ISSN 0147-6882, Scientific and Technical Information Processing, 2020, Vol. 47, No. 4, pp. 241–247. © Allerton Press, Inc., 2020.
Russian Text © The Author(s), 2020, published in Nauchno-Tekhnicheskaya Informatsiya, Seriya 1: Organizatsiya i Metodika Informatsionnoi Raboty, 2020, No. 11, pp. 1–8.

The Validity of Information Security Risk Assessment Methods for Organizations

L. V. Astakhova*

Department of Information Security, South Ural State University (National Research University), Chelyabinsk, 454080 Russia
**e-mail: astakhovalv@susu.ru*

Received April 18, 2020

Abstract—Based on statistical data, a contradiction is shown between an increase in financial investments in the information security (IS) of organizations and a steady increase in the number of IS incidents caused by internal users. A conclusion is made about the cognitive vulnerability and low degree of validity of modern IS risk assessment methods. Stereotypes have been identified, the result of which are cognitive errors in assessing IS risks: the priority of technical protection of information from external threats of IS over organizational and technical protection from internal threats; distrust of the internal client, perception of it exclusively as an object of tough managerial influence, ignoring its subjective role in IS management; restriction of work with personnel within the IS management system with one-time measures and static criteria for assessing human risks and inattention to systemic measures and dynamic, situational criteria. The necessity of updating standards for IS risk management, as well as the development of new methods and tools for assessing, IS risks based on rejecting outdated stereotypes, is substantiated.

Keywords: risk, information security, methodology, validity, cognitive biases, cognitive errors, internal violator, human risks, involvement, situational awareness

DOI: 10.3103/S014768822004005X

INTRODUCTION

Human capital is the most important asset of any organization; therefore, like any capital, it has its own vulnerabilities. Information security threats from a person (employee, organization employee, internal client, internal violator, information system user, etc.) are very dangerous. Annual analytical reports prepared by foreign and Russian companies indicate a steadily continuous increase in the number of incidents of threats to information-security organizations that occurred through the fault of internal violators. For the first time since 2004, internal information leaks have shown higher "power" than external ones: as a result of one internal leak, a much larger amount of data was compromised than in the result of one external leak [1]. According to the research results, 77% of companies consider internal incidents more dangerous than external ones; 16% of Russian companies reported an increase in the number of internal incidents. At least 40% of companies in Russia and 30% in the CIS have faced attempts by dismissed employees to harm the company. In 2019, managers were responsible for information-security threats in 27% of cases and ordinary employees in 73%. This is despite the fact that companies are investing financial resources in information security (64% of companies reported no dynamics in changing the information-security budget in 2019, and 25% reported its increase) and are working on awareness of employees in the field of information security (75% of enterprises named information-security training among the methods of protection that are used in the organization) [2].

The results of a comparative analysis of the distribution of confidential information leaks in the financial segment are interesting: in the world in 2019 the share of internal attackers was 37.4%; in Russia it was 91.3%. In Russia, there were more than 2 times more leaks for the purpose of data fraud, compared with other countries of the world (44.2% and 19.3%, respectively) [3].

The increase in the number of incidents of information-security threats caused by internal customers with stable budgeting and measures to raise their awareness leads us to the conclusion that the threat of human threats is increasing, their malicious nature increases, and, therefore, the importance of effective management of them. The low efficiency of all efforts to prevent IS threats indicates the deepening of cognitive distortions in the process of assessing IS risks and the cognitive vulnerability of modern methods of such an assessment, and their low degree of validity.

The validity reflects the quality of measurement of parameters of objects, the degree of correspondence of the measured indicator to what is to be measured, and

assumes the absence of initial cognitive errors at the stage of development of the measurement methodology.

Errors are a consequence of the cognitive distortion of the properties of the studied objects. *Cognitive distortion* in the understanding of foreign scientists, it is a systematically that occurs with evolutionarily formed deviation in perception, behavior and thinking, which at the situational level is due to the subjective perception of the individual, social, moral and emotional stereotypes, as well as the specificity of the limited capabilities of the human brain to receive, process and represent information [4]. Cognitive biases affect both perception, thinking and, in particular, people's actions.

