Countering threats to quality of life

Dmitry Golovin[1], *Antonina* Deniskina[1], *Irina* Pocebneva[2*], and *Violetta* Polity[3]

[1] Moscow Aviation Institute (National Research University), Moscow, Russia
[2] Voronezh State Technical University, Russia
[3]Moscow State University of Civil Engineering, Yaroslavskoe sh., 26, 129337, Moscow, Russia

Abstract. The article considers the use of quality management methods for the safety of industrial, transport and municipal facilities in the face of modern challenges: international strategic instability, hybrid war and the coronavirus pandemic.

1 Introduction

The National Security Strategy of the Russian Federation, as one of the priority areas for the development of our state, notes "improving the quality of life of citizens by ensuring ... the availability of social, engineering and transport infrastructure ... protecting the population and territories from natural and man-made emergencies ... updating the fleet of technological equipment and production technologies at potentially hazardous facilities and public life support facilities, developing a system for monitoring and predicting emergency situations ... developing a system for taking preventive measures to reduce the risk of emergencies and taking preventive measures ... "[1]. This requires the introduction of new methods of system analysis and counteraction to risks and threats. Threats are of a natural, man-made and sociogenic nature, and according to the degree of probability of committing, they are divided into potential, immediate and direct. Currently, regulatory documents regulate the process of protecting an object from the most probable destructive impact of 20 factors of various nature. These factors can be divided into 5 groups: natural and man-made factors, acts of unlawful interference, human factor, safety culture. An act of unlawful interference (AIA) is an unlawful action (inaction), including a terrorist act, threatening the safe operation of an object, causing harm to human life and health, material damage, or creating a threat of such consequences, implemented by external or internal violators. Internal violators are the disloyal 6% of employees who are accomplices and direct participants in the AIA or contribute to its implementation by their inaction. The goals of the ANV, carried out to determine vulnerability, are objects of industry, transport, and urban infrastructure [2]. The strategy and tactics of the ANV are being improved, they are disguised as natural and man-made factors. The transport complex is the most protected, but even there new threats are possible [3]. Conducting operations to destabilize the situation is characterized as a "hybrid war". It has become a reality and is being conducted not from the borders of the state, but in cities, at strategically and critically important facilities. Hybrid warfare is a set of ANV, including terrorist attacks carried out by external

* Corresponding author: ipocebneva@vgasu.vrn.ru

and internal violators, implementing various types of threats, scenarios, technologies, engineering and technical means. Often this is a process of unauthorized activity in the facility's infrastructure, remotely controlled via the Internet in real time. ANV in the form of threats are more effective in obtaining the greatest publicity in order to escalate tension [4]. The moment of transition to active operations remains hidden, which makes it difficult to warn of the outbreak of war in a timely manner.

Therefore, in the context of a hybrid war, the basis for ensuring security is the management of resilience [5], the ability of the system to purposefully maintain the functions, structure, control, and smooth out short-term impacts of AEs, including terrorist attacks, recover after them, and adapt through modernization to the consequences of emergencies. The main characteristic of the stability of the system is the time it takes to reach the limit state, the increase of which helps to reduce the risk of developing emergencies. Resilience is determined by an integrated understanding of the situation emerging as a result of the NIA, the vulnerabilities of the system (identified as a result of the vulnerability assessment), the available adaptation resources of the system and its environment. Resilience management focuses on resilience optimization, on risk-informed management of vulnerabilities and available adaptive capabilities, which are determined by the constraints and properties of the system's physical infrastructure. "Resilience Management" does not replace, but expands "risk management" with a more detailed and complete account of organizational, economic realities and subsystem vulnerabilities [6].

Security, like security and resilience, is a qualitative, not a quantitative category. Therefore, it is necessary to apply the quality management apparatus to the management of the security level, operating with quality categories [7]. When developing the concept of safety quality management, the provisions of Total Quality Management [8] should be used, which are an organization philosophy based on the pursuit of quality and management practices leading to total quality. Accordingly, the quality of security is the essence of the object. Therefore, its safety is not a function of a separate system, but the ability of the object as a whole to work stably under normal conditions and under conditions of various types of destructive influences [9]. Safety quality management is a fundamentally new approach to managing an object, aimed at compliance with the normative level of its safety (safety quality of the object), based on the participation of all the personnel of the object and the use of special engineering and technical systems, hardware and software systems, aimed at achieving success through satisfaction of regulatory requirements and benefits for the employees of the facility and for society as a whole [10]. In conditions of a real threat, it is especially important to improve measures to ensure the safety of facilities. At the same time, the concept of mobilization is changing, which becomes a set of measures to concentrate and bring the available forces, resources and means into an active state due to emergency circumstances in the country (hybrid war) or in the world (coronovirus pandemic, trade war, economic crisis, countering Islamic non-governmental and terrorist organizations).

