Information security of power enterprises of North-Arctic region

O P Sushko
Northern (Arctic) Federal University named after M.V. Lomonosov, Severnaya Dvina Emb., 17, Arkhangelsk, 163000, Russia
E-mail: o.sushko@narfu.ru

Abstract: The role of information technologies in providing technological security for energy enterprises is a component of the economic security for the northern Arctic region in general. Applying instruments and methods of information protection modelling of the energy enterprises’ business process in the northern Arctic region (such as Arkhenergo and Komienergo), the authors analysed and identified most frequent risks of information security. With the analytic hierarchy process based on weighting factor estimations, information risks of energy enterprises’ technological processes were ranked. The economic estimation of the information security within an energy enterprise considers weighting factor-adjusted variables (risks). Investments in information security systems of energy enterprises in the northern Arctic region are related to necessary security elements installation; current operating expenses on business process protection systems become materialized economic damage.

1. Introduction
For present-day industries, especially those of strategic importance, such as energy providers, information technologies play an increasingly important role. While power engineering drives nations’ social and economic growth, electricity providers are seen as socially significant entities whose trouble-free performance is what all other sectors of economy depend on. Being the key constituents of a commonly shared infrastructure, energy providers may not subject their information infrastructure to restructuring or innovation. At the same time, the production processes of energy enterprises are complex. Accordingly, an important role is given to their automation and safety. In the context of the development of a threats to security of critical infrastructures. The tragedy at the Sayano Shushenskaya hydropower station is indicative as well as detection of the stuxnet malicious code at the Bushehr nuclear power plant in Iran, etc. The critical infrastructure security risk has been ranked very high on the ‘effect criticality’ scale, according to the annual risk report by Global Risks since 2007 as part of the World Economic Forum. That is why since 2011, Federal law № 256-FZ «On security of fuel and energy facilities» requires every energy enterprise to establish an information protection system [1].

Based on the authors’ analysis of the information security concepts being adhered to the electric energy providers operating in the North of Russia and the areas classified as High North areas of Russia, an observation can be made that the information security systems in place are rather weak. The conditions, in which the energy providers under analysis operate, are demanding, defined by northern climate. The cold climate requires them to produce enough energy to meet not only the electricity but
also the heating needs of the industries and the public. In some of the High North areas, they are required to produce energy for mining companies to ensure their trouble-free performance. In addition, the worn-out physical assets of the Northern Russia's power grid and the lacking investment in energy sector limit any further expansion of the grid, thus making it impossible to meet the area’s energy needs. The situation is further aggravated by the information security issues that the North Arctic Region’s electric energy providers are trying to solve. These include:

- insufficient protection of wireless networks and mobile devices;
- enterprises’ weak authentication systems;
- inadequate data cipher systems;
- low reliability of electronic signature systems and of contractor confidentiality;
- insufficient protection from viral or hacker attacks on electric energy companies;
- possibility of unauthorized data copying;
- lack of a commonly accepted ‘information security perimeter’.

The above mentioned information security challenges, faced by the North Arctic Region’s electric energy providers, can be tackled provided that a two-tier coordination system is in place – the one where the higher level would be occupied by national and international bodies responsible for information security standardization and cyber crime prevention, and the one that would be under constant attention of the CEOs of electric energy providers. While the lower level of this system would deal with the development of information security know-hows, the higher one would be more of executive nature. Within this system, the information security systems would have to be constantly audited and supported so that more protection applications could be developed in future. The company the authors have selected for evaluating the information security levels is Interregional Distribution Grid Company (IDGC) North-West, a leading energy corporation for North Arctic Region. Servicing an area of 1.4 mln sq.m, it operates seven branches – ArkhEnergo, VologdaEnergo, KarelEnergo, KolEnergo, KomiEnergo, NovgorodEnergo, and PskovEnergo. IDGC’s overhead and underground power lines have a total length of 175 000 km. [2].

A factor seen as a constraint in the development by energy providers’ of their information-related business processes is the security systems design lag. As a result, automation systems operators either say no to the use of the information security systems or, in case where such use is obligatory, spend a lot of time developing them. In the process of creating a digital society, a discrepancy exists between the need to speed up the upgrade of safe information technologies and the actual practice of designing the security systems for certain business entities. The design gap and the long time that enterprises spend creating their information security systems lead to an increased risk of economic damage. Among the goals of this study is to analyze the information security levels achieved by energy providers operating in North Arctic Region; to determine whether their information security levels meet reliability standards; and to define what further actions may be needed to upgrade information security levels in the context of the digital transformation the world community is undergoing. The study targets to explore the levels of information security – its performance and peculiarities – at the electric energy providers operating in North Arctic Region.

2. Methodology
Information security risks can be assessed using different methodologies, the two that are relying on threats and information flows modeling. By applying various tools and methods designed to simulate a business process-related information protection, the authors have identified and analyzed the most common risks calling for protective measures. In doing the qualitative and quantitative analysis of information system security, the authors made use of economic and mathematical methods. There currently exists no unified methodology for qualitative and quantitative risk assessment. When assessing risks in monetary terms, such costs as equipment purchase and installation, and personnel training costs should be taken into account.

