ISSN 0147-6882, Scientific and Technical Information Processing, 2021, Vol. 48, No. 2, pp. 71–77. © Allerton Press, Inc., 2021.
Russian Text © The Author(s), 2021, published in Nauchno-Tekhnicheskaya Informatsiya, Seriya 1: Organizatsiya i Metodika Informatsionnoi Raboty, 2021, No. 4, pp. 1–7.

Transformation of Strategic Models for Managing Human Risks of Information Security of an Enterprise as an Imperative of the Digital Industry

L. V. Astakhova*

South Ural State University, Chelyabinsk, Russia

**e-mail: astakhovalv@susu.ru*

Received December 19, 2020

Abstract—This article substantiates the imperatives of transforming the information security (IS) human risk management model at a digital industry enterprise using the theories of strategic management, psychological ownership (involvement), and cultural parameters of human activity. The types of strategies and strategic models of information security culture (ISC) have been substantiated. With the use of sociological research, the dominance in organizations of the ISC defensive strategy was revealed, the pattern of the transition from the defensive to the developing strategic ISC model was revealed, and then the transition to the integrative ISC management strategy, thus combining both strategic models. The concept of the draft Information security culture national standard, which can be the basis for the design and implementation of a standard of the same name for any enterprise, is presented.

Keywords: information security culture, awareness, management, strategies, organization, human risks, trust, involvement, employer, employee

DOI: 10.3103/S0147688221020027

INTRODUCTION

The fact of human dominance in the composition of sources of information security (IS) incidents in organizations of all types of all industries remains unchanged. No matter how rapidly technologies and means of information protection develop, an information system becomes vulnerable if its user is left unattended. Based on the results of an analytical study of the Infowatch company [1], for 4 years in a row, the share of internal leaks in the total number of leaks has remained in the range of 53–61%, that is, more than half of all information leaks recorded in the world are not due to the influence of external hackers, but due to errors or willful actions of employees (including management), owners, and operators of information: "The total amount of data compromised as a result of internal leaks in 2019 amounted to 9.87 billion records. For the first time ever, the volume of records compromised as a result of internal leaks exceeded the same indicator for external leaks: 4.7 billion records." In the context of the COVID-19 coronavirus pandemic, the threats of information impact on employees of organizations working remotely have intensified: the number of phishing sites and mailings on the topic of the virus and related malicious codes has sharply increased; the scale of fraud and misinformation, aimed at exploiting fear or incomplete information about the pandemic, etc., has increased [2]. The strengthening of anthropogenic threats to the information security of an enterprise in the context of a rapidly developing digital industry cannot avoid generating global strategic changes in information security management processes. The purpose of this article was to substantiate the direction and essence of the transformation of the strategic model for managing human threats to the information security of an enterprise.

IS CULTURE STRATEGIES AND MEANS OF THEIR IMPLEMENTATION

World science and practice are intensively studying the problem of threat management in the context of information security culture. In Russia, unfortunately, the attempt to adopt the Fundamentals of State Policy on the Formation of a Culture of Information Security in the Russian Federation document was unsuccessful; its task was to be a strategy to create a culture of safe behavior among Russian citizens when using information technologies, Internet surfing, electronic payments, etc., starting with children and ending with the elderly [3]. Therefore, the entire burden of responsibility for the formation and development of information security culture lies today with the heads of organizations.

The main role of the head of an organization as a subject of the development of information security culture is also due to the dynamics of the cultural parameters of human activity. The fact is that "culture is not a branch of activity that produces its own specific product, but a universal modality that permeates all branches of activity and brings into them the possibility of collectively carrying out this activity or consuming its results, a certain ordering, as well as the symbolism associated with the system value orientations. Culture is a system of relationships between people, contributing to their mutual understanding and joint activities or the consumption of its products" [4]. The cultural parameters of human activity in the modern post-industrial era are: the dominant form of social organization of the subjects of activity (association around common work; professional self-realization as the most effective way of managing human consciousness and behavior), the procedure for its implementation (innovations), and the profile of symbolizing results (modern/archaic dichotomy). With these means this culture regulates the consciousness and behavior of people, keeping them within the framework of the historically formed value orientations in the post-industrial community [4, p. 302]. Unlike socialization, which orients a person in the conditions of life, as determined mainly by utilitarian, pragmatic tasks, inculturation (the process of mastering the norms of social life and culture) orients a person in conditions determined by value attitudes characteristic of a given social environment, historical traditions, mental characteristics, etc. [5, p. 1].