2 Model and method

To solve these problems, quality management is used in the development of complex engineering, technical and organizational measures. Safety quality management is an operational activity carried out by the management and personnel of the facility to ensure the regulatory level of safety quality by performing planning and control, information services, developing and implementing measures, making decisions on the quality of their execution. Safety quality control is understood as a system of measures that solves the problem of object safety quality, the cost of its implementation and maintenance, taking

into account requirements and capabilities. The safety quality of an object is not considered at the final stage, but at each stage of its creation and operation [11].

The choice of safety quality management methods and the search for their effective combination has a direct impact on the mobilization of the human factor. In practice, security is implemented with the help of security systems, the stages of development of which are presented in Table.1.

Table 1. Stages of development of security systems.

Stages of development of security systems	Functions performed
Autonomous security systems	A set of technical solutions and tools
Integrated (complex) security systems	Centralized data processing
PSIM security information management systems - hardware and software systems that integrate unrelated applications and security devices to manage them through a single user interface	Incident Definition Mechanism Incident Response Scenario Management Real-time alert and reporting Managing an object or a group of objects

The concept of quality in this case applies not only to the final product (security equipment) or service, but also to every process, task, activity and decision taken on the site. General requirement: quality must be internal and exist in everything that is done on its territory. At the same time, in order to prevent and localize the consequences of UA, it is proposed to use as a basis the “Swiss cheese” model of James Reason (Fig. 1), which is used in the field of risk management, which describes errors leading to disaster and is designed to assess risks and understand why Emergency.

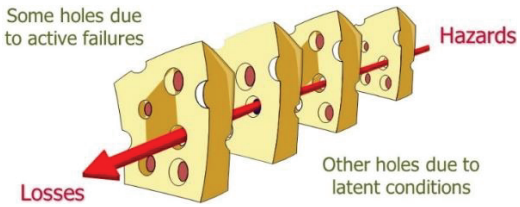

Fig. 1. Swiss cheese model by James Reason.

Each hole in a slice is a separate mistake in creating a security system. There are many such “holes” in any security system at every level, they are located in different places and have different degrees of potential destructiveness. However, the next slice level, in which there is no problem in the same place, protects the entire security system from disaster. Problems begin when there is an error at different levels of the security system in the same area - that is, when the "hole" goes deep, through all the slices along the trajectory of a possible incident. The next layer (element of the security system), which should have worked as a protective barrier, has the same weak point as the next one, and thus, failure in the case of ANV becomes more and more likely [12]. An assessment of the vulnerability of an object, during which such “holes” are discovered, shows that not all mistakes are made due to inattention or inaction (assisting the intruder) and sometimes it is more correct to blame the system than people. The basis of Reason's concept is the allocation of: management problems, insufficient control, prerequisites for unsafe actions and unsafe actions themselves. Management problems are management decisions that lead to disaster. Insufficient level of object security is the lack of systematic control. The prerequisites for unsafe actions and the unsafe actions themselves are the result of a low safety culture of personnel. Reason's model recognizes that there are many conditions that generate errors or violations that affect the individual or collective performance of personnel and members of the security forces. The Reason model allows you to identify barriers to ensuring a regulatory level of safety and act as shown in Figure 2.

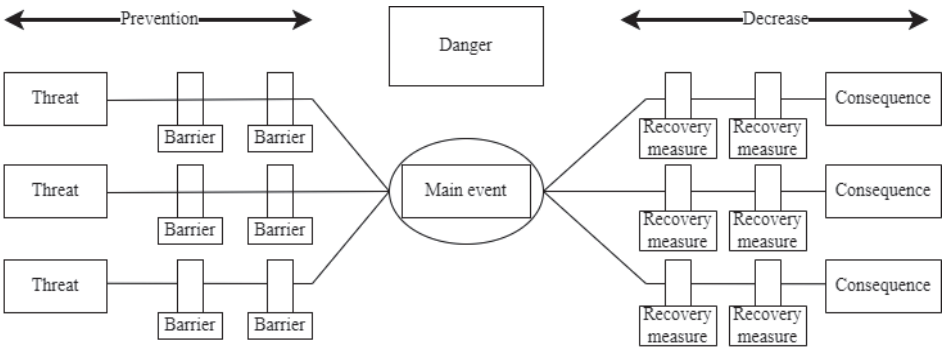

Fig. 2. ANV counter model.

