner**[4]

[1] Engineer, Federal State Unitary Enterprise «Mining and Chemical Combine», Zheleznogorsk, Krasnoyarsk region, Russia
[2] Full Doctor, Prof., Department of Physical and Power Plants, Institute of Physics and Technology, National Research Tomsk Polytechnic University, Tomsk, Russia
[3] Doctor, Assoc. Prof., Department of Physical and Power Plants, Institute of Physics and Technology, National Research Tomsk Polytechnic University, Tomsk, Russia
[4] Bachelor of Arts, Department of Physical and Power Plants, Institute of Physics and Technology, National Research Tomsk Polytechnic University, Tomsk, Russia

E-mail: antaresbav@tpu.ru

Abstract. Physical protection system (PPS) is created at a nuclear object to prevent unauthorized acts regarding to nuclear materials, nuclear installations, points of storage of nuclear materials and other items under physical protection. The ability of the PPS to prevent unauthorized actions of intruder was adopted as the main criterion for evaluating the efficiency of the physical protection system. The article considers the possibility of creation of the intruder analytical model to determine time indicators of overcoming boundaries of protection of nuclear object by an intruder with set features.

1. Introduction

Physical protection system integrates people, procedures and equipment for the protection of assets or facilities against theft, sabotage or other malevolent attacks. Among critical facilities, nuclear facilities and nuclear weapon sites require the highest level of PPS. Thus, the International Atomic Energy Agency (IAEA) adopted a convention [1] and published documents outlining requirements for physical protection at nuclear facilities [2]. After the September 11, 2001 terrorist attacks in the U.S.A., the international community, including the IAEA, have made substantial efforts to protect nuclear material and nuclear facilities. These efforts include the Nuclear Security Fund established by the IAEA in 2002 and the Global Initiative to Combat Nuclear Terrorism launched by the USA and Russia in 2006.

Principles of physical protection are realized through administrative and technical measures, including physical barriers. The measures for the physical protection of nuclear material in use and storage and during transport, and of nuclear facilities presented herein are recommended for use by States as required in their physical protection systems. These measures are based on the state of the art in physical protection hardware and systems and on the types of nuclear material and nuclear facilities.

Physical protection system consisting of the physical protection personnel, organizational and technical measures and actions carried out by it, as well as complex of the physical protection engineering & technical facilities, should perform the following tasks: prevention of unauthorized

Content from this work may be used under the terms of the Creative Commons Attribution 3.0 licence. Any further distribution of this work must maintain attribution to the author(s) and the title of the work, journal citation and DOI.
Published under licence by IOP Publishing Ltd

actions; prompt detection of unauthorized actions; hindering (slowing down) the intrusion (advancement) of offenders; responding to unauthorized actions of offenders and neutralization of such in order to prevent the unauthorized actions.

The implementation of the basic principles when designing a physical protection system is aimed at achieving the required level of system efficiency, which is determined by its ability to resist unauthorized actions of intruders regarding to physical protection items. A numerical value characterizing the effectiveness of the physical protection system is a system efficiency index. Its value is determined during the assessment of the effectiveness of PPS subject to certain external and internal threats, the list of vulnerabilities and the model of the intruder.

2. Efficiency index

PPS is a complex system, which includes a variety of structural and functional subsystems. One of the basic properties of PPS as an integrated system is ability to work in conditions of uncertainty. The latter leads to the need of defining efficiency index that has stochastic nature.

The ability of the PPS to prevent unauthorized actions of the intruder is taken as the main criterion. The probability of suppression of the intruder action (P_s) is considered as an efficiency index, since the fact of restraint is a random event. In general, the suppression can be considered as a combination of the following events: intruder detection by technical means of PPS, the delay of the intruder in the progress toward goals, reaction and neutralization of the intruder action [3]. In this approach, the probability of suppression of unauthorized actions in relation to items under physical protection can be described by the formula [4]:

$$P_s = P_{dt} P_{dl} P_n \tag{1}$$

- probability of timely detection of unauthorized actions of the intruder (P_{dt}) is determined by the characteristics of detection equipment and capabilities of the security forces; in the first case it can be derived from the detection equipment technical characteristics, in the second – on the basis of available statistics or as a result of simulation;
- the probability of delay and slow progress of the intruder (P_{dl}) represents the quantile of a random variable of time delay, i.e. the probability that the delay t is not less than a predetermined value (t_{dl}):

$$P_{dl} = P(t \geq t_{dl}) \tag{2}$$

The calculation of P_{dl}, as a rule, is carried out using simulation and requires knowledge of time needed for physical barriers overcoming by different types of intruder, who differs in action tactics, special training, level of technical equipment, etc.

