VI International Forum on Teacher Education

Technologies for the Formation of Personal-Activity Thinking and Self-Organization Skills in Pedagogical Practice

Elena V. Muraveva (a), Svetlana G. Dobrotvorskaya (b), Evgeniya A.Knyazkina[*] (c)

(a), (c) Kazan National Research Technical University named after A. N. Tupolev - KAI, 420111, Kazan (Russia), 10 Karl Marx Street, elena-kzn@mail.ru;knazek1@mail.ru
(b) Kazan Federal University, 420111, Kazan (Russia), 1 Martina Mezhlauka Street, sveta_dobro@mail.ru

Abstract

This article is dedicated to representation and embodying of the main idea of «risk-based thinking», as well as to justify the use of integrated system and competency-based approaches in the formation of this concept as a professional competence for students studying in the field of «Technosphere Safety». For this study, we proposed the wording "risk-based thinking". The criteria for developed risk-oriented thinking were identified.
The systemic and knowledge-based approaches to the development of higher education programs in the direction of «Technosphere security» were used as a theoretical framework of the study. The organization of studying of problem included three stages. The experiment was run in KNRTU named after A.N. Tupolev.
The study concludes that risk thinking is based on understanding and analyzing decision-making processes when operating complex technical methods based on risk-oriented activities. Also, it was established that risk activity is the cognitive activity of a person, which comes down to analyzing and understanding of decision-making processes in the operation of complex technical methods.

Keywords: role-playing games, risk thinking, disaster risk reduction, and active methods situational risk.

---

[*] Corresponding author. E-mail: knazek1@mail.ru

Introduction

Over the past half-century, there has been a rapid development of technologies that have made it possible to tame nuclear energy, drill multi-kilometer wells for oil production, and create a global financial system. At the same time, the complexity and interconnectedness of technical systems have increased, which has led to the fact that they have become more vulnerable. Failures in the operation of technical systems can lead to irreparable damage to life, environment, and economics. (Romanovsky, 2010).

However, against the background of ongoing processes, contradiction between the need to exercise highly qualified specialists in the field of man-made risk management and the lack of prescribed standards for their training is becoming more and more obvious. In addition, the issue of understanding the essence of risk-based thinking and the methodology for its formation has not been fully developed yet (Aven & Reniers, 2013).

The main goal of this study was to substantiate the notion of a risk-based approach for its further application in educational activities in the field of «Technosphere security» in the development of competencies established by the Federal standard.

Currently, in the Russian Federation, specialists (bachelors, masters and postgraduates) are trained in the field of human security in order to create a technosphere that is comfortable for human life and activity, and to minimize the technogenic impact on the environment. For example, the order of the Ministry of education and science of Russia dated March 24, 2016 No. 246 "on approval of the Federal state educational standard of higher education in the field of personnel training dated 20.03.01 "Technosphere security (bachelor's level)" defines the requirements for the formation of competencies for risk management specialists. In particular, in addition to professional competencies that set requirements for abilities in future professional activities (mastering methods, technologies, approaches, etc.), General cultural competencies are also proposed. One of these competencies is to have a safety culture and a risk-oriented mindset, while environmental safety issues are considered top priorities in a person's life and work (OK-7) (Shavalieva et al., 2013; Muraveva, 2014).

The concept of a risk-based approach was introduced by the national standard of the Russian Federation "GOST R ISO 9001-2015 quality management. System. Requirements". At the same time, the standard (Schon, 1983), refers to the need for such an approach to achieve the effectiveness of the quality management system. To meet the requirements of this standard, the organization must plan and implement actions related to risks and opportunities to prevent them (Schon, 1983). If we understand person`s

cognition process as a subjective way of reflection of reality, then, in fact, the concept of a risk-oriented approach to the formation of thinking comes down to comprehension the processes that can provoke the implementation of risks in this activity for employees in the organization (Grote, 2012). In addition, at the moment, in the field of ensuring the safety of the population from various threats, the efforts of specialists are focused on the following areas: identification of hazards, risk assessment, and forecasting of emergency situations; development of measures for risk reduction and effective protection of the population and territories; state regulation in the field of risk reduction, as well as improvement and development of emergency response forces and means. Specialists with formed risk-oriented thinking are necessary for the implementation of all these areas (Berkimbaev, Akeshova, Meirbekov, & Meirbekova, 2013; Wua, Daia, Leeb, & Yan, 2013).

