Security management at facilities vulnerable to attack model development

D A Ukraincova¹, V G Burlov¹, D E Sipovich¹, V V Gryzunov¹ and S Y Kapitsyn²

¹ Russian State Hydrometeorological University (RSHU),3 Metallists Av, St. Petersburg, 195027, Russia
² Higher School of Technosphere Safety, Peter the Great St. Petersburg Polytechnic University, Polytechnicheskaya, 29, St. Petersburg 195251, Russia

E-mail: ukraincova2000@yandex.ru

Abstract. The article describes the development of a 'security management at facility vulnerable to attack model'. The result is the creation of a mathematical model of managerial decisions. The concept of synthesis-based management is presented. The approach is based on the resolution of the inverse control problem. It is shown that a human decision lies at the core of security management at vulnerable to attack facilities.

1. Introduction
In modern conditions, ensuring the security of a vulnerable to attack facilities is considered one of the main activities of security officer. There is a large number of facilities falling under the ‘vulnerable to attack’ category in Russia, including nuclear power plant and radiation hazardous facilities, whose operation is guided by special security regulations.

Neglect of security measures at a vulnerable to attack site can lead to serious irreversible consequences. The facility’s level of security is determined based on the probability of prevention of the maximum number of threats in various breach of security scenarios. Graphical representation of the threat model is shown in Figure 1.

The subject of protection is the life and health of nuclear power plant employees, enterprise employees, citizens, as well as the integrity of the on-site assets (including information) and preservation of the facility’s routine mode of operation, especially in case of an important social institution or a facility with high anthropogenic or environmental risks [1].

Figure 1. Threat model
2. Basic information

Problem statement. When building a security system for a vulnerable to attack facility, the following operation models should be considered:

1. Vulnerable facility operation model
2. Security system operation model

Research Problem. To develop the ‘assessment of effectiveness of security measures at a vulnerable facility methodology’, an array of decisions made by the Occupational Safety and Health Manager (hereinafter – OSHM) will be considered since decision constitutes the basis of human activities [2, 3].

To solve the above specified problem, a correlation between the ‘security management at a vulnerable to attack facility models’ and the ‘management decision-making model’ will be established. For the managers of high-security facilities to make viable decisions, a relevant methodology has to be in place.

Enforcement of security at a vulnerable to attack facility is always tied to human decisions made based on the characteristics of the model. An object model is an informative representation of the corresponding object featuring its main properties and characteristics. Therefore, a decision can be presented in a form of a process model where process can be described as an object achieving the intended purpose [4].

For the intended purpose to be fully achieved while complying with the security requirements, it is necessary to develop process models with pre-set properties. In management, decisions are usually generated based on the analysis-based models aimed at solving a direct management problem. However, analysis-based models might not address all the existing conditions. The article presents a synthesis-based management model that factors in all existing conditions. The new approach is based on the inversion of control principle.

A process model can be built only after all its conditions are established, which presents a challenge in case of process models with pre-set conditions [5-6]. Such a limitation, as well as the unavailability of a viable security management methodology, undermines the achievement of the intended purpose [7].

In this article, the management decision is presented in a form of a mathematical model, where:

\[ \Delta t_{MP} \] is an average problem acknowledgment time

\[ \Delta t_{IP} \] - an average problem-solving time

\[ \Delta t_{NP} \] - an average problem identification time.

The above conditions are an integral part of the security management process at high-security facilities where the key characteristic is the time required for the operation of a vulnerable to attack facility (\( T_{TP} \)). A graphical representation of the process is shown in Figure 2 [8].

![Figure 2. Manifestation of the basic elements of a decision-making model](image.png)

Let's analyze the main target processes at a vulnerable to attack facility, where a 'target process’ is an object achieving the intended purpose. The input parameters characteristic of this target process are: \( T_{TP} \) -- an average vulnerable to attack facility officers travel time, \( \Delta t_{MP} \) -- an average time of appearance of a perpetrator, \( \Delta t_{IP} \) -- an average time required to identify the perpetrator using a surveillance system, \( \Delta t_{NP} \) -- an average perpetrator neutralization time.

Synthesis of the ‘security management at a vulnerable to attack facility model’. It is advisable to present the ‘security management at a vulnerable to attack facility model’ in the form of a graph with two states: initial (1) and final (2). The average target task time is set as an average high-security facility officer travel time (\( T_{TP} \)), which can be presented as follows: \( T_{TP} = f_0 (x_1, x_2, ..., x_n) \), where \( x_1, x_2, ..., x_n \) are the high-security facility operation parameters.
Where the average query execution is "\( \zeta^+ = 1 / T_{TP} \)". There is a chance, however, that the query will not be satisfied. This can be described as the frequency of query failure, "\( \zeta^- \)". Operation of a vulnerable to attack facility can be described as the frequency of query execution, or "\( \zeta^+ = 1 / T_{TP} \)". Among the repercussion of perpetrator activities are the threat of sabotage, disasters of technological origin (such as chemical disasters or nuclear explosions) and other risks. Hence the problem: "How to link the process of the vulnerable to attack facility operation with the operation of the security system." We will develop our model within the framework of the natural scientific approach (NSA). NSA is determined by the integration of properties of the human mind, the world and cognition.