These factors formed the basis for the definition of an organization's information security culture presented in our publications. As a result of the analysis of a large array of foreign articles, we formulated the definition of an organization's information security culture, understanding it as a method of purposeful creative joint activity of managers and employees to ensure and improve the organization's information security level, which is expressed in their values, needs, knowledge, and behavior: (a) in shaping value models of their information interaction as senders and recipients of information; (b) in harmonizing the needs of the employer (in ensuring the organization's information security) and employees (in self-realization and self-development); (c) in the continuous improvement of their knowledge, including awareness of information security; and (d) in the ability of the employer and employees to realize and develop their cultural resources in information behavior in the process of joint professional activity [6, 7]. Obviously, such an interpretation of information security culture is applicable for the most developed, highest forms of its manifestation, which are associated not only with the protection of information resources of the organization and the interests of the employer, but also with the interests of employees, which significantly differs from existing social and professional stereotypes. It is this approach to the concept of IS culture that correlates with the values of modern post-industrial culture and will be used in this article.

Since any organization always has features of the internal and external environment, the problems of independent choice on the grounds of a certain strategy for the development of information security culture are very relevant. However, in the theory of information security, this problem has not been studied and has not yet become the subject of a special study.

According to the classical theory of strategic management, a strategy is the totality of all actions by managers, contributing to the achievement of the organization's goals [8, p. 44]. Consequently, the strategy of information security culture is a generalizing model of actions necessary to achieve the set goals. It is a functional strategy, as it refers to one of the functional areas of the organization's activities: ensuring its information security related to personnel.

The most important requirement for a strategy is its ability to adapt to changing circumstances [8, p. 44]. Therefore, for the study of strategies of culture of information security, we consider a situational approach to be mandatory. It is known that the theory of situations explores the concept of strategy in two dimensions: in statics (as a unity of subjective and objective factors) and in dynamics (as conditionally (conventionally) semantic interaction) [9, pp. 1003–1010]. It is logical to assert that an organization's IS culture strategy is formed by objective and subjective (external and internal), as well as situational, communication, and behavioral factors within the organization and its interaction with the external environment at each current moment of time.

In the theory of strategic management, defensive and offensive strategies of the organization are distinguished [8, p. 249], which differ in their goals and means of implementation. It is logical to argue that the same classification is applicable to information security culture strategies. The choice of a defensive (let us call it defensive) or offensive (let's call it developing) strategy is undoubtedly influenced by objective, external factors: national-cultural, political and legal, economic, socio-cultural, technical, and technological. Thus, the lack of conceptual and regulatory documents on the culture of information security, the crisis state of the economy in Russia, and the budget deficit determine the intuitive choice of a protective strategy.

The defensive strategy of information security culture: the goal of this strategy is to reduce threats to be attacked through the fault of internal users, the ability to transfer their intentional and unintentional attacks to information systems with minimal losses for the organization. At the same time, minimizing human threats to information security is the initial stage in the development of an organization's information security culture. Achievement of its higher level is possible only as a result of the implementation of an offensive strategy.

The offensive (developing) strategy of information security culture: the goal of this strategy is to obtain and develop the competitive advantages of the organization through the formation of human, intellectual, and cultural capital of each employee individually and the organization as a whole, which is the prevention of the human threats to information security.

In criminology, prevention is the earliest, initial stage of preventive activity aimed at preventing an offense. According to experts, prevention should be understood as a process of identifying and eliminating the causes and conditions that contribute to the commission of offenses and warning–prevention of already contemplated and prepared illegal acts [10, p. 45]. Therefore, prevention can be qualified as a protective measure and as a developmental one.