Purpose and tasks of the research

The purpose of the research is to formulate and embody the concept of «risk-based thinking», as well as to justify the use of integrated system and competency-based approaches in the formation of this concept as a professional competence for students studying in the field of "Technosphere Safety".

Literature review

The considered standard in the field of «Technosphere safety» (Schon, 1983) includes certain types of professional activities for which graduates are prepared (design, service and operational, organizational and management, expert, supervisory, inspection and audit, research and development activities). The educational program can be oriented both to the research and/or pedagogical type(s) of professional activity, and to the practical, applied type(s) of professional activity. Therefore, there is an absolute necessity to understand the core and content of the professional activity of the graduate in the specialty «Technosphere security», i.e. it is necessary to characterize the subject area being studied. Given that, people with higher technical education are engaged in providing technosphere security and their way of cognition can be determined as «technical»… «Technical», professional training should be based on understanding the operation of technical systems as the most complex objects. For this purpose, in our view, one of the most effective approaches will be the approach using the Perrow's concept.

According to Perrow's concept (Romanovsky, 2010), systems are exposed to risks under the influence of two factors. If we accept these factors, we can determine which system is most vulnerable.

The first factor concerns how different parts of the system interact with each other. Some systems are linear: it's like an Assembly line in a car factory, where everything happens in an easily predictable sequence. Each machine goes from the first Assembly point to the second, then to the third, and so on. at

each of these stages, different parts are installed on it. Therefore, if a system failure occurs, the person responsible for the pipeline operation can immediately see at what stage the problem occurs.

The consequences are also obvious: machines may not reach the next stage of Assembly and accumulate where the failure occurred.

Other systems, such as nuclear power plants, are more complex: parts of them are more likely to engage in hidden or unexpected interactions. Complex systems are more like a thin network than an Assembly line. Many of their parts are closely related and can easily influence each other. Even explicitly incompatible parts can be indirectly linked, and some subsystems interact with many parts of the main system. Therefore, when something goes wrong, problems "jump out" everywhere and it is difficult to make a clear conclusion about what is happening.

Complicating the situation is the fact that most of the work of complex systems goes unnoticed by the naked eye. Imagine that you are walking along a path that descends along the edge of a cliff. You are only a few steps from the abyss but your senses protect you. Your head and eyes are focused on making sure you don't stumble or get too close to the edge.

 When forced to follow the same route, looking through binoculars one cannot see the whole picture. Instead, one will have to navigate through narrow and not always clear areas of visibility, i.e. look where a left foot should go. Then, move the binoculars to determine the distance to the edge of the road. Then, be ready to move your right foot and look at the track again. Imagine that you are running along the path, relying only on episodic and fuzzy images. This is what we do when we try to manage a complex system.

The difference between linear and complex systems is in their maintenance. The Assembly line at the automobile plant is not quite simple, but its parts, nevertheless, interact with each other mainly linearly and clearly or take the dam. They represent the pinnacle of technology, but they are not complex.

In the case of complex systems, we cannot get inside to see what's going on "in the monster's belly". When evaluating most situations, we have to rely on indirect indicators. For example, at a nuclear power plant, we can't send someone to see what is happening in the core of an active reactor. We need to put the whole picture together in small pieces – pressure sensor readings, water measurements.

Methodology

Speaking about professional education and the formation of risk-based thinking in the development of competencies, we can recommend the integration of systemic and competence-based approaches to the development of higher education programs in the direction of "Technosphere security".

Using the system approach, we act in terms of the theory of complex objects, systems that represent a single structure of elements, parts and perform certain functions, and the use of the competence approach allows us to form key and professional competencies, that is, the readiness of a future security specialist who will use the fundamental principles, knowledge, skills and abilities to analyze the dangers inherent in complex technical and technical-social systems.

Experimental base of the study was the KNRTU named after A.N. Tupolev. The research tools are a forum and a school contest.