We distinguish three main cognitive biases in the assessment of information-security threats. The existing methods reflect, first, a focus on the technical aspects of protection against external attacks and insufficient attention to the influence of internal factors (motivation and user behavior); second, a low degree of use of their human potential, lack of employee involvement in the process of managing information-security threats; and third, the problems of implementing situational, dynamic assessment of information-security threats. Let's consider them in more detail.

COGNITIVE DISTORTION OF THE ESTIMATION OF IS THREATS DUE TO LACK OF ATTENTION TO INTERNAL HUMAN RISKS

Organizations are more focused on protecting against external attacks and threats to ensure the confidentiality, integrity and availability of their information assets, often ignoring internal threats.

This problem has recently become the object of special scientific research. Thus, foreign experts considered well-known threat-assessment techniques (OCTAVE Carnegie Mellon method, COBIT, ITIL, CORAS, ISRAM and CRAMM, as well as others that are presented and listed by ENISA) [5]. The results of this and other studies [6, 7] showed the low efficiency of information-security management processes. The authors of these studies demonstrated that enterprises that adopt widely used security practices continue to struggle to assess, manage their threats, and implement appropriate security measures. They came to the conclusion that the existing models and structures of information-security threat management are mainly focused on technical aspects and do not pay much attention to the influence of internal factors (motivation and user behavior) on the reliability of decisions [8, 9].

Foreign researchers intensified the study of the problems of prevention and detection of internal threats in the early 2000s. Thus, they proposed a framework for predicting attacks from insiders, mainly based on personality traits and verbal behavior [10]; they used attributes of metrics of the knowledge, privileges and skills of users [eleven]; modeled an insider profile by identifying the attributes of personnel, studied the relationship between the intentions and actions of the user [12]; proposed a method for measuring the misuse of the ISO17799 standard by insiders [thirteen]; etc. Even then, developments appeared in which attempts were made to integrate technical and psychological solutions. As an example, the authors of [14] presented a model for predicting insider behavior using user taxonomy, psychological profiling, and a decision-making algorithm to identify potentially dangerous users.

For the sake of fairness, we note that in purely technical solutions there are also assessments of internal threats. Thus, intrusion detection systems can be used to detect internal violations of security policies and anomalous activities in the information system. This can be achieved using artificial intelligence technologies [15]. The authors of [16] illustrated this with an example of a system that models the user's life cycle to analyze his interaction with internal security strategies. Other approaches rely on the production of decoys to detect potential abuse by insiders.

It is clear that the end threats are still those that do not leave a technologically detectable mark on the system or do not use routine actions to commit malicious acts. Therefore, broader methods of assessing information-security threats associated with personnel are required. This fact is taken into account in modern methods and tools for assessing information-security systems. As an example, the Microsoft Security Assessment Tool (MSAT) is a threat assessment tool that provides information about the security of IT infrastructure and recommendations for improving it based on best practices. According to the developer, "this tool uses a holistic approach to assessing the security system and analyzing the influence of the human factor, processes and technologies" [17].

The assessment of human factors is based on the following questions: does the company have individual or group responsibilities in relation to safety; does a person or group of persons have adequate security experience; is this person or group involved in defining security requirements for new and existing technologies; at what stages of the technology life cycle is this person or group involved in ensuring security (planning and design, implementation, testing, and deployment); are roles and responsibilities defined for each person involved in information security; are independent third-party experts used to assess the security of the environment; is the security assessment of the environment performed by internal specialists of the organization; Does the organization practice background checks as part of the hiring process; is an official policy regarding employees leaving the company; is there is an official policy for regulating third-party relationships; does the company have a safety notifi-

cation program; and is thematic training provided for employees, depending on their role in the organization. The questions and recommendations proposed by the developers of this tool [17] are based on existing standards (ISO/IEC 17799-2005 Technologies de l'information–Techniques de security–Code de pratique pour la gestion de security d'information. Information Technology–Security Methods–Practical Guide for Information Security Management (clause 8. Human Resource Security) [18] and NIST-800.x NIST (National Institute of Standards and Technology) (Section Creating awareness in the field of IT security) [17, 19, 20,]. Unfortunately, they do not take the psychological aspects of the behavior of internal clients into account and therefore are limited.

