Enhancing the safety of energy systems functioning at their digitalization

Natalia Kuznetsova [1], and *Yuri* Konovalov[2,*]

[1]PhD in Economics, Novosibirsk State Technical University, Novosibirsk, Russia
[2]Candidate of technical sciences, Angarsk State Technical University, Angarsk, Russia

Abstract. Informational safety threats have been analyzed for energy systems digitalization. It was established, it is impossible to completely eliminate the human factor in insuring cybersecurity of energy facilities being digitized. At the same time, a better understanding of how human actions affect reliability and safety will make it possible to predict the human factor influence and help to enhance safety of the power systems operation. The analysis of the digital transformation evelopment lines indicates that power generation companies have to move to more complex forms of digital management organization for all processes with due consideration of the human factor. Using the anthropocentric approach, the main factors that determine the reliability of IT employee ensuring functioning of energy systems during their digitalization, have been considered. A profile of the reliable employee, who is an empirically constructed set of qualitative characteristics inherent in personnel involved in the digital transformation of the power generation sector at all its levels.

1 Introduction

Energy sector of the XXI century is the basic part of the contemporary industrial complex. In the course of their development, power generation companies are faced with the problem of modernizing their own information structures to enhance the performance of big data processing [1, 2]. Currently, the cloud technologies facilitate the implementation of this task. The principle of cloud technologies operation is the use of third-party resources by clients, subject to the resources required:
for data storage, for creating one's own operating systems and applications and, up to the presentation of completely ready-to-use workstations.

In relation to the power engineering facilities the advantages of 'clouds' are the availability of information in the joint document flow for the facility state for different services monitoring the operating mode, defining the service life of the facility, scheduling repairs and replacement of devices when accessing databases that are structured in the 'cloud'. Taking into account the distributed nature of electrical devices in the distribution networks of different configurations, information exchange through the cloud structure is also an undisputable advantage. An important element is the ability to provide the required reliability for power facilities by specialized structures with the presence of additional power sources, security, professional employees, with continuous data backup, high resistance to DDOS-attacks.

As a result, cloud technologies are becoming increasingly important for power engineering companies with the ambition to grow and develop. The 'cloud' helps them get on-demand access to more data than ever before, and to increase computing capacity to obtain significant results and recommendations. There is a need to study the impact of cloud technologies and related processes on the safety of power engineering facilities functioning, with due consideration of their activities specifics [3].

Due to migration to the 'cloud', digitalization of energy sector occurs. The digitalization of energy can be called the basic part of the architecture of the 'Digital Economy of the Russian Federation' program, which is reflected in the passport of the 'Russia's energy sector digital transformation' program [4].

The aim of digitalization is to create a unified information environment and a common programming language. It includes the following benefits:
increasing automation and diagnostics levels; development of information infrastructure dedicated to data transmission; digitalization of innovation activities; development of human capital.

The demand for digital technologies among Russian energy companies is associated with the need for a considerable replacement of fixed assets in the domestic energy sector.

According to the decree of the President of the Russian Federation 'On national goals and strategic objectives of the Russian Federation development for the period up to 2024' [5], the power generation industry, being one of the fundamental life support systems covering the state needs, has to make a scientific, technical and socio-economic breakthrough. The development strategy of Russia's power grid companies, currently, consists in the comprehensive modernization

* Corresponding author: yrvaskon@mail.ru

of the power grid infrastructure using up-to-date electrical equipment and digital technologies.

A number of technological innovations, such as the Industrial Internet of Things, real-time information technology systems and solutions to optimize energy production and distribution, have given impact to global changes in the energy sector around the world, which have opened up new growth opportunities. In this regard, the problem of digital technologies' uniform standards development for the use in energy companies and ensuring cybersecurity, comes to the fore.

Studies show that energy companies could increase their capitalization by using a combination of several lines of digitalization [6, 7]. About 50% of energy companies executives say they are trying to effectively combine fast-growing technologies. However, only 9% of companies chief executives declare that their profit growth is due to digitalization and indicate the difficulty in measuring the effectiveness of investments in digital technologies.

The digitalization of energy systems, along with the solution of technical issues, the development of information infrastructure, implies the development of human capital in the formatting of new professional competencies in energy companies employees [8].