For the first time, the term "prevention" was normatively enshrined in Art. 2 of the Federal Law On the Foundations of the System for the Prevention of Offenses in the Russian Federation[1], according to which "prevention of offenses is a set of measures of a social, legal, organizational, informational and other nature aimed at identifying and eliminating the causes and conditions conducive to the commission of offenses, as well as providing educational influence on persons in order to prevent the commission of offenses or antisocial behavior." An independent type of crime prevention is formed by victimological prevention, which is understood as "purposeful specialized impact on persons with unlawful or immoral behavior, as well as on the factors causing victimization associated with similar behavior. Its object is equally factors and persons whose positive behavior, nevertheless, is a danger for them" [11, p. 241]. The main task of victimological prevention is creating a system of effective protection of a person from potential victimization [12, p. 103]. This is the essence of the developing strategy of information security culture: the creation of a system of effective protection of the organization's employees from potential victimization, which can become a threat to protected information.

Taking into account the classification of prevention according to the objects of impact [12, p. 104], it can be argued that the objects of influence within the framework of the protective strategy of the IS culture are the reasons and conditions for committing offenses, as well as the behavior of persons who are potentially capable of committing or are already committing an offense; within the developmental strategy, this is factors that influence the formation and development of personality. Therefore, the disadvantage of a protective strategy is that each employee of the organization is considered as a potential violator, regardless of his personal qualities. The dignity that arises in the development strategy of information security culture lies in determining the possibilities of personal self-realization of each employee in order to protect him/her from becoming a violator.

Different goals of IS culture strategies and objects of influence determine the specifics of the means of their implementation.

In the course of functional and strategic planning in an organization that has chosen a protective strategy, subjective, intra-organizational factors of influence on the level of development of the IS culture are taken into account: the internal state, the stage of the organization's life cycle, the level of the general organizational culture, and the presence of an operating system for protecting confidential information in the organization. The strategic plan of information security culture depends on this, i.e., what management activities will be carried out: development and implementation of policies for managing risks, information security incidents, changes, personnel, awareness, training, etc. We believe that the Federal Law On the Foundations of the Crime Prevention System in the Russian Federation is aimed at the defensive strategy of crime prevention, according to which the implementation of crime prevention is carried out through identification, assessment, and forecasting of criminogenic factors of a social nature; legal regulation of crime prevention; development of special programs in the field of crime prevention; identifying and eliminating the causes and conditions conducive to antisocial behavior and the commission of offenses; identifying persons prone to committing offenses; monitoring in the field of crime prevention, etc. (Article 6).

In addition to these management procedures provided by the protective strategy, the strategic plan for the implementation of the developmental strategy includes activities related to the development of the organization and its employees: the study of their personal qualities and values, needs and attitudes, emotional state; developing their knowledge of information security; and control over compliance with the rules of information security behavior. The degree of mutual trust, loyalty (commitment) of employees to the organization, their involvement in the implementation of the company's information security strategy, the degree of harmonization of the needs of the employer (in ensuring the organization's information security) and employees (in self-realization and self-development) are of great importance. This significantly increases the chances of success in ensuring information security and developing an information security culture. A high level of employee loyalty to the organization assumes that he/she identifies himself/herself with it, represents himself/herself and the organization as a whole, identifies himself/herself with its culture, and is able to realize all his/her personal characteristics in information behavior in the process of his professional activities. As a result, both

[1] Federal Law of 23.06.2016 N 182-FZ "On the Basics of the Crime Prevention System in the Russian Federation". – URL: http://www.consultant.ru/document/cons_doc_LAW_199976/ (Cited December 19, 2020).

the employee and the organization develop, which is the main preventive means of ensuring information security.