Other experts have come to the same conclusion, claiming that, despite the fact that there are a significant number of models designed to eliminate internal threats, they, as a rule, solve the problem only to a limited extent, paying special attention to individual highlighted metrics that are very difficult to integrate into a unified approach to threat assessment [14, 21].

Russian scientists also have drawn attention to the threats of uncontrolled, ignored internal vulnerabilities. To solve this problem, A.A. Kononov proposed a methodology of detailed criterial modeling, which includes a number of methods, whose complex use allows one to largely remove the problems associated with the coverage and hazard assessment of the entire set of possible vulnerabilities, no matter how great it may be [22]. Therefore, more and more experts are discussing methodological problems for assessing internal threats and their consequences, as well as their integration into the structure of security threats, which was defined in accordance with the security standards of the ISO/IEC 27000 series for information-security management [5].

The ability to script internal threats can be a useful mitigation tool. The authors of [23] have developed models of insider threats that help to quantify threats and determine the likelihood of specific scenarios.

Thus, it becomes clear that in order to assess internal IS threats, the primary tasks of the employer are assessment of the user's predisposition to malicious behavior and his IT skills; developing procedures for collecting information on user perceptions, attitudes and feelings, safety behavior and associated risks; and creation of metrics. At the same time, all the above actions should be documented in international and national IS standards used for certification of organizations [5], in the documents of state regulators that are binding. Suffice it to say that such standards exist in other areas [24, 25].

COGNITIVE DISTORTION OF THE ESTIMATION OF IS THREATS DUE TO EMPLOYEES WHO ARE DISABLED IN THE MANAGEMENT PROCESS

In recent years, in management theory, special attention has been paid to the involvement of employees of the organization, that is, their willingness to fully invest cognitive, emotional and physical energy into their work [26–28]. In all spheres of cognitive society, a person has become a full-fledged subject of information activity. However, in the field of information protection, a stable practice of distancing the employer from employees has developed, who, in all existing methods of assessing threats, remain passive objects of managerial influences. Hypertrophied control over the organization's employees by the management inevitably leads to negative psychological consequences: stress, anger, loss of confidence in management and other issues, which, as a rule, lead not to the expected decrease, but, on the contrary, to an increase in their vulnerability in the information-security system. In conditions of mutual mistrust, the employer sooner or later loses his even very loyal employees. In other industries, the critical importance of the trust factor has long been recognized. Thus, in the nuclear power industry there is a principle of "organization imbued with trust" to achieve a culture of nuclear safety. The atmosphere of trust in the organization is formed from a conscious attitude of the work environment to safety issues (SCWE: safety-conscious work environment) and respect between managers and staff, when there are no signs of a "chilling effect" in the actions and decisions of management, harassment, intimidation, retaliation, or discrimination against employees [29].

The field of information security is in dire need of increasing trust between the employer and employees of the organization. In one of our studies, we defined the ontological status of trust in information security as follows: "Trust in information security is an *information-measuring control mechanism* (planning, implementation, control, and motivation) by the safe interaction of subjects of information relations, aimed at their sustainable functioning and development" [30]. The emphasis on employees of the organization as subjects of information relations, their needs for security and development, the degree of harmonization of their information interaction with employers, and their information and psychological security, of course, allows us to measure the degree of their loyalty to the organization. A positive, mutually trusting relationship between the manager and employees is more effective for ensuring information security.