2 Safety issues of energy systems functioning

If we talk about cybersecurity in the course of digitalization, then it should be noted that the 'cloud' is exposed to the same threats as traditional infrastructures. It doesn't matter what kind of data you transferred to the 'cloud': whether it's a list of personal data or data of a utility company's consumers, they are all attractive targets for attackers. At the same time, the severity of potential threats directly depends on the importance and significance of the data stored. For energy facilities, this can be commercial information on tariffs and mutual settlements, tender purchases of expensive equipment, on the operation of relay protection and automation devices setpoints and algorithms, the change and violation of which can result in significant damage and even death. Thus, increased requirements are imposed on energy facilities with respect to information protection and cybersecurity.

An overview of information security threats during the power systems digitalization allows us to highlight the most important of them.

1. Inconsistency of the digitalization objectives with the real situation at the facility. The existing high energy intensity of the Russian economy, low rates of equipment renewal, high moral and physical wear and tear of fixed assets pose a threat to the energy facilities safety, on the background of violating the existing conditions for their functioning. In this case, the digitalization of individual parts of the power system complex equipment leads to an increase in the load on personnel, who, while performing their main functions, must simultaneously fend off all the shortcomings and unreliability of power systems equipment in order to preserve its operability. All this leads to an increase in the power facilities personnel role in ensuring their trouble-free operation, as well as the scientific justification of the operability and the limits of permissible actions of personnel in the real conditions of power systems operation [9].

2. The threat of data loss, when the necessary information from the cloud can permanently disappear. Note, that now, with the development of cloud services, cases of data loss without the possibility of recovery due to the service provider are extremely rare, but hackers may well set such a goal for themselves and achieve success.

3. Data leakage, which is often the result of negligence in authentication mechanisms issues, where weak passwords are used and encryption keys and certificates are not properly managed. In addition, energy companies encounter issues of rights and permissions management, whereby employees are assigned much more authority than it is actually required. The problem also occurs when an employee is transferred to another position or dismissed, in which case his account should be immediately deleted, but this rarely happens. As a result, the account contains much more capabilities than it is required. And this is a cybersecurity bottleneck. In addition, cyberthreat experts point out that one should always remember that hackers can be helped by an insider or he himself can be a hacker. This risk can come from current or former employees, system administrators, contractors, or business partners. Insiders-attackers pursue a different goals, ranging from data theft to just a revenge. In the case of the 'cloud', their aim may be to completely or partially destroy the infrastructure and gain data access.

4. Cyberattacks are possible that pose a threat of violation of the automation and relay protection functioning algorithms. Security threat analysis shows that cyberattacks are not uncommon these days. Possessing sufficient knowledge and a set of relevant tools, one can achieve a desired result. It is not so easy to detect an attacker who wants to establish and nail down his own presence in the target infrastructure. Cloud providers use advanced security tools to minimize risks and prevent such threats.

5. Other threats to domestic energy companies that have decided to use cloud technologies, include a lack of understanding of such decisions essence. If an entity switches to cloud solutions just because it is a current trend, without understanding cloud capabilities, then it encounters risks. For example, when the development team is not sufficiently familiar with the specifics of cloud technologies and the principles of cloud applications deployment, operational and architectural problems arise. In this case, security is at risk again.

6. Downgraded qualifications of employees. Digital transformation leads to a decrease in the personnel role, who are reduced to passive observers, which leads to downgrading of their qualifications.

7. Misuse of the advanced technologies advantages. The proliferation of IoT (Internet of Things), equipped with embedded technologies to interact with each other or with the external environment [10] and 5G networks,

contributes to the development of new technologies and applications, such as intelligent transport systems, intelligent electrical grids, 'smart city', 'smart home', virtual reality, geolocation, etc. However, IoT technology is becoming ineffective due to the increase in the number of devices equipped with various sensors, such as smartphones, tablets, smart home appliances, etc., which can read a large amount of data from the environment. In manufacturing, including energy sector, the Industrial Internet of Things (IIoT) is being developed – one of the most promising concepts in the global industry. This problem pushes developers to move into the era of IoE (Internet of Everything – the concept of intelligent connecting everything: people, processes, data and objects ('things')) [10, 11]. Compared to IoT, IoE is more oriented toward the intelligent communication of people, processes, data and devices, rather than communication between IoT devices. With the introduction of IoE technology at industrial facilities IIoE (Industrial Internet of Everything), edge network devices are getting transformed from consumers to data producers with huge information processing capabilities, such as data collection, pattern recognition and data mining. At the same time, edge devices are equipped with Internet applications providing the integration of user computing services with cloud data processing centers. But now it is high time to think about safety, especially at production facilities. IIoE offers unprecedented possibilities, but if used incorrectly, the likelihood of human-related threats increases.