At an early stage, the implementation of such projects, given there is insufficient information for making decisions, expert methods are effective. Quantity assessment of information risks was carried
out by defining their weighting coefficients with the analytic hierarchy process method, applied in multi-criteria assessment tasks [3].

Ten specialists from energy enterprises were involved as experts. Dedicated research demonstrated that this number of experts is sufficient to receive sustainable quantity evaluation of expert statements being averaged when applying the analytic hierarchy process method. Experts have a long-term experience in analyzing the applied aspects of energy enterprises' information security, as well as developing and adjusting these enterprises' information systems. The assessment of experts' work quality was based on the criterion of 'consistency', used in the analytic hierarchy process, which indicates a value of coherence relation at the level, not exceeding 10% statement deviations. The majority of expert statements fitted in this criterion, which confirms the high level of expertise.

3. Research and results
Stage one of the study involved the analysis of the software and hardware operated by IDGC, with greater focus placed on IDGC's branch ArkhEnergo and KomiEnergo [2]. They see the software and hardware it operates, especially its antivirus programs, as very critical to ensuring its information security. During the period from 2006 to 2007, ArkhEnergo and KomiEnergo faced repeated malfunction of its antivirus software Symantec [2, 4, 5]. Among the most common power data communication protocols in its use, there was the family of IEC 60870-5-101/104 [2], a standard developed with little attention paid to cyber security. It should be noted that the company uses a more recent version of the protocol – IEC 61850, which has not yet penetrated many of the Russian energy providers. Another thing to note is that the Russian energy providers tend to rely on their own, non-standardized protocols, as well as the in-built information security engines (authentication; access control; event logging; among others), which may not at all be in line with the present-day standards. Exposed to viruses that had spread within the company's local network, the obsolete software and the functionality-lacking protocols malfunctioned, causing ArkhEnergo and KomiEnergo to switch to the antivirus protection software by ESET, a global leader in antivirus software development [6]. Highly scalable, ESET NOD32 Business Edition allows for encompassing of up to one hundred thousand of users within a single structure, is compatible with all sorts of system resources, and boasts high-performance threat detection and scanning rate [2, 6]. This product's high malware detection reliability has been confirmed by tests conducted by outside teams such as Virus Bulletin, AV-Comparatives, and CheckMark. All this made IDGC's ArkhEnergo opt for ESET NOD32 Business Edition and install 570 suites in its local offices to protect file servers and workstations from viruses, Trojans, worms, spyware, adware, phishing attacks, rootkits, and other Internet-related threats [6, 7].

Another factor to be considered by North Arctic Region's electric energy providers, including ArkhEnergo, when developing their information security systems or selecting the protection software, is that the asset to be protected is not information per se but a process technology. It is meant here not the conventional protection from data leakage but the protection of a process technology from cyber attacks [7]. A security system should therefore be built based on the principles of integrity and accessibility of a process technology and on the automated enterprise control system in place (Figure 2).

Figure 1 shows some of the viral threats, the most dangerous being information theft (leakage). Yet, in the light of ArkhEnergo’s and KomiEnergo’s recent information security trends, scheduled work is in process to upgrade the information security systems only in some of ArkhEnergo’s divisions, not in the entire company. Even where information security unit forms part of the IT Service, the official responsible for information security policy would be a deputy director for security, a position to be gradually introduced in many of IDGC North-West’s affiliates [2].
When it comes to production facilities and information processes, it is important to take into consideration the nature of APCS (Automatic Process Control System) in general and the electric power engineering-specific systems in particular (control systems, telemechanics, relay protection and automatics, electricity metering, and others). When designing the information security system, it is essential for the asset to be protected and for the process technologies (with all their nuances) to be explored and analyzed in every detail.

Today, the OS built-in anti-malware protection alone no longer looks an ample protection. The majority of larger companies are now looking into composite data protection systems that employ not only dedicated software but also the full-package hardware and software suites for safe data storage, processing and communication within a business’s information security perimeter. Among the producers of such composite systems are InfoTeCS and InfoWatch [4, 5].

Stage two of the study will involve the quantitative and qualitative risk analysis. It is designed to estimate the probability of and the extent to which information risks may affect the company. It is expected that this analysis will also define the economic consequences the risks may entail.

The weighting coefficient values are indicated in the table, calculated with the analytic hierarchy process. For more convenient comparison, every value is multiplied by 100, i.e., expressed in percentage.

| №  | Risks                              | Weighting coefficient |
|----|------------------------------------|-----------------------|
| 1  | Unauthorized copying of data       | 25.2                  |
| 2  | Virus attacks, Trojans             | 15.2                  |
| 3  | DDoS attacks                       | 21.8                  |
| 4  | Wireless Security                  | 12.3                  |
| 5  | Losses from the activities of insiders | 10.2              |
| 6  | Mobile Security                    | 15.3                  |
The authors’ analysis of IDGC’s information security levels involved the elaboration of a risk prevention action plan (Table 2). The authors’ task is also to calculate the expenditure the company would have to sustain in order to eliminate or mitigate the damage from the information risks.