A striking example of our conceptual approach to the status of trust in information security is the concept of a person as a security sensor (sensor) (The Human-as-a-Security-Sensor paradigm), which is actively developing today in foreign science and prac-

tice. Foreign experts are confident that employees can be empowered to take responsibility for the organization's information security [31], they can be the "last line of defense" [32], they develop special products so that users can independently detect social engineering attacks and report them to the appropriate departments of the organization [33]. This means that trust delegation and empowerment of employees in the field of information-security management can and should be included both in the standards for managing information-security threats, and in the structure of indicators in the methods for assessing these threats.

COGNITIVE DISTORTION OF THE ESTIMATION OF IS THREATS DUE TO THE IMPLEMENTATION OF DYNAMIC SITUATIONAL ASSESSMENT

National Institute of Standards and Technology NIST SP 800-53 rev. 5 Security and Privacy Controls for Information Systems and Organizations (Security and Privacy Controls for Information Systems and Organizations, revision 5, March 2020) [19] provides an update of the assessment threats using the results of their continuous monitoring (Section 3.16 RISK ASSESSMENT). The annexes to this standard contain examples of calculations for each of the subtasks, as well as lists of possible threat sources, threat events, vulnerabilities, and preconditions. NIST SP 800-137 rev. 2 Information Security Continuous Monitoring for Federal information Systems and Organizations [20] describes a strategy for continuous monitoring of information security (Continuous monitoring of information security for federal information systems and organizations edition 2, December 2018). The purpose of its construction is to assess the effectiveness of protection measures and the security status of systems to respond to constantly changing challenges and tasks in the field of information security. Continuous information-security monitoring helps to provide situational awareness of the state of security of the company's information systems based on data collected from various resources (such as assets, processes, technologies, and employees), as well as information about the available capabilities to respond to changes in the situation [34].

However, experts point out that the identified methods of comprehensive threat assessment for protection and security still do not take the system information for dynamic risk assessment into account, which is necessary to make this assessment more effective [35].

Reasonable cognitive distortions in the assessment of information-security threats are caused by objectively established stereotypes. The rapid growth of technological progress and the development of informatization and communication facilities in the 20th century were focused on the technical protection of information. The conditions of the Cold War fully explain the priorities of external IS threats. The lack of attention to the internal threats of information security is largely due to the experience of regime protection of state secrets and the effective Soviet system of education, highly developed patriotic and moral values of citizens. Difficulties in formalizing the processes of assessing the psychological aspects of human activity did not allow the inclusion of human criteria in the standards and methods for assessing IS threats. Finally, the lack of technological foundations for monitoring the level of information security of an organization explains the lack of attention to situational management of human threats to its security.

As can be seen, the named cognitive biases in assessing IS threats are of a completely objectively deterministic nature. Theoretical studies also show that "distortion is an integral part of the process of cognition of the surrounding, fluid and flickering reality, reflecting the peculiarities of the subject's adaptation to these processes" [36, p. 68], this is "a part of the nature of cognitive mechanisms, all subjects are a priori subject to them" [36, p. 67]. However, "distortion can be subjective, reflect the uniqueness of the individual's intrapsychic processes, caused by situational factors" [36, p. 67]. According to experts in the field of cognitive biases, we cannot "rationalize" what is irrational from the beginning - as if a lie were called the truth. One can get more people to believe a particular judgment, but one cannot make it more true. To strengthen the truth of a belief, we must change those beliefs [37] by testing them in practice.

Therefore, we believe that the concept of cognitive error is much more heuristic for the practice of information-security threat management. Unlike cognitive biases, cognitive errors have an important characteristic of verifiability and provide the quality of forecasting the development of the situation and the effectiveness of activities: they assume the presence of accurate data on *what decision should have been made and what are the consequences of using a particular cognitive scheme*. For example, a doctor who misdiagnoses a patient, i.e., who has committed a medical error, can admit this fact when the patient's condition worsens. In other words, "an error places a person in a verifiable condition, subject to verification and finding the right answers to the challenges of reality" [36]. Finding the right answers to the growth of internal threats and vulnerabilities is exactly what the information-security threat management area needs today.