Thus, the introduction of digitalization in the energy sector entails the above disadvantages, largely related to the human factor. Research results indicate that the human factor accounts for up to 90% of accidents and failures, which are caused by operator errors in the power facilities management [12]. Roughly 30% of equipment failures are also directly or indirectly related to the human error. The most common causes of errors are [12, 13, 14]: the lack of practical skills in active management in emergency situations, monotony in the operator's work, which reduce the acuteness of his reaction, reduce the situation-based thinking while leading to a loss of vigilance, insufficient level of professional training, discrepancy between personal (primarily psychophysiological) qualities and required ones, ergonomic shortcomings of technical systems. Largely unintentional actions are due to the fact that a person's capabilities are limited by the physiological properties of the its body and the psychological characteristics of each individual [15]. At the same time, the power systems digitalization increases the psychophysiological load on the employee due to the continuous increase in the complexity of the actions performed, their abundance of intellectual functions, an increase in the volume and intensity of data processed, and the indirect participation of a person in the systems operation.

To reduce the negative impact of the human factor, a proactive approach should be employed, which includes personnel recruiting in accordance with the profile of the reliable employee having appropriate qualifications. For the successful implementation of digital and technological transformation, a common security structure is required, which considers the human factor as well. Expert assessments show that work on probabilistic safety assessments cannot be considered apart from an integral assessment of human reliability [12]. Therefore, taking into account the human factor in the energy facilities digitalization, the management of which can be represented as human-machine systems, is a factor to increase the safety of energy systems functioning.

3 Approaches to improve safety when considering the human factor

[13, 14, 16] are referred to the main methods in eliminating the human factor in the energy facilities management in the course of their digitalization:

- Transfer of decision-making functions from the man to intelligent technical control systems.
- Taking into account the features of human interaction with technical systems, which implies taking into account the equipment ergonomic properties, as well as the conditions of human interaction with them: improving the structure of the human operator's activity, rational distribution of functions between man and machine, using the concept of an active operator, the machine adaptation to the man.
- Assessment of the main factors that determine the reliability of the human-operator, including the degree of engineering and psychological consistency of technology with the psychophysiological capabilities of the human-operator, the level of the operator training and fitness, his psychophysiological properties: features of the nervous system, sensitivity thresholds, health status, psychological constitution of the individual, etc.
- Human-operator state management based on social and psychological events.
- Professional and psychological selection, including a set of measures aimed at ensuring that persons who, in terms of the level of development of professionally important qualities, cannot master the profession in a timely manner and effectively perform their functional duties, should not be appointed to this position. At the same time, this procedure shall be used not only for hiring, but also personnel transfer, and must also be applied, if the employee has committed violations when operating and maintaining the technical system.
- Raising the level of personnel professional training. At the same time, a modern personnel training system should be carried out based on a two-stage cycle: the first – the study of equipment and technological processes, the rules of operation, the electrical installations and safety codes using specially developed computer programs and examiners, the second – training in the skills of operating in regular and emergency modes on specially designed simulators and digital twins, which adequately simulate both the operator workstation, and technological processes of power facilities.
- Periodic control of whether the employee has the necessary professionally important qualities as a

guarantee to prevent his dysfunctional behavior: incompetence, inconsistency with the position held, errors caused by this in the course of performing his functions that entail damage.

- Conducting specialized training for employees on recognizing hacker techniques, using advanced security tools, the ability to properly manage processes, on gaining knowledge about scheduled incident response, and applying preventive methods that enhance the cybersecurity level.

The importance of the human factor forms the tasks for the personnel selection, ensuring the safety of power systems functioning in the course of their digitalization.