Ensuring the quality of safety is the locomotive that moves the other subsystems of the facility, makes them raise the level of their quality. Given the definition and function of the important safety elements and their associated activities and tasks, the relationship between safety and quality in the operation of an entity becomes apparent. If the quality of important safety elements is questionable due to poor design, the probability of an accident during an emergency shutdown is higher, which jeopardizes the human life of the facility personnel and local residents, the integrity of assets. This means that risk mitigation measures have been in vain. The management of subjects and objects focuses on safety, not realizing its relationship with quality (Fig. 3), and quality refers to everything that the subject and object does or does not do. The question arises: what should come first in order to ensure the safety of an object - quality or safety? The answer is simple. Without the inclusion of work on the formation and implementation of quality management in everything that is done on the territory of the facility and, first of all, safety quality, the processes will not be safe for the facility personnel and local residents, the integrity of equipment and systems will be questionable, and the processes will be unstable [13].

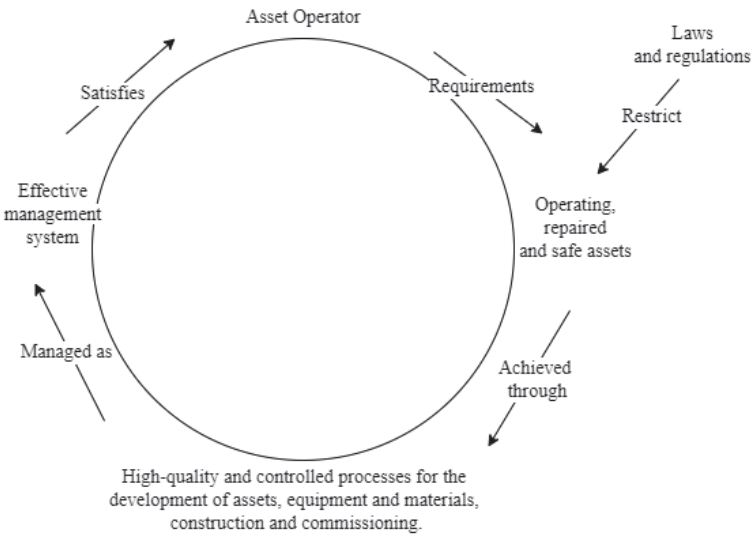

Fig. 3. Relationship between quality and facility safety management systems.

An analysis of the implementation of regulatory safety requirements shows that, first of all, security systems created with the help of safety quality management should be equipped with objects of those industries and transport that have a regulatory framework - where

activities are tightly controlled by government agencies. The regulatory framework for solving security problems has been formed most fully in accordance with the Federal Law-16 dated February 9, 2007 "On transport security", Federal Law-256 dated July 21, 2011 "On the safety of fuel and energy facilities", RP RF N 2446-r dated December 03, 2014 " On approval of the Concept for the construction and development of the AIC "Safe City", RF GD No. 272 dated March 25, 2015 "On approval of the requirements for anti-terrorist protection of places of mass stay of people and objects (territories) subject to mandatory protection by the police, and the forms of safety passports for such places and objects (territories)". The most effective security systems will be implemented at those facilities that are controlled by these regulatory documents, and even better, several of them[14]. Clusters that unite objects of all directions are objects integrating various types of transport, fuel and energy complex, urban transport interchange hubs.The mass construction of the same type of objects allows you to create a line of security systems based on yu on a modular principle with a limited type, to create a program for their creation, optimized at all stages of the life cycle, taking into account the basic provisions of safety quality management and significantly reduce the cost. Such security systems take into account departmental requirements for zoning, allocation of critical elements, information security and cybersecurity [15].