This statement allows us to conclude that a new threat of information security consists of cognitive errors in the results of assessing the risks of information security of organizations based on modern methods that are developed on the basis of the stereotypes described in this article. These errors are evidenced by the steady increase in the number of information-security threat incidents associated with internal violators of organizations, even if they practice the assess-

ment of these threats. The implementation of the presented methods does not allow avoiding damage from the growing number of incidents of the IS threat. Acknowledging the fact of errors requires finding more correct answers to the question of how to assess these threats. One obvious conclusion is that it is necessary to include formalized and nonformalized methods for monitoring and processing human threats and taking the degree of involvement of internal clients in information-security management processes into account and trust in them in the threat assessment methods.

A positive fact of recognizing cognitive distortions and errors in assessing information-security threats is the emergence of tools on the modern information-security market that are capable of monitoring data on employee actions in the workplace. Thus, the InfoWatch Person Monitor is a simple and fast way to identify disloyal employees and monitor the actions of privileged users. Collecting complete information about user actions allows one to record screenshots and video from a screen, images from a webcam, sound from a microphone and speakers; incoming and outgoing e-mails, attachments; monitoring of communications in the messengers Lync, Skype, Teams, Viber, Telegram, WhatsApp, Bitrix24, etc.; visited sites and Internet requests, file transfer through file hosting services, web mail and chats; application usage statistics and text input monitoring; face recognition from webcams to control the presence and identification of employees; operations with documents: deletion, printing, copying to external media and to the cloud; the fact of being in the workplace and in the office, time spent at the computer; the geolocation of mobile devices and laptops on Android, Windows 10 platforms; and expanding monitoring capabilities on PCs running macOS and Astra Linux. These measures will allow the information-security service to take control of the management of human threats to information security [38].

ProfileCenter is another software solution that is used to detect fraudulent activities and to predict and detect destructive behavior of employees towards the organization; it also allows one to calculate personal threats to others or the company. ProfileCenter is ready to provide an up-to-date and detailed description of each employee, to identify significant fluctuations in the mood of employees, and also to assess the psychological atmosphere in the team at any time. The DLP system collects the employee's correspondence: outgoing letters, messages in Skype, Viber, WhatsApp, Lync, Telegram, other messengers and social networks. At any time, using this system, one can see potential threats associated with a specific employee, and recommendations for mitigating them: which employee needs to be monitored from time to time, constantly or in certain situations; whether the employee is suitable for a particular position, whether he has the necessary qualities, etc.; how safe is it to give an employee access to confidential information, financial assets and valuable company resources; which persons in the team it is possible to maintain emphatically business and formal relations, and with which persons, on the contrary, to establish friendly relations; for which of the employees are "suggestion" and preventive conversations enough, and which should be regularly trained on information security; who should be punished more severely for breaking the rules, etc. [39]. The development and use of new similar methods and assessment tools, their integration into existing methods and tools, as well as updating the standards for information-security threat management and the adoption of special standards for managing human security threats is the reaction that should follow the recognition of cognitive biases and errors in assessment information-security threats.

In organizations, it is advisable to develop local documents on information-security threat management, which should provide the requirement to use threat assessment methodology that is developed on the basis of a triangulation strategy, that is, a combination of at least three quantitative and qualitative measurement methods. The study of the validating function of triangulation in methodology is a significant trend in modern social sciences and psychology [40]. Based on the totality of different types of triangulation [41], it is logical to conclude that in order to increase the reliability of the results of assessing IS threats, one should consider not only static, but also dynamic indicators of threats, changes in time and space (data triangulation); evaluative opinions of heads of different structural divisions as different subjects of IS threat assessment (triangulation of researchers); not only the theory of engineering and technical protection of information systems, but also the theory of organizational and technical support of information security related to personnel (triangulation of theories); data obtained using a variety of methods: analysis of statistics on the sources and types of incidents of information-security threats in the organization; and data on the properties of risk sources obtained through observation, questionnaires, instrumental monitoring, expert assessments, the degree of personnel involvement in information-security management, etc. (methodological triangulation). Only the presence of a stable correlation between the results obtained using different approaches within the framework of such an integrative technique can serve as one of the grounds for recognizing this technique as valid. In the context of the development of machine-learning technologies, it should be assumed that it is necessary and possible to create tools for assessing information-security threats based on the integrative techniques that were presented in this article.