It is obvious that the connection between the developing strategy of information security culture and the development of the knowledge and the intellectual and cultural capital of a person requires an appeal to the strategies of knowledge management in the organization. Experts consider knowledge management in the context of sustainability [13]; on the basis of empirical research, they recognize that management of threats to knowledge is a significant mechanism for increasing organizational effectiveness [14]. This fully applies to information security culture management.

The ten strategies for transferring information from employees to the external, internal environment and for the development of individual competencies of employees by E. Sveibi are well known [15]. Russian scientists have substantiated the classification of knowledge management strategies, which is based on seven combinations of basic strategies that are aimed either at the exchange of knowledge within one type of intellectual capital in order to increase it, or at the effective transfer of knowledge from one type of intellectual capital to another. At their core, they have the movement of knowledge between individual employees (within the framework of individual competence); individual elements of the internal structure; separate elements of the external structure; elements of the external structure and employees of the organization; elements of the internal structure and employees of the organization; elements of the internal and external structure; and simultaneously between all types of intellectual capital [16, 17]. Other authors have identified four strategies for knowledge management according to the criterion of their origin: external and internal codification, as well as external and internal personalization [18]; they develop a management model based on knowledge—management—measurement—action, seeking to combine three areas that are usually considered separately: knowledge management, measurement of intellectual capital, and strategic actions [19].

The movement of knowledge between external and internal structures requires knowledge management not only of employees, but also of customers, that is, *Customer Knowledge Management* (CKM), a data-driven approach to customer relationship management (*CRM*) and a human-centered approach to knowledge management. CKM is characterized as an innovative practice of extracting and exploiting three types of knowledge: about customers, from customers, and for customers. This integrated approach involves recognizing customer knowledge as part of the company. Management of this intellectual asset is a source for product development, project management, and business success in general [20, p. 92].

Special attention is paid to knowledge management systems in small and medium enterprises, which are divided into two categories: *KM-Practices* (defined as a set of methods and techniques to support organizational knowledge management processes) and *KM-Tools* (namely, specific systems based on IT supporting KM-Practices). Small and medium-sized enterprises are adopting and using more traditional tools (KM-Tools) rather than newer and more updated ones, which are usually cheaper and easier to use. They introduce and use practices more intensively (KM-Practices) that do not focus exclusively on the knowledge management process, but seek to adapt the practices they already know to the requirements of knowledge management.

Several authors have proposed a taxonomy that integrates the KM-Practices and KM-Tools usage strategies and defines four strategies: landmark, exploiter, researcher, and latecomer. This classification is based on a set of tools and methods used for knowledge management [21].

All these approaches to the essence and types of knowledge management, as a result of the implementation of which professional and personal self-realization of the organization's employees can be achieved, are easily adapted to the management of the information security culture.

As part of the development strategy, we will consider the key factor that influences the culture of information security of an employee as a creator involved and immersed in the production and management processes of the organization.

Foreign experts have studied the role of the psychological state of full immersion of an employee in the activity and his psychological property, that is, the involvement in an organization's information security. As a result, they concluded that both immersion and psychological ownership significantly increase the desire and willingness of employees to be in compliance with information security requirements, lead to increased productivity, and also lead to initiate ethical and responsible behavior [22]. Involvement in the work of the organization allows a person to see his/her reflection in the goals and feel his/her efforts in its implementation. According to research, when people are immersed in a certain activity, they are inherently motivated to actively participate in that activity and at the same time experience a strong sense of control over the environment [23]. Employees with strong psychological involvement are reluctant to exhibit behaviors such as theft, damage to organizational property, deliberate mistakes in work, or cyber inaction [24].

All this is of great importance for information security management. In the process of implementing a defensive cybersecurity culture strategy, organizations invest heavily in employee awareness programs. For this purpose, online trainings, group meetings, e-mail communications and seminars, etc. are held. However, this does not provide the expected results. Many employees consider attending such events an additional burden and consider them as obstacles to normal work [25]. The use of intrinsic motivation inherent in a developmental strategy is usually more effective than strictly forcing employees to learn. Therefore, the transition of an enterprise from a defensive to a developing strategic model of information security culture, which allows activating the motivation of employees, launching a mechanism for their self-realization and development in information security management, is a pattern of managing human threats to an enterprise's information security. The gradual transformation of a defensive strategic model of information security culture into an offensive one is an inevitable trajectory of an enterprise in the digital industry, which is unthinkable without that of a person and his involvement in the innovative development of the economy.