3 Research and results

An analysis of the overall quality factors makes it possible to formulate the basic principles of facility safety quality management, and a systematic approach to determine effective feedback from the facility management for the formation of strategic plans and safety quality plans integrated into them. The introduction of procedures to improve the quality of safety requires a fundamental change in the safety culture, especially for critical elements of facilities, on which the regular functioning of the entire facility depends. Improving the efficiency of the implementation of security systems is achieved by creating a methodology for the synthesis of multi-level security systems, taking into account quality indicators [16]. The main stages of work are shown in Fig. 4.

To ensure the safety of high-risk objects, artificial intelligence is used to manage data exchange, a mechanism for scenario response to events and situation management, which makes it possible to create a system consisting of intelligent subsystems (agents) that solve parts of a common task. Such a multi-agent system is a distributed solution system that organizes the effective interaction of agents and the distribution of tasks based on their capabilities, which leads to resonant, synergistic effects [17]. The work is based on machine learning in expert systems using parallel computing technologies, open distributed processing, security and mobility of agents, network computer programming technologies. The integration of a multi-agent system provides new features and a high level of counteraction to the components of a hybrid war. Thus, the use of safety quality management methods and the methodology of Total Quality Management to optimize the level of safety allows you to get a synergistic effect. This work is carried out systematically, taking into account the contribution of a particular type of security to integrated security, taking into account the overall synergistic effect [18].

In parallel with the development of security systems, training of personnel to maintain these systems, expert groups for preparing scenarios and developing solutions, and training of security forces should be carried out. With such an integrated approach, it is possible to effectively ensure security, but it determines a clear delineation of the functions and powers of the subjects, and the development of methods of public-private partnership (PPP) in the field of security [19]. PPP acts as a powerful factor in strengthening the counteraction

against anti-nuclear activity and terrorism in the face of the emergence of new types of threats [20].

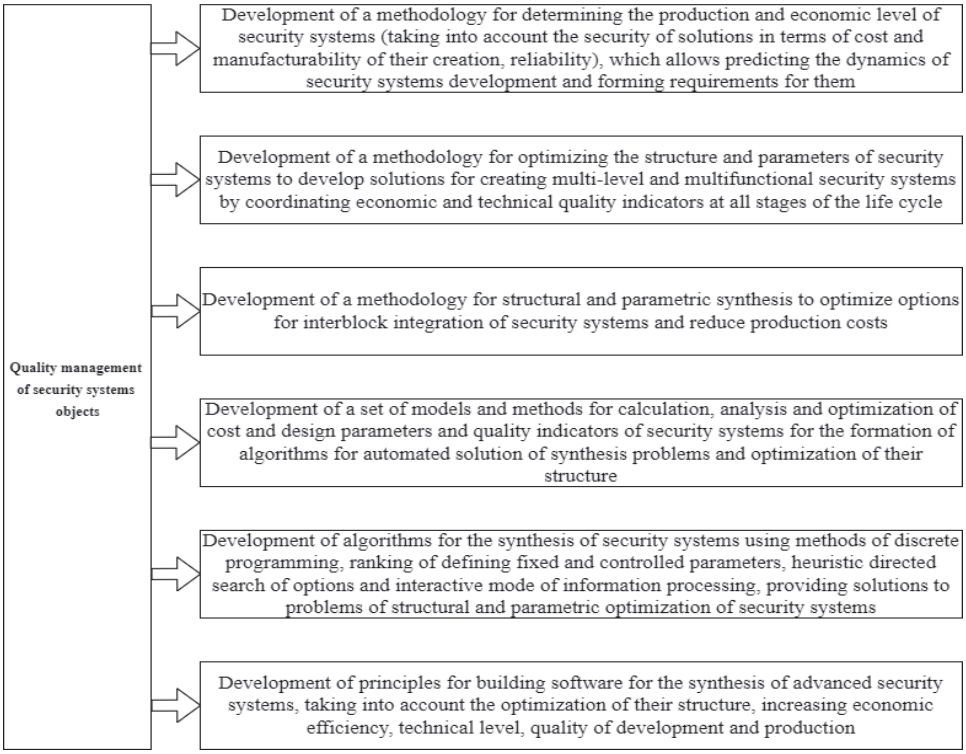

Fig. 4. Quality management of facility security systems.