CONCLUSIONS

Information-security-threat management is practiced in most organizations today, but the number of threats caused by internal users is growing steadily. This indicates that the existing methods for assessing IS threats and the tools created on their basis are imperfect, i.e., possess cognitive vulnerability. Risk assessment according to these methods is based on deviations in perception, behavior and thinking, and on erroneous stereotypes: (1) on the priority of technical protection of information from external IS threats; (2) about the internal client solely as an object of tough management influence, denying their subjective role in information-security management; and (3) on the adequacy of working with personnel within the IS management system and the impossibility of taking situational assessment criteria into account. These stereotypes not only lead to erroneous results in assessing information-security threats, but also impede the harmonization of relations between the employer and employees or lead to the destruction of their mutual trust, increasing the vulnerability of the organization. Therefore, the processes of assessing information-security threats based on existing methods represent a cognitive distortion, and the results of these processes are cognitive errors, which are new threats to information security in the era of transformation of culture and social roles in the knowledge society. To correct these errors, it is necessary to abandon the stereotypes shown in this article and develop fundamentally new practices for working with internal clients, as well as methods and tools for assessing human threats to information security. The most important task is to update the standards for managing information-security threats, adopt special standards for managing human threats, develop integrative methods for assessing information-security threats, and create new tools on their basis.

FUNDING

This article was prepared with the support of the Government of the Russian Federation (Resolution No. 211 of March 16, 2013, Agreement No. 02. A03.21.0011).

CONFLICT OF INTEREST

The authors declare that they have no conflicts of interest.

REFERENCES

1. PriceWaterhouseCoopers. The Global State of Information Security® Survey 2018. https://www.pwc.com/us/en/services/consulting/cybersecurity/library/information-security-survey.html. Accessed March 31, 2020.
2. Investigation of the Level of Information Security in Companies in Russia and the CIS for 2019. https://searchinform.ru/research-2019/. Accessed March 31, 2020.
3. Investigation of Confidential Information Leaks from Financial Segment Organizations in 2019. https://www.infowatch.ru/analytics/reports/21649. Accessed March 31, 2020.
4. Kahneman, D., Slovic, P., and Tversky, A., *Judgment under Uncertainty: Heuristics and Biases,* Cambridge Univ. Press, 1982.
5. Pereira, T. and Santos, H., Insider threats: The major challenge to security risk management, *Human Aspects of Information Security, Privacy, and Trust. HAS 2015*; *Lect. Notes Comput. Sci.,* 2015, vol. 9190, pp. 654–663.
6. Sadok, M. and Spagnoletti, P., A business aware information security risk and analysis method, in *Information Technology and Innovation Treads in Organization,* D'Atri, A., Ferrara, M., George, J.F., and Spagnoletti, P., Eds., 2011, pp. 453–460.
7. Asosheh, A., Dehmoubed, B., and Khani, A., A new quantitative approach for information security risk assessment, *IEEE International Conference on Intelligence and Security Informatics (ISI 2009),* 2009, pp. 229–239. http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5137311&isnumber=5137253. https://doi.org/10.1109/ISI.2009.5137311. Accessed March 31, 2020.
8. Posey, C., Roberts, T.L., Lowry, P.B., Bennett, R.J., and Courtney, J., Insiders' protection of organizational information assets: Development of a systematics-based taxonomy and theory of diversity for protection-motivated behaviors, *MIS Q.,* 2013, vol. 37, no. 4, pp. 1189–1210.
9. Posey, C., Roberts, T.L., Lowry, P.B., and Hightower, R.T., Bridging the divide: A qualitative comparison of information security thought patterns between information security professionals and ordinary organizational insiders, *Inf. Manage.,* 2014, vol. 51, no. 5, pp. 551–567. http://dx.doi.org/CrossRefGoogleScholar. Accessed March 31, 2020.
10. Schultz, E.E., A framework for understanding and predicting insider attacks, *Comput. Secur.,* 2002, vol. 21, no. 6, pp. 526–531.
11. Wood, B., An insider threat model for adversary simulation, in *Research on Mitigating the Insider Threat to Information Systems*, Anderson, R.H., Ed., RAND, 2000, no. 2. https://www.yumpu.com/en/document/read/22015185/an-insider-threat-model-for-adversary-simulation-. Accessed April 1, 2020.
12. Caputo, D., Marcus, A., Maloof, M., and Stephens, G., Detecting insider theft of trade secrets, *IEEE Secur. Priv.,* 2009, vol. 7, no. 6, pp. 14–21.
13. Theoharidou, M., Kokolakis, S., Karyda, M., and Kiountouzis, E., The insider threat to information systems and the effectiveness of ISO17799, *Comput. Secur.,* 2005, vol. 24, no. 6, pp. 472–484.
14. Kandias, M., Mylonas, A., Virvilis, N., Theoharidou, M., and Gritzalis, D., An insider threat prediction model, *TrustBus 2010: Trust, Privacy and Security in Digital Business*; *Lect. Notes Comput. Sci.,* 2010, vol. 6264, pp. 26–37. https://doi.org/10.1007/978-3-642-15152-1_3.