The classification of strategies of information security culture, like any classification, is conditional. Here, one should use an integrative, protective and developmental strategy for managing the information security culture, which combines both grounded strategies. An integrative strategy should be inherently situational, based on monitoring the level of information security culture of employees in the process of both internal and external communications of the organization.

In the course of the study, we conducted a survey of employees of organizations of different types in order to determine their perception of the strategic aspects of information security culture management; 51 people took part in the survey, of which 64.7% were ordinary employees and 66.7% of the participants were employees from 18 to 25 years old. Organizations belonged to different areas: technology and software (19.6%), services (17.7%), education (13.7%), public services (11.8%), trade (9.8%), financial services (7.8%), industry (5.9%), healthcare, communications and energy (2% each), etc.; 56.9% of them are private enterprises, 33.3% are state-owned, and 9.8% are nonprofit organizations. Private enterprises are represented by small (41%), medium-sized (33.3%), and large (25.6%) businesses; 84.3% of all the organizations are Russian, 7.8% have a representative office in the countries of the Near Abroad, 5.9% in Europe, and 2% in North America.

The overwhelming majority of respondents answered that their organization has an information security policy (82.4%); there is an information security officer (76.5%); and that awareness raising among employees about information security is carried out (76.5%). However, only 39.2% of the organizations have employees involved in the information security breach/incident detection process and have a reporting facility/e-mail address. Disciplinary penalties for noncompliance with information security policies are in place in 66.7% of the organizations, but only 19.6% have an employee reward system (recognition, performance evaluation, remuneration, etc.) to ensure compliance with the information security policy. From this we can conclude that most organizations use a protective strategy of information security culture, which means they are at the initial stage of its development.

To stimulate the development of a culture of information security in science and practice, standardization of this process is required. Thus, for the life safety industry, this is a stage that was passed long ago: it has developed, adopted, and applied GOST R 22.3.07–2014 Safety in emergency situations. Life safety culture. General provisions [26]. GOST R IEC 62508–2014 Risk management. Analysis of the impact on the reliability of the human factor. Being identical to the international IEC 62508: 2010 standard Analysis of the impact on the reliability of the human factor (IEC 62508: 2010 Guidance on human aspects of dependability) [27] is used in other industries. These standards have given impetus to the development of scientific research and practical activities in our country. Thus, the study of indicators and criteria for assessing the human factor in order to reduce its influence is very common in the field of transport [28].

It is logical to assume that the reduction of human threats in information security and the development of an information security culture should also become objects of reflection in such standards. The Culture of information security draft standard we developed contains seven sections, in which definitions of the concepts of the human factor, human risks, culture, development strategies are formulated; factors of influence on the culture of information security at the individual and organizational levels; goals, directions, means, and methods of its formation and development; organizational principles and organizational and methodological requirements (requirements for the organization and methodology for its planning, assessment, control, and improvement); and requirements for documenting these processes (for the policy of developing an information security culture and other local documents for organizing this topic) as part of the implementation of both protective and developing strategies of information security culture. It is also advisable to supplement the standards of the ISO/IEC 27000 series on information security management and their sections on information security related to personnel with this content.

CONCLUSIONS

No matter how rapidly technologies and means of information protection develop, an information system becomes vulnerable if its user is left unattended. According to the results of analytical studies, for 4 years in a row, the share of internal information leaks of the total number of leaks accounts for more than half of all leaks recorded in the world, which occur due to errors or deliberate actions of employees (including management) and information owners. Based on the cultural parameters of human activity in the modern post-industrial digital era, as well as the theories of strategic management and psychological ownership (involvement), we present two strategies for managing human threats to an organization's information security: defensive (defensive) and offensive (developing) strategies.