The problem study was carried out in three phases: at the first phase - a theoretical study of the available methodological approaches to the philosophical, psychological and pedagogical literature, thesis work on the issue, as well as the theory and educational research methodology; highlighted the problem, the purpose and methods of research, drawn up a plan of experimental study. At the second phase, experimental work was carried out; conclusions obtained in the course of experimental work are analyzed, verified and refined. At the third phase, completed experimental work clarified the theoretical and practical conclusions; the results are summarized and classified.

Results

As a result of the analysis, it becomes clear that none of the systems completely fit into the categories invented by Perrow but some of them are more complex and tightly related than others. The question arises as to what extent. To understand this, we can present these technical systems as a diagram (Figure 1).

Dams and nuclear power plants at the top of the matrix are tightly interconnected systems, but dams (at least of traditional design) are much less complex. They consist of fewer components and have fewer opportunities for unexpected and often invisible interactions.

If you look at the lower part of the matrix, there are quite primitive from a technical point of view universities and post offices. Actions in them are not regulated by a very strict order and failure in their work will not be critical from the point of view of a threat to the life and health of others.
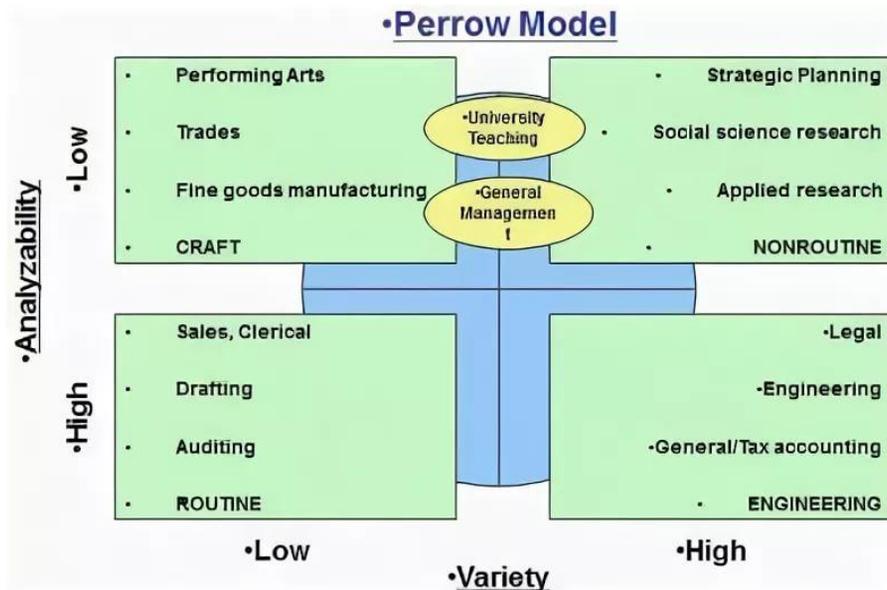
Figure 1. Matrix of Perrow

Of course, post offices are the simplest systems, even compared to universities, where life is regulated by a complex bureaucratic mechanism, where there are many departments, departments, educational divisions, etc. Universities perform various functions: educational, administrative and scientific, etc. All this is a complex, if not technical, but an administrative system. Life at the University is multifaceted and regulated by both administrative acts and self-government bodies, which can lead to some conflict situations. For example, the conclusion of an administration contract with a teacher for only a year can be challenged by the decision of the Academic Council, both the faculty and the University itself, and there are many such examples. However, since the connections in the "University" system are not rigid, it is always possible to maneuver. At the same time, the work of the University is not disrupted, moreover, other faculties may not even know about this problem.

The most dangerous area in the Perrow's matrix is the upper right square. Systems located in it with complex and rigid connections can lead to large-scale disasters. Failures in these systems will apply the "cascade", i.e., quickly and uncontrollably, creating a "Domino effect". Let's remember how the Sayano-Shushenskaya hydroelectric power station collapsed instantly and what catastrophic consequences this accident had. Moreover, as the situation worsens, external manifestations will become more ambiguous. With all the effort, it will be hard to accurately diagnose the problem, and it is also can aggravate it by solving not a primary task that is such, but the one that we think is the most important.