- the probability of neutralization of an intruder by the guard forces (P_n) represents the quantile of a random variable generated at the slice implementation of random functions, defined as "neutralization" in a fixed moment of time *t*.

Simulation is commonly used to determine the value of P_n based on special programs.

Currently, the most prevalent approach to evaluate the effectiveness of security systems in models of the functioning of the PPS is the approach which examines possible scenarios of unauthorized actions and routes of intruder to locations of physical protection items in protected areas on the object. Further, the system's ability to counter the actions of intruders on selected routes is assessed.

In this case, the choice of the efficiency index should meet the following requirements [5]:

- representativeness - strict compliance of the indicator to security system goals;
- sensitivity – a sufficient change of the value of efficiency index when changing the most important parameters and initial data describing the system and affecting its effectiveness;
- simplicity – a lack of mathematical difficulties in the calculation of the efficiency index;
- visibility – clear physical meaning of the defined indicator.

The ability of the PPS to prevent unauthorized actions of intruder was adopted as the main criterion for evaluating the effectiveness of the physical protection system. System efficiency is measured by quantitative indicators, reflecting the probability of restraint of the intruder's actions by the security forces, acting on the alarm.

Efficiency index depends on threats, model of the intruder and vulnerabilities that were adopted in the process of analyzing the nuclear object. Following indicators are used to assess the effectiveness of the physical protection system [6]:

- differential efficiency index takes into account the probability of preventive action against the intruder to one target. When considering multiple scenarios of the intruder action against selected targets, the differential indicator of the effectiveness of the physical protection system of this vulnerability is taken equal to the minimum (worst) value among all the considered scenarios. The scenario of the intruder's actions, corresponding to the minimum value of the probability of preventing actions against selected targets, is adopted as the critical;
- integral indicator represents an average efficiency index of physical protection system for nuclear object with regard to the rank of targets importance.

The realized approach involves using the probability of suppressing the actions of the intruders moving along the route, providing the maximum probability of success with minimal time to achieve the goal, as the primary indicator of the effectiveness of physical protection systems [7]. Elements of the route that intruders have to overcome in different ways depending on intruder chosen tactics are engineering tools (i.e. physical barriers), areas of open terrain, the construction elements of buildings, premises and facilities, equipped with means of detection and control. Overcoming each element of the route is characterized by tactics, method, time of intruder movement and the probability of their detection by technical means of physical protection, site personnel, guard forces. Further measures are taken to intercept, block and neutralize intruders.

3. Intruder model

Intruders can be separated into three classes:

- outsiders;
- insiders;
- outsiders in collusion with insiders.

For each class of intruder, the full range of tactics (i.e., deceit, force, stealth, or any combination of these) is considered. Deceit is the attempted defeat of a security system by using false authorization and identification; force is the overt, forcible attempt to overcome a security system; and stealth is the attempt to defeat the detection system and enter the facility covertly. Adversary capabilities include knowledge of the PPS, level of motivation, skills useful in carrying out the attack (e.g., knowledge of the safety systems), the speed with which the attack is carried out, and the ability to carry and use tools and weapons.

Theft and sabotage may be prevented in two ways: by deterring the adversary or by defeating the adversary. Deterrence occurs by implementing a PPS that is seen by potential adversaries as too difficult to defeat; it makes the facility an unattractive target. In addition, legal ramifications associated with attacking a site may deter some adversaries, although not a determined one. The problem with deterrence is that it is impossible (or, at least, extremely difficult) to measure, and therefore, will not be discussed further. Defeating the adversary refers to the actions taken by the protective or response force to prevent an adversary from accomplishing his goal once he actually begins a malevolent action against a facility. There are three major functions that the PPS must perform. These include: detection, delay and response.

The goal of an adversary is to complete a path with the least likelihood of being stopped by the PPS. To achieve this goal, the adversary may attempt to minimize the time required to complete the path. This strategy involves penetrating barriers with little regard to the probability of being detected. If the adversary completes the path before the guards can respond to interrupt his activities, he is successful. Alternatively, the adversary may attempt to minimize detection with little regard to the time required. If the adversary completes the path without being detected, he is successful.

Selection and description of the intruder model is one of the key issues for creating an effective physical protection system, as the characteristics of the intruder determine the shape, the functionality and the structure of the security system. Characteristics and the parameters of an intruder in its mathematical nature can be divided into three groups [5].

Random with a non-stochastic nature. The values of these parameters for the intruder could not be identified in the analysis of preparation for the implementation of the illegal action or by analytical methods described in the formation of an intruder model. An example of such a parameter may be the following: the intruder group size seeking to realize a threat. The common technique of working with these parameters is to assign probabilistic characteristics to these parameters by the using of various techniques. In many cases modification the mathematical nature of the parameters of this group are carried out through the use of one or simultaneously several methods of expert estimations.