15. Cappelli, D.M., Moore, A.P., Trzeciak, R.F., and Shimeall, T.J., *Common Sense Guide to Prevention and Detection of Insider Threat,* Pittsburgh: Carnegie Mellon Univ., 2009, 3rd ed.

16. Duran, F., Conrad, S., Conrad, G., Duggan, D., and Held, E., Building a system for insider security, *IEEE Secur. Priv.,* 2009, vol. 7, no. 6, pp. 30–38.

17. Microsoft Security Assessment Tool 4.0. https://www.microsoft.com/ru-RU/download/details.aspx?id=12273. Accessed March 31, 2020.

18. *ISO/IEC 17799-2005: Technologies de l'information – Techniques de security – Code de pratique pour la gestion de security d'information*. https://www.iso.org/standard/39612.html. Accessed March 31, 2020.

19. *NIST SP 800-53 rev.5: Security and Privacy Controls for Information Systems and Organizations*. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5-draft.pdf. Accessed March 31, 2020.

20. *NIST SP 800-137: Information Security Continuous Monitoring for Federal information Systems and Organizations*. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST. SP.800-37r2.pdf. Accessed March 31, 2020.

21. Beres, Y., Mont, M.C., Griffin, J., and Shiu, S., Using security metrics coupled with predictive modeling and simulation to assess security processes, *3rd International Symposium on Empirical Software Engineering and Measurement, Lake Buena Vista, FL,* 2009, pp. 564–573. https://doi.org/10.1109/ESEM.2009.5314213

22. Kononov, A.A., Cognitive distortions as threats to information security and methods of countering them, in *Sovremennye problemy i zadachi obespecheniya informatsionnoi bezopasnosti: Sb. statei* (Current Problems of Information Security: Collection of Papers), Moscow, 2017, pp. 27–32.

23. Coles-Kemp, L. and Theoharidou, M., Insider threat and information security management, in *Insider Threats in Cyber Security. Advances in Information Security,* Probst, C., Hunker, J., Gollmann, D., and Bishop, M., Eds., Boston, MA: Springer, 2010, vol. 49, pp. 45–71.