Since human threats to information security cannot be considered outside the sphere of culture, these strategies are strategies of the organization's information security culture, which have specific goals, objects, and means of implementation.

The defensive strategy is aimed at minimizing information security threats, targets employees as potential violators, and is implemented primarily through coercive measures. The development strategy aims to create a system to reduce the threats of potential victimization of employees, is aimed at developing the factors of their personal development, and is implemented through cooperation between the employer and employees, increased involvement in production and management processes, and the development of psychological property of employees.

The modern imperative of the digital industry and the regularity of the transition from a defensive to an offensive strategy of information security culture have been revealed.

The results of a sociological survey of employees of organizations of various industries and forms of ownership on information security management were carried out using tools in Google forms.

The conclusion has been made of the dominance of a defensive strategy in organizations using awareness raising and disciplinary sanctions for violation of information security policies.

The necessity of using knowledge management technologies, as well as an integrative, situational strategy for information security culture management, which combines both grounded strategies at the levels of internal and external communications of the organization, has been proven.

The need for standardization of information security culture is substantiated using the experience of culture standardization in a related area, that is, life safety. The concept of the draft Culture of information security national standard is presented.

FUNDING

The work was supported by Act 211 of the Government of the Russian Federation, contract no. 02.A03.21.0011.

REFERENCES

1. Leaks of These Organizations through Fault or Negligence of Insiders. Comparative Study. 2013–2019: Analytical Report. https://www.infowatch.ru/sites/default/files/analytics/files/InfoWatch_Analytical_Report.pdf. Cited December 19, 2020.
2. Lukatskii, A., Exploitation of Coronavirus Agenda in Information Security Threats. https://habr.com/ru/company/cisco/blog/494726/. Cited December 19, 2020.
3. Lukatskii, A., Cybersecurity Is Victim's Own Business. https://lukatsky.blogspot.com/2019/12/blog-post_23.html. Cited December 19, 2020.
4. Flier, A.Ya., Human activity and its cultural parameters, *II Moiseevskie chteniya: Kul'tura kak faktor natsional'noi bezopasnosti Rossii. Doklady i materialy Obshcherossiiskoi (natsional'noi) nauchnoi konferentsii* (II Moiseev Readings: Culture as a Factor of Russia's National Security. Reports and Materials of the All-Russian (National) Scientific Conference), Moscow, 2019, pp. 299–305.
5. Flier, A.Ya., Local cultural system: Factors of sustainability, *Kul't. Kul't.,* 2020, no. 1, p. 1.
6. da Veiga, A., Astakhova, L.V., Botha, A., and Herselman, M., Defining organisational information security culture—perspectives from academia and industry, *Comput. Secur.,* 2020, vol. 92, p. 101713.
7. Astakhova, L.V., Issues of the culture of information security under the conditions of the digital economy, *Sci. Tech. Inf. Process.,* 2020, vol. 47, no. 1, pp. 56–64.
8. Tompson, A.A. and Striklend, A.Dzh., *Strategicheskii menedzhment. Iskusstvo razrabotki i realizatsii strategii* (Strategic Management. The Art of Developing and Implementing a Strategy), Moscow: Banki i birzhi, YuNITI, 1998.
9. Veklenko, P.V., Situational approach in the social-human cognition: Objectives, principles and categories, *J. Sib. Fed. Univ., Humanit. Soc. Sci.,* 2015, vol. 8, no. 5, pp. 1003–1010.
10. Lekar', A.G., *Profilaktika prestuplenii* (Crime Prevention), Moscow: Yuridich. Lit., 1972.
11. Rivman, D.V., *Kriminal'naya viktimologiya* (Criminal Victimology), St. Petersburg: Piter, 2002.
12. Gerbekov, I.I., The concept and types of crime prevention, *Yuridich. Nauka Pravookhr. Prakt.,* 2017, no. 4, pp. 99–105
13. Martins, V.W.B., Rampasso, I.S., Anholon, R., Quelhas, O.L.G., and Leal Filho, W., Knowledge management in the context of sustainability: Literature review and opportunities for future research, *J. Cleaner Prod.,* 2019, vol. 229, pp. 489–500.
14. Durst, S., Hinteregger, C., and Zieba, M., The linkage between knowledge risk management and organizational performance, *J. Bus. Res.,* 2019, vol. 105, pp. 1–10.
15. Sveiby, K.-E., A knowledge-based theory of the firm. To guide strategy formulation, *J. Intell. Cap.,* 2001, vol. 2, no. 4. file:///C:/Users/1D1D~1/AppData/Local/Temp/knowledgetheoryoffirmfin-draft-1.pdf.
16. Gaponenko, A. and Orlova, T., *Upravlenie znaniyami* (Knowledge Management), Moscow: Eksmo, 2008.