Random with a stochastic nature. The values of these parameters can be obtained statistically or with using specialized computer programs, based on a statistical database and implementing special procedures with them. Examples of such characteristics and parameters may be the following: intruder movement speed on the object site, the time of physical barriers overcoming, the chance to trigger the technical means of protection (detection) under different actions of the intruders and many others. The main difficulty when using parameters of this group is the lack of completeness of source data bases. At the same time, obtaining of any individual parameter of the intruder is time consuming and requires a large number of relevant experiments.

Deterministic. The values of these parameters are constant and depending on the accepted limitations of the performed calculations. Examples of such parameters in the particular case may be the rate of fire of weapons, the power of explosives, the number of physical barriers that intruder must overcome when moving towards the location of the physical protection items at the nuclear object. The proportion of deterministic parameters in the totality of characteristics of an intruder model is small.

Unauthorized actions against nuclear materials, nuclear installations and points of storage of nuclear materials are the set of actions aiming to overcome the boundaries of protection, movement in a protected area of a nuclear object in the direction of the physical protection items placement, participation in the armed clash with security forces. In this case, the time required for intruders to perform the task can be divided into time of overcoming the route elements and time of action with the target object. The time required for moving on a site between the selected boundaries of protection is determined by the speed of the intruder, the nature and length of the surmounted site and security forces actions. The value of the detection probability and the delay time at the turn of protection depends on characteristics of the technical means of physical protection and ways of overcoming the boundaries of engineering means. Analysis of the interactions in the system «intruder – PPS» allows to determine intruder general characteristics (technical equipment, level of physical training, group size) and tactics of action (power, covert, deceptive, or mixed) that affect the value of the efficiency index of PPS.

Nowadays, time of physical barriers overcoming is determined by conducting exercises and by the expert way taking into account selected characteristics and parameters of the intruder. The exercise is difficult in organization, time-consuming and lengthy process, requiring usage of large number human and material resources. Thus, obtained data allow covering only a small sample of events with different initial conditions, and data in most cases are random with the stochastic nature. The characteristics may be determined by the laws of random variables distribution or parameters of these laws.

Data obtained by the expert estimates has low reliability and directly depends on the subjective views and competence of the expert. The original data obtained by the expert estimates is recorded in the database as deterministic parameters and weakly depends on the characteristics and parameters of intruder model. In this case, there are difficulties of taking into account the level of skills and abilities of intruder in overcoming physical barriers due to their random nature. Usually there are three conditional levels of skills of the intruder in specialized programs: high, medium, low [8]. Also, features and specifications (material, dimensions, fences, locations of obstacles) of physical barriers cannot be fully taken into account. All this reduces the reliability of results obtained in the evaluation of the effectiveness of the nuclear object physical protection system.

4. Conclusion

Solving practical issues associated with the evaluation of the effectiveness of the nuclear object security system allows making a conclusion about the necessity for determining more accurate time values of overcoming actually installed physical barriers established within the existing security system. The approach allows to apply for this purpose the algorithm describing the motion of the intruder on the territory of the object and overcoming the boundaries of protection, taking into account the equipment, physical and physiological characteristics of the human body and other factors influencing the possibility of performing unauthorized actions. Its use in the definition of the source data to assess the effectiveness of the physical protection system will require the creation of analytical model of intruder actions. Obtained data allow to take into account the internal and external factors of the interactions in the system «intruder – PPS» that provide the maximum security of nuclear materials at the nuclear facility.

References

[1] IAEA, INFCIRC/274 Convention on the Physical Protection of Nuclear Material (1981)

[2] IAEA, INFCIRC/225/rev.4 The Physical Protection of Nulcear Material and Nuclear Facilities (1999); IAEA, TECDOC-967 (2000); IAEA, TECDOC-1276 (2000).

[3] Garcia M L 2001 *The design and evaluation of physical protection systems* (Oxford: Elsevier Butterworth-Heinemann)

[4] Anton V. Bukovetskiy, Boris P. Stepanov, Denis A. Tatarnikov 2016 *Initial Data Forming for Process Simulation in System "Intruder – Physical Protection System"* (Key Engineering Materials) vol 685 (Switzerland: Trans Tech Publications) pp 148-152

[5] Barnard R L 1988 *Intrusion Detection Systems, 2nd ed.* (Boston: Butterworth-Heinemann)

[6] Fischer R J, Halibozek E, Green G 2008 *Introduction to Security, 8th ed.* (Boston: Butterworth-Heinemann)

[7] Fennelly L 2013 *Effective Physical Security,4 ed.* (Boston: Butterworth-Heinemann)

[8] Fischer R J, Halibozek E, Walters D 2013 *Introduction to Security, 9nd ed.* (Boston: Butterworth-Heinemann)