4 Solving the problem of taking into account the human factor for purposes of safety improvement

To take into account the influence of the human factor on ensuring the energy facilities safety, it is important to understand how security threats are associated with an employee's certain personal qualities and characteristics. These circumstances made it possible to formulate an assumption about the possibility of constructing some generalized profile of an employee, who is 'reliable' for the control and maintenance of energy facilities.

Based on the study of theoretical approaches to assessing the employees reliability, its moral and ethical component, special methods used to assess the personnel reliability, stable characteristics were identified that correlate with the concept of a 'reliable employee'. All in all, six groups of characteristics were identified, forming its generalized profile: he knows and understands the rules and procedures for ensuring cybersecurity, has a commitment to a safety culture, is professionally reliable, does not suffer from various kinds of addictions, does not have an increased vulnerability to external environment, is morally and psychologically reliable (fig. 1).

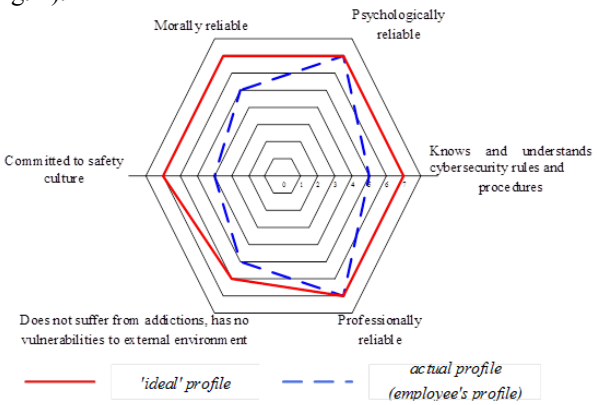

Fig. 1. Reliable employee profile model

Further, each group of profile characteristics was subjected to a detailed study, which resulted in a detailed description of the qualities, character traits, and behavioral features of the reliable employee. As a result, a detailed profile of the reliable employee was generated, which presents the most significant qualities, character traits and behavioral indicators that reveal his characteristics.

To analyze the obtained expert assessments of the values of characteristics maturity of the reliable employee profile, it is possible to use a scale with seven assessment values: complete characteristics immaturity; initial level of immaturity; under average level; middle level; the above average level of maturity; high level; complete characteristics maturity (fig. 2).

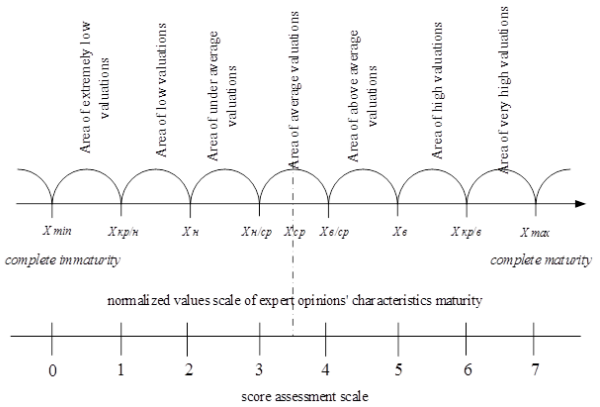

Fig. 2. Evaluation scale of values of the reliable employee's characteristics maturity

To determine the regions of the characteristics maturity, the following values are calculated: Xav – the arithmetic mean; Xmin – the minimum value; Xmax – the maximum value. Based on this data, the boundaries of the regions are determined.

The final assessment of the degree of profile characteristics maturity (S) can be determined using the formula:

$$S = \sum_{i=1}^{6} (Q_i \cdot k_i) / m,$$

where Q_i – the sum of points for the i-th profile characteristic, which are given by experts; k_i – the weight (significance) of this profile characteristic, which is assigned by experts; m – the number of experts who have assessed the degree of the profile characteristics maturity.

Thus, a profile of the reliable employee has been obtained – an empirically constructed set of qualitative characteristics inherent in an employee whose activities are safe for an energy facility in the course of its digitalization. Using this profile, the requirements for personal and professionally important qualities, the behavior of IT employees from the point of view of ensuring the cybersecurity of energy facilities can be meaningfully described and the degree of their manifestation can be assessed. The profile can be used at the stage of employee selection, in the process of personnel promotion and training, and is an effective tool for assessing an employee's reliability.