17. Panikarova, S.V. and Vlasov, M.V., *Upravlenie znaniyami i intellektual'nym kapitalom* (Knowledge and Intellectual Capital Management), Yekaterinburg: Ural. Univ., 2015.
18. Kim, T.H., Lee, J.N., Chun, J. U., and Benbasat, I., Understanding the effect of knowledge management strategies on knowledge management performance: A contingency perspective, *Inf. Manage.,* 2014, vol. 51, no. 4, pp. 398–416.
19. Córdova, F.M., Durán, C. A., Pincheira, M., Palominos, F., and Galindo, R., Knowledge management of intangible actives, *Serv. Co. Procedia Comput. Sci.,* 2019, vol. 162, pp. 596–603.
20. Gerbina, T.V., Management strategies: Customer knowledge management, *Sotsial'no-orientirovannoe upravlenie v usloviyakh globalizatsii. Materialy VI Vserossiiskoi zaochnoi nauchno-prakticheskoi konferentsii* (Socially Oriented Management in the Context of Globalization. Proc. VI All-Russian Correspondence Scientific and Practical Conference), Moscow, 2017, pp. 91–96.
21. Cerchione, R. and Esposito, E., Using knowledge management systems: A taxonomy of SME strategies, *Int. J. Inf. Manage.,* 2017, vol. 37, no. 1, part B, pp. 1551–1562.
22. Yoo, C., Sanders, G., and Cerveny, R., Exploring the influence of flow and psychological ownership on security education, training and awareness effectiveness and security compliance, *Decis. Support Systems,* 2018, vol. 108, pp. 107–118.
23. Ho, L.-A. and Kuo, T.-H., How can one amplify the effect of e-learning? An examination of high-tech employees' computer attitude and flow experience, *Comput. Human Behav.,* 2010, vol. 26, no. 1, pp. 23–31.
24. Shantz, A., Alfes, K., Truss, C., and Soane, E., The role of employee engagement in the relationship between job design and task performance, citizenship and deviant behaviours, *Int. J. Human Resour. Manage.,* 2013, vol. 24, no. 13, pp. 2608–2627.
25. Bulgurcu, B., Cavusoglu, H., and Benbasat, I., Information security policy compliance: An empirical study of rationality-based beliefs and information security awareness, *MIS Q.: Manage. Inf. Syst.,* 2010, vol. 34, no. 3, pp. 523–548.
26. *GOST* (State Standard) *R 22.3.07–2014: Safety in Emergency Situations. Life Safety Culture. General Provisions,* Moscow: Standartinform, 2019. http://docs.cntd.ru/document/1200109440. Cited December 19, 2020.
27. *GOST* (State Standard) *R IEC 62508–2014: Risk Management. Analysis of the Impact of the Human Factor on the Reliability* (*IEC 62508:2010 Guidance on Human Aspects of Dependability*). http://docs.cntd.ru/document/1200113803. Cited December 19, 2020.
28. Yan'shina, I.V. and Repina, I.B., The state, indicators, and criteria for assessing the human factor in the structure of failures of technical means of the track complex of the railway, *Vestn. Sib. Gos. Univ. Putei Soobshch.,* 2019, no. 3, pp. 53–58.