The decision-making process involves the setting of a goal, data gathering and processing, generation of a range of solutions, coordination, decision-making and monitoring.

The goal is to cut the time a security office needs to make a decision on how to handle the perpetrator while keeping in focus the logic of the security management operation. To reduce the decision-making time, a system of smart video analytics should be introduced. To implement automatic control, it is necessary to identify the conditions of the process and provide feedback. Process diagram (Figure 4):

3. Results and Discussion
As a result of the synthesis, a ‘security management at facility vulnerable to attack model’ was transformed into a mathematical model.

The alleged threat must be identified when the object of control enters state 3 under the influence of \( \lambda \). It is expected that a security officer will need time \( \Delta t \) to detect a security breach. At this stage, involvement of additional resources required to eliminate the threat is deliberated. Next, the controlled object enters state 4. This is when the security officer acknowledges the threat and decides what resources to involve in order to neutralize it. At the next stage, the threat is neutralized, and the controlled object goes from state 4 to state 2 'problem solved.' At this point, another threat surfaces and has to be analyzed. The process repeats.

To describe the development process in the graph, it is necessary to make assumptions.
1. Human decision-making scheme is considered a form of data management system.
2. Time intervals between problems identification facts are random variables.
3. Facts discovered in time form an arrival close to the Poisson arrival.
4. Time of processing the data on the required characteristic is a random variable.
5. We consider the case, when the time of location of the required characteristics (facts) in the system (person) area is very limited and commensurable with the time required for their identification, as well as for processing the data and taking appropriate actions on these characteristics.
6. The system is prepared for problem identification and elimination.

The transition of the system back to its original state. The frequency of transition from state 1 to state 2 (\( \zeta^- \)) is equivalent to the inverse of the average target task completion time, which depends on the security officer’s response speed. Frequency (\( \xi^- \)) is an average frequency of uncompleted target tasks. Usually this value fluctuates within 0.1%.

Following this logic, the following graph can be built (Figure 5):

![Figure 5. Process of decision-making](image.png)

A model establishing a correlation between these four processes and the facility performance indicator can be developed now. In this case, the facility performance indicator is equivalent to the probability of identification and neutralization of each security threat.

The Kolmogorov equations (1) can be used:

\[
\frac{dP_i(t)}{dt} = \sum_{j=1}^{n} \lambda_{ij}(t) \cdot P_j(t) - \sum_{j=1}^{n} \lambda_{ji}(t) \cdot P_i(t)
\]

where \( i=0,1,2,\ldots,n \).

Nonzero probabilities of occurrence can be calculated by solving a system of linear algebraic equations derived from the Kolmogorov equations, if the derivatives are equal to zero, and the probability functions of states \( P_1(t), \ldots, P_n(t) \) in the right part of the equations pass into the unknown finite probabilities \( P_1, \ldots, P_n \). To find the value of \( P_1, \ldots, P_n \), a normalizing condition is added to the equations:

\[ P_0 + P_1 + \cdots + P_n = 1. \]

For the graph shown in Figure 4, the Kolmogorov equations will look like this (2):

\[
\begin{align*}
\frac{dP_1(t)}{dt} &= -(\xi^+ + \lambda) \cdot P_1(t) + \xi^- \cdot P_2(t) + v_3 \cdot P_4(t) \\
\frac{dP_2(t)}{dt} &= \xi^+ \cdot P_1(t) - \xi^- \cdot P_2(t) + v_4 \cdot P_4(t) \\
\frac{dP_3(t)}{dt} &= \lambda \cdot P_1(t) - v_1 \cdot P_3(t) \\
\frac{dP_4(t)}{dt} &= v_1 \cdot P_3(t) - (v_3 + v_2) \cdot P_4(t)
\end{align*}
\]

Then the nonzero probabilities of occurrence can be calculated by solving a system of linear algebraic equations (3).

\[
\begin{align*}
0 &= -(\xi^+ + \lambda) \cdot P_1 + \xi^- \cdot P_2 + v_3 \cdot P_4 \\
0 &= \xi^+ \cdot P_1 - \xi^- \cdot P_2 + v_4 \cdot P_4 \\
0 &= \lambda \cdot P_1 - v_1 \cdot P_3 \\
1 &= P_1 + P_2 + P_3 + P_4
\end{align*}
\]