24. *GOST* (State Standard) *R 22.3.07–2014: Safety in Emergency Situations. Life Safety Culture. General Provisions*. https://base.garant.ru/70981162/. Accessed March 31, 2020.

25. *GOST* (State Standard) *R IEC 62508–2014: Risk Management. Analysis of Human Factor Impact on Reliability*. https://base.garant.ru/71268248/. Accessed March 31, 2020.

26. Saks, A.M., Translating employee engagement research into practice, *Organ. Dyn.,* 2017, vol. 46, no. 2, pp. 76–86.

27. Employee Engagement and Motivation. Understand the Concept of Employee Engagement and Learn How to Build an Engaged and Motivated Workforce. Chartered Institute of Personnel and Development, 2018. https://www.cipd.co.uk/. Accessed March 31, 2020.

28. Veretkovskaya, O.V., Organization's personnel Engagement as a relevant task of modern companies, *Ekon. Biz.: Teor. Prakt.,* 2019, no. 4-2, pp. 40–43.

29. Mashin, V.A., Safety culture: The principle of an atmosphere of trust in the organization, *Elektr. Stantsii,* 2018, no. 9, no. 1046, pp. 2–14.

30. Astakhova, L.V., The ontological status of trust in information security, *Sci. Tech. Inf. Process.,* 2016, vol. 43, no. 1, pp. 58–65.

31. Ashenden, D. and Sasse, A., CISOs and organisational culture: Their own worst enemy?, *Comput. Secur.,* 2013, vol. 39, part B, pp. 396–405.

32. Mansfield-Devine, S., Raising awareness: People are your last line of defence, *Comput. Fraud Secur.,* 2017, vol. 2017, no. 11, pp. 10–14.

33. Heartfield, R. and Loukas, G., Detecting semantic social engineering attacks with the weakest link: Implementation and empirical evaluation of a human-as-a-security-sensor framework, *Comput. Secur.,* 2018, vol. 76, pp. 101–127.

34. Rakhmetov, R., Information security risk management. Part 5. NIST SP 800-30 Standard (continued). NIST SP 800-137 Standard. https://www.securityvision.ru/blog/upravlenie-riskami-informatsionnoy-bezopasnosti-chast-5-standart-nist-sp-800-30-prodolzhenie-standar/. Accessed March 31, 2020.

35. Chockalingam, S., Hadžiosmanović, D., Pieters, W., Teixeira, A., and van Gelder, P., Integrated safety and security risk assessment methods: A survey of key characteristics and applications, *Critical Information Infrastructures Security. CRITIS 2016*; *Lect. Notes Comput. Sci.,* 2017, vol. 10242, pp. 50–62.

36. Legostaeva, E.S., Methodological prerequisites for the study of cognitive errors, in *Sovremennaya nauka v teorii i praktike: Monogr.* (Contemporary Science in Theory and Practice: Monography), Akutin, S.P., Ed., Moscow, 2018, pp. 53–72.

37. Yudkowsky, E., Cognitive biases potentially affecting judgment of global risks, in *Global Catastrophic Risks,* Bostrom, N. and Ćirković, M.M., Eds., New York: Oxford Univ. Press, 2008, pp. 91–119. https://intelligence.org/files/CognitiveBiases.pdf. Accessed April 1, 2020.

38. Infowatch Person Monitor. https://www.infowatch.ru/products/person-monitor. Accessed March 31, 2020.

39. Searchinform Profilecenter. https://searchinform.ru/products/kib/profilecenter. Accessed March 31, 2020.

40. Mel'nikova, O.T. and Khoroshilov, D.A., Strategies for validating qualitative research in psychology, *Psikhol. Issled.,* 2015, vol. 8, no. 44, pp. 3. http://psystudy.ru. Accessed April 18, 2020.

41. Denzin, N., *The Research Act: A Theoretical Introduction to Sociological Methods,* New York: Imprint Routledge, 2009. https://doi.org/10.4324/9781315134543. Accessed April 18, 2020.