### Table 2. Characteristics of Information Security Risks of ArkhhEnergo and KomiEnergo

| Name of risk                        | Risk identification (risk level) | Brief description of risk                                                                 | The cost of eliminating the risk (costs of equipment, software, operating costs, etc.) |
|------------------------------------|---------------------------------|------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------|
| Unauthorized copying of data       | $X_1$                           | The ability to copy the organization’s internal information to removable media             | $Z_1$                                                                                |
| Virus attacks, Trojans             | $X_2$                           | Unauthorized access to data, data loss                                                     | $Z_2$                                                                                |
| DDoS attacks                       | $X_3$                           | Suspension of the organization’s web services                                              | $Z_3$                                                                                |
| Wireless Security                  | $X_4$                           | Access to the wireless LAN segment of the enterprise, receiving data transmitted over the wireless channel; Access to mobile devices of employees | $Z_4$                                                                                |
| Losses from the activities of insiders | $X_5$                       | Data transferred between employees, partners and contractors                              | $Z_5$                                                                                |
| Mobile Security                    | $X_6$                           | Network attacks on mobile devices, access to processed data                                 | $Z_6$                                                                                |

The primary risk assessment being completed, the authors ranked the risks according to their severity (low, moderate, high) for energy providers’ business processes. Below is the formula the authors followed when assessing IDGC information security risks:

$$RA = X_1Z_1k_1 + X_2Z_2k_2 + X_3Z_3k_3 + X_4Z_4k_4 + X_5Z_5k_5 + X_6Z_6k_6 = \sum_n X_n Z_n k_n \quad (1).$$

Variables in this formula are the above mentioned risks (assets’ susceptibility to risk) and the risk elimination expenditure, corrected for the coefficients calculated by experts using the points-based system. The effort to provide the information risk evaluation will be justified provided that the optimum size of the investment needed by the protection systems is defined. This investment should be such that it ensures minimal expenditure and maintains the energy provider’s level of profitability. In fact, any investment into information security systems mainly targets installation of the essential security elements, whereas the operating expenses to keep the business processes protected may turn into actual economic damage [10, 11].

The final stage of the study will involve the development of an operation algorithm for the security system of business information protection of the North Arctic Region’s energy provider – a set of information security services, and security software and hardware.

### 4. Conclusion

Provided that there is the unpromising forecast of increasing risks for critical infrastructure and emerging trends of enhanced state regulations related to energy enterprises security, the energy industry becomes most promising from the perspective of information security solutions implementation. The findings of this study are indicative of the fact that the economic conditions, in which electric energy providers operate, continue to be unfavourable. This and the unstable macroeconomic situation have lead to lower levels of contractors’ payment discipline and made
borrowed capital much more expensive. Provided that there are the limited fundraising opportunities and the excessively worn out physical assets, energy providers channel their funds primarily to the needs of the electric energy infrastructure refurbishment and upgrade, whereas their IT infrastructure is often funded with whatever funds remain, which should not be the case in a Smart City environment. The fact that energy providers’ business information security will suffer can be evidenced by the current projections, which forecast an increase in the risks, to which the strategically important infrastructure facilities may be exposed. Once the economic evaluation of the energy providers’ business information security is completed, it will be possible to estimate the economic damage from the information risks and the expenditures related to their prevention, so that energy providers could channel their efforts to what constitutes the most risk-sensitive elements. The next stage of this study will involve the development of the energy providers’ information security evaluation algorithm. The authors will also provide a rationale for differentiating the types of information security solutions, based on the security services available.

References
[1] Ministry of Energy of the Russian Federation 2018 (URL: https://minenergo.gov.ru/)
[2] Interregional Distribution Grid Company (IDGC) of the North-West "Rosseti" 2018 (URL: http://www.mrsksevzap.ru/)
[3] Saati T, Kerns K 1991 Analytical planning. Organization of systems (M.: Radio and Communication)
[4] InfoTeX 2018 (URL:https://infotecs.ru/)
[5] InfoWatch 2017 (URL: https://www.infowatch.ru/)
[6] ESET 2017 (URL:https://www.esetnod32.ru/business/)
[7] A Guide to Risk Management for Information Technology Systems Recommendations of the National Institute of Standards and Technology / Extended abstract on materials: NIST Special Publication 800-30 Risk Management Guide for Information Technology Systems; Recommendations of the National Institute of Standards and Technology et al 2002 p 20 (URL:http://csrc.nist.gov/publications/PubsSPs.html#800-30)
[8] RS BR IBBS-2.2-2009 2010 Ensuring information security of organizations of the banking system of the Russian Federation Methodology for assessing the risks of information security breaches et al (Moscow)
[9] Semenov Y A Direction and tendencies of development of IT-technologies (URL: http://book.itep.ru/4/7/resources.htm)
[10] Voitic A I and Prozherin V G et al 2012 Economics of information security (SPb.: NIIT ITMO)
[11] Shushkov G M, Sergeev I V 2016 Topical issues of scientific and scientific-pedagogical activity of young scientists (Moscow: IIU MGOU)