4 Conclusion

The creation of security systems based on security quality management should be carried out in conjunction with the use of best practices, best available technologies (BAT), energy-saving technologies. These works should be carried out with the support of insurance companies directly interested in the effectiveness of the protection of the insurance object. In this case, the facility's security system can be turned from a planned unprofitable system into a cost-effective system. Purposeful operational formation of security quality control, increasing the level of security culture allow us to effectively solve the pressing security problems facing our state in a crisis, sanctions and hybrid war.

References

1. R. Galanti, M. de Leoni, N. Navarin, A. Marazzi, Expert Systems with Applications **213** (2023) doi:10.1016/j.eswa.2022.119173
2. M. Hasnain, I. Ghani, S.R. Jeong, M.F. Pasha, S. Usman, A. Abbas, Computers, Materials and Continua **74(1)**, 783-799 (2023) doi:10.32604/cmc.2023.030162
3. D. Ivanković, T. Jansen, E. Barbazza, Ó.B. Fernandes, N. Klazinga, D. Kringos, Health Research Policy and Systems **21(1)** (2023) doi:10.1186/s12961-022-00931-1

4. P. Wang, Y. Guo, Z. Xu, W. Wang, D. Chen, Mechanical Systems and Signal Processing **187** (2023) doi:10.1016/j.ymssp.2022.109956
5. X. Huang, J. Zhan, Z. Xu, H. Fujita, Expert Systems with Applications **214** (2023) doi:10.1016/j.eswa.2022.119144
6. R. Togai, T. Tsunakawa, M. Nishida, M. Nishimura, IAES International Journal of Artificial Intelligence **12(1)**, 12-22 (2023) doi:10.11591/ijai.v12i1.pp12-22
7. A. Mishra, A. Shukla, N.P. Rana, W.L. Currie, Y.K. Dwivedi, International Journal of Information Management **68** (2023) doi:10.1016/j.ijinfomgt.2022.102571
8. J. Li, Y. Feng, International Journal of Approximate Reasoning **152**, 310-324 (2023) doi:10.1016/j.ijar.2022.10.020
9. S. Serebryansky, B. Safoklov, I. Pocebneva, A. Kolosov, Model of information support of the quality management system (2022) doi:10.1007/978-3-030-80946-1_90
10. A. Kadykova, A. Smolyaninov, A. Kolosov, I. Pocebneva, Methodology for assessing the quality of services based on the discrepancy model (2022) doi:10.1007/978-3-030-80946-1_89
11. E. Ermolaeva, I. Fateeva, A. Bakhmetyev, N. Kolosova, A. Orlov, Transportation Research Procedia **63**, 1569-1574 (2022) doi:10.1016/j.trpro.2022.06.169
12. I. Novikov, A. Deniskina, V. Abyzov, O. Papelniuk, Transportation Research Procedia 63, 1601-1607 (2022) doi:10.1016/j.trpro.2022.06.174
13. M. Akhmatova, A. Deniskina, D. Akhmatova, L. Prykina, Transportation Research Procedia **63**, 1512-1520 (2022) doi:10.1016/j.trpro.2022.06.163
14. B. Safoklov, D. Prokopenko, Y. Deniskin, M. Kostyshak, Transportation Research Procedia **63**, 1534-1543 (2022) doi:10.1016/j.trpro.2022.06.165
15. A. Korchagin, Y. Deniskin, I. Pocebneva, O. Vasilyeva, Transportation Research Procedia **63**, 1521-1533 (2022) doi:10.1016/j.trpro.2022.06.164
16. K. Gumba, S. Uvarova, S. Belyaeva, V. Vlasenko, E3S Web of Conferences **244** (2021) doi:10.1051/e3sconf/202124410011
17. E. Avdeeva, T. Davydova, O. Belyantseva, S. Belyaeva, E3S Web of Conferences **244** (2021) doi:10.1051/e3sconf/202124411003
18. O.S. Dolgov, B.B. Safoklov, D.S. Shavelkin, 2022 International Conference on Industrial Engineering, Applications and Manufacturing, ICIEAM 2022, 659-663 (2022) doi:10.1109/ICIEAM54945.2022.9787125
19. E.N. Ermolaeva, Russian Engineering Research **41(10)**, 980-982 (2021) doi:10.3103/S1068798X21100075
20. K. Hou, P. Tang, Z. Liu, Z. Dong, Energy Reports **9**, 829-836 (2023) doi:10.1016/j.egyr.2022.11.075