Discussions

Failures spread quickly and uncontrollably. Perrow admits that normal accidents are extremely rare. Most incidents are completely preventable, and the direct reasons for their occurrence are not the complexity or rigidity of the connections. These are usually management errors, ignoring warning signals, problems communicating with people, poor training, and reckless risk taking. However, the Perrow's concept allows us to understand such incidents correctly: these preventable accidents also increase the complexity and rigidity of connections. If this is a complex system, our understanding of how it works and what happens inside it is likely to be incorrect. And, most likely, our errors will intersect in the most confusing way with other failures. The rigid connectivity of the system makes it difficult to counteract the appearance of all new failures (Salmon, Cornelissen, & Trotter, 2012).

Imagine a repairman who accidentally makes a small mistake, such as closing the wrong valve. Many systems quietly tolerate such trivial failures every day. Small failures can cause huge damage under the appropriate conditions. The complexity and close interconnection of systems create dangerous zones in which small errors lead to disasters (Muraveva, 2012).

Our range of actions which can be useful in changing systems is short, but we can change the way we navigate them, as well as the way we think that leads to new options for risk analysis. Often it seems that the cause of an accident or disaster is a technique, but in most cases, a deeper analysis reveals that the person is to blame. Luckily, better part of accidents is predictable, because the immediate causes will not be a difficulty or stiffness of joints, and reckless risk, ignoring the warning signals, problems in communication, low staff training and mistakes in management that could be avoided with proper training.

Conclusion

Therefore, specialists with a high level of security culture and developed risk-thinking should develop and operate complex technical systems.

Using the integration of system and competence approaches, we proposed the formulation of the concept of risk-based thinking as a professional competence for higher education programs in the field of training «Technosphere security». Risk activity is the cognitive activity of a person, which comes down analyzing and understanding of decision-making processes in the operation of complex technical methods. In this case, we can say that risk thinking is thinking that is based on the analyzing and understanding of decision-making processes in the functioning of complex technical methods, based on risk-oriented activities. The criterion for developed risk-based thinking is the ability to analyze the largest number of possible options

per unit of time and make a choice for favorable consequences. (Masalimova, Ikramova, Shaidullina, Gubaidullina, & Apraksina, 2014).

Acknowledgements

References

Aven, T., & Reniers, G. (2013). How to define and interpret a probability in a risk and safety setting. *Safety science*, *51*(1), 223-231.

Berkimbaev, K. M., Akeshova, M. M., Meirbekov, A. T., & Meirbekova, G. P. (2013). Correlation of the traditional approach and information – communicational technologies in training of the future ecologists in Kazakhstan. *Life Science Journal*, *10*(6), 501-507.

Zhang, G., Wua, L., Daia, G., Leeb, S. S. L., & Yan, L. (2013). Landscape ecological approach to the ecological significance of cultural heritage sites. *Life Science Journal*, *10*(2), 1982-1993.

Grote, G. (2012). Safety management in different high-risk domains–all the same?. *Safety Science*, *50*(10), 1983-1992.

Masalimova, A. R., Ikramova, G. D., Shaidullina, A. R., Gubaidullina, G. T., & Apraksina, N. D. (2014). Distant in-company foreign language learning involving university student-tutors. *American Journal of Applied Sciences, 11*, 1123-1127.

Muraveva, E. V. (2014). College Students' Ecological Education as a Strategy of Ecological Crisis Overcoming. *Life Science Journal, 11*(8), 1-15.

Muravyeva, E. V. (2012). Situational component technospheric risks. *Journal of the Samara scientific center of Russian academy of Scienc*e, *1*(3), 43-47.

Romanovsky, V. L. (2010). *Applied technospheric risk. Ecological aspects*. Kazan: RIC School.

Salmon, P. M., Cornelissen, M., & Trotter, M. J. (2012). Systems-based accident analysis methods: a comparison of Accimap, HFACS, and STAMP. *Safety science*, *50*(4), 1158-1170.

Shavalieva, Z. Sh., Ahmuldinova, A. N., Isinbayeva, K. G., Ayapbergenova, G. S., Alibayeva, Zh. E., & Sakenov, D. Zh. (2013). Improvement of quality of vocational training of students (based on courses of humanitarian and ecological cycles). *Life Science Journal, 10*(12), 838-841.

Schon, D. A. (1983). *The Reflective Practitioner.* New York: Basic Books.