5 Conclusions

It is impossible to completely eliminate the human factor in managing and ensuring the cybersecurity of

energy facilities during their digitalization, at the same time, a better understanding of how human actions affect reliability and safety will make it possible to predict the influence of the human factor and help to improve the safety of the power systems functioning.

The analysis of the digital transformation development lines indicates that power generation companies have to move to more complex forms of digital management organization for all processes with due consideration of the human factor.

Using the anthropocentric approach, the main factors that determine the reliability of IT employee ensuring functioning of energy systems during their digitalization, have been considered. A profile of the reliable employee has been developed, which is an empirically constructed set of qualitative characteristics inherent in personnel involved in the digital transformation of the power engineering at all its levels

References

1. A.N. Kopaigorodsky, L.V. Massel, *Methods and technologies for data and knowledge storage construction for energy studies purposes* Research service in the Internet: supercomputer centers and problems: proceedings of International supercomputer conference 481-485 (2010)
2. V.L. Arshinsky, A.G. Massel, S.M. Senderov, Information technology *of intellectual support for research on energy safety problems* Bulletin of IrGTU **7 (47)**, 8-11 (2010)
3. A.M. Shaykhutdinov AM2015 *The possibility of using cloud technologies in energy sector Contemporary scientific research and innovations **2.P.3.***. [Electronic source] Available at: Unpubl URL http://web.snauka.ru/issues/2015/02/45646 (access date 02/02/2020)
4. Ministry of Energy site / Top news // *Passport of 'Russia's energy sector digital transformation' program has been approved* [Electronic source] Available at: https://minenergo.gov.ru/node/10859 (access date 01/10/2020)
5. *On National Goals and Strategic Objectives of the Russian Federation through to 2024* [Electronic source] Available at: https://minenergo.gov.ru/view-pdf/11246/84473 (access date: 5/25/2019
6. A.E. Mozokhin and V.N. Shvedenko, *Analysis of the directions of digitalization development of home and foreign energy systems* Scientific and technical bulletin of information technologies, mechanics and optics **19 No.4**, 657–672 Preprintdoi: 10.17586/2226-1494-2019-19-4-657-672 (2019)
7. Source: Site: *Power and industry in Russia – energy sector employee's information portal. How to hack the Cloud* [Electronic source] Available at: URL: https://www.eprussia.ru/epr/347-348/4553050.htm (access date 02/14/2020)
8. *Russia's energy sector digital transformation* Electronic source] Available at: http://digitenergy.ru/wp-content/themes/energy/img/materials-2018/2/5.pdf (access date: 5/25/2019
9. M.V. Pluzhnik, M.A. *Saprykina, Energy security and threats to its provision in modern Russian economy* Russian entrepreneurship **6 (238)**, 41-50 (2013)
10. Kevin Ashton *That 'Internet of Things' Thing. In the real world, things matter more than ideas. (Engl.)* RFID Journal (July 22, 2009) [Electronic source] Available at: URL: http://www.rfidjournal.com/articles/view?4986 (access date 12.06.2017)
11. V.V. Ryabokon', A.A. Kuzkin, S.Yu.Tutov, A.S. Mahov *Review of information security threats in the concept of edge computing* The Eurasian Scientific Journal [online] **3(10)**. Available at: https://esj.today/PDF/79ITVN318.pdf (in Russian) (2018)
12. B.P. Okorokov, R.V. Okorokov, *The role 'the human factor' in ensuring reliability and safety of energy facilities* Energy safety **1(39)**, 60 (2011)
13. M.V. Artyukhovich, O.G. Feoktistova, *The role of The role of the technical staff in the flight safety* MGTU GA science bulletin. **204**, 41 (2014)
14. S.I. Magid, E.N. Arkhipova, *'The human factor' and insuring reliability and safety in energy sector* Reliability and safety in energy sector **10** (2010)
15. A.M. Zavyalov, V.I. Apatsev, *Ensuring trains operation safety based on reduction of the human factor influence* Transport Egineering Sience **2**, 75 (2014)
16. A.I. Karmanchikov, A.A. Troynikova, *Prediction and optimal formation of human behavior in emergencies* Vector nauki (Science vector) TGU: Series: Pedagogy, psychology **4(19)**, 66 (2014)