The system solution will look like this (4):

\[
\begin{align*}
P_1 &= \frac{v_1 \cdot v_2 \cdot \xi^- + v_4 \cdot v_3 \cdot \xi^-}{\lambda \cdot v_1 \cdot v_2 + \lambda \cdot v_1 \cdot \xi^- + \lambda \cdot v_2 \cdot \xi^- + v_3 \cdot v_2 \cdot \xi^- + v_1 \cdot v_2 \cdot \xi^+ + v_4 \cdot v_2 \cdot \xi^+} \\
P_2 &= \frac{\lambda \cdot v_1 \cdot v_2 + v_1 \cdot v_3 \cdot \xi^- + v_4 \cdot v_3 \cdot \xi^-}{\lambda \cdot v_1 \cdot v_2 + \lambda \cdot v_1 \cdot \xi^- + \lambda \cdot v_2 \cdot \xi^- + v_3 \cdot v_2 \cdot \xi^- + v_1 \cdot v_2 \cdot \xi^+ + v_4 \cdot v_2 \cdot \xi^+}
\end{align*}
\]
\[ P_3 = \frac{\lambda * v_1 * \xi^- + \lambda * v_3 * \xi^-}{\lambda * v_1 * v_2 + \lambda * v_1 * \xi^- + \lambda * v_2 * \xi^- + v_1 * v_2 * \xi^+ + v_1 * v_2 * \xi^-} \]

\[ P_4 = \frac{\lambda * v_1 * v_2 + \lambda * v_2 * \xi^- + v_2 * \xi^+ + v_1 * v_2 * \xi^-}{\lambda * v_1 * v_2 + \lambda * v_2 * \xi^- + \lambda * v_2 * \xi^- + v_1 * v_2 * \xi^+ + v_1 * v_2 * \xi^-} \]

The probability of detecting and neutralizing a capacity problem is determined by the following correlation (4):

\[ P_2 = \frac{\lambda * v_1 * v_2 + v_1 * v_2 * \xi^+ + v_3}{\lambda * v_1 * v_2 + \lambda * v_1 * \xi^- + \lambda * v_2 * \xi^- + v_1 * v_2 * \xi^+ + v_1 * v_2 * \xi^-} \]

Three parameters are present in this relation. Thus, we have established an analytical dependence of the generalized characteristics of the security breach occurrence (\( \Delta t_{MP} \)), acknowledgment (\( \Delta t_{IP} \)) and neutralization (\( \Delta t_{NP} \)) [9].

4. Conclusion.

Application of this solution to synthesis-based modeling opens a way to the development of a system of security management at a high-secure facility with the required performance efficiency. The key advantage of such a system is that it is void of the major pitfall -- discrepancy between the OSHM's expectations and results [10]. This solution allows to evaluate any decision from the perspective of time and resource costs, as well as to establish a clear scientifically based relationship between the decision and the result.

This model can be built for a range of different states, including a threat to an economic entity, law enforcement agencies, as well as to the life and health of facility employees. In addition, the model allows to consider different threat origins. For example, errors of the security system development, automated image evaluation failures, human factor or deliberate violation of the site access policy, etc.

References

[1] Lazorkin V I., Mikhailin A I and Silnikov M V 2015 Optimization of measures to ensure the survivability of objects // Questions of defense equipment. Ser. 16. Technical means of countering terrorism. 3-4, pp. 3-10

[2] Anokhin P K., System mechanisms of higher nervous activity. The science. Moscow. p 453

[3] Burlov V G 2018 The methodological basis for solving the problems of the information warfare and security protection. // 13th International Conference on Cyber Warfare & Security ICCWS 2018 8-9 March 2018 National Defense University, Washington DC, USA pp 64-74

[4] Burlov V G 2007 Fundamentals of modeling socio-economic and political processes (methodology, methods). Saint Petersburg: SPbGPU publishing house. p. 265

[5] Tsvetkov V Y and Matchin V T. Aggregation of information models Slavic forum. 2(6), pp 77-81

[6] Goode H H Machol R E 1957 System Engineering: An Introduction to the Design of Large-Scale Systems. McGraw-Hill Book Co. New York, pp. 551

[7] Burlov V G, Popov N N and Garcia Escalona H A 2018 Managing the process of using the space geoinformation system in the interests of ensuring the environmental safety of the region //Scientific notes of RSHU 50. Scientific and theoretical journal. - SPb: RSHU. p 226

[8] Burlov V G , Grobitski A M and Grobistskaya A M 2016 Construction management in terms of indicator of the successfully fulfilled production task. Magazine of Civil Engineering, 63(3), pp. 68-71

[9] Burlov V, Andreev A, Gomazov F and Somga-Bichoga N 2018 System integration of

[10] security maintenance processes in knowledge management. Proceedings of the European

[11] Conference on Knowledge Management, ECKM pp. 112-122

[12] Burlov V, Andreev A and Gomazov F 2018 Development of a model for the management of

[13] environmental safety of the region, taking into account of the GIS capacity. MATEC Web of

[14] Conferences 193, 02038