Economic Evaluation of the Information Security Levels Achieved by Electric Energy Providers in North Arctic Region

O P Sushko¹, A A Kaznin¹, A V Babkin² and D A Bogdanov³

¹Northern (Arctic) Federal University named after M.V. Lomonosov, Severnaya Dvina Emb., 17, Arkhangelsk, 163000, Russia,
²Peter the Great St. Petersburg Polytechnic University, Politechnicheskaya st., 29, St. Petersburg, 195251, Russia,
³Arkhenergo, "IDGC of the North-West", Free st., 3, Arkhangelsk, 163000, Russia.

E-mail: o.sushko@narfu.ru

Abstract. The study we are conducting involves the analysis of information security levels achieved by energy providers operating in the North Arctic Region. We look into whether the energy providers’ current information security levels meet reliability standards and determine what further actions may be needed for upgrading information security in the context of the digital transformation that the world community is undergoing. When developing the information security systems for electric energy providers or selecting the protection means for them, we are governed by the fact that the assets to be protected are process technologies. While information security risk can be assessed using different methods, the evaluation of the economic damage from these risks appears to be a difficult task. The most probable and harmful risks we have identified when evaluating the electric energy providers’ information security will be used by us as variables. To provide the evaluation, it is necessary to calculate the costs relating to elimination of the risks identified. The final stage of the study will involve the development of an operation algorithm for the North Arctic Region’s energy provider’s business information protection security system – a set of information security services, and security software and hardware.

1. Introduction
For present-day industries, especially those of strategic importance, such as energy providers, information technologies (hereinafter referred to as ‘the IT’) play more and more 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.

With internal cohesion and non-market income, the nature of power engineering is specific. Being the key constituents of a commonly shared infrastructure, energy providers may not subject their information infrastructure to restructuring or innovation.

Their workflows are complex and it is important that they are properly automated. In terms of process automation and IT support, power engineering is middle-ranking [1, 2] as compared to other branches of industry, which is due to Russia’s power engineering sector’s financial and economic performance.

Since electric energy is mostly consumed by industries, any growth in energy production will coincide with the overall economic growth (Table 1).
Table 1. Economic and technical performance characteristics achieved by Russian power engineering sector in 2015 – 2017 [1]

| Characteristic                                           | 2015       | 2016       | 2017, projected |
|---------------------------------------------------------|------------|------------|-----------------|
| Index of production, % against previous year            | 105.7      | 104.2      | 103.6           |
| Level of profitability, %                               | 5.3        | 3.8        | 3.8             |
| Share of loss-making enterprises, %                     | 53.8       | 50.1       | 48              |
| Share of actively innovating enterprises, %             | 4.0        | 4.2        | 4.5             |
| Index of innovativeness (volume of innovative products in the total output), % | 0.08       | 0.1        | 0.15            |
| Index of investment in IT awareness among workforce (IT knowledge upgrade costs per employee), RUR/person | 50.1       | 70.2       | 150             |
| Index of IT-intensity, %                                 | 0.64       |            |                 |
| Employee’s IT availability (PCs per 100 employees), %    | 5          | 16         | 20              |
| IT infrastructure integratedness index (number of PCs integrated into LAN), % | 70.2       | 76.6       | 80              |

Judging by the above performance, a statement can be made that energy providers’ business processes should receive wider IT support and automation.

2. The purpose of the current study into energy providers’ information security
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 enterprises spend creating their information security systems lead to an increased risk of economic damage. Among the goals of our 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.

3. Brief overview of recent information security studies
In performing our study, we relied on the practical achievements and the project designs available in the field of information security. Scientists in Russia and worldwide contributing to the theory and practice of information security system design, efforts are now being channeled into upgrading and developing the adjustable smart systems to support the information security of business processes. Shushkov, G.M. and Sergeev, I.V. define information security as “a process of establishing a balance between the emerging, affecting threats and the efficiency of the public authorities responsible for national security in countering them” [3]. Among investigators of information security is the highly reputable team of researchers Ernst&Young. Its annual reports since 2002 focus on the core IT-related risks, the basic trends in and the concepts of information security management, facilitating adequate decision-making [4].

4. IT risks analysis methodology
There exists a variety of concepts adhered to by different industries in setting up their information security. Pertaining to corporate networks and systems, all of them vary only to a small extent. The main international standard of information security which is adhered to globally is ISO/IEC 27001, developed
in cooperation with the International Organization for Standardization and the International Electrotechnical Commission and revised in 2013. It contains requirements to designing, developing and maintaining information security management systems (ISMS). [4]. ISO 27001 is governed by the following key principles: information confidentiality, information integrity, and information accessibility.

The recommendations developed by National Institute of Standards and Technologies on IT risk management (NIST Special Publication 800-30) contain a classical risk calculation formula [5]:

\[ R = S \times P(t) \]  

(1)

where:
- \( R \) is the degree of risk;
- \( S \) is the extent to which a threat may influence an asset (the value of an asset on qualitative and quantitative rating scale);
- \( P(t) \) is the probability for information security threat to actually occur (a combination of qualitative and quantitative rating scale) [4].

The degree of risk is ultimately expressed in relative units and can be ranked in terms of its significance for information security risk management procedure.

Unlike NIST 800-30, the Guidelines for software documenting management GOST R ISO/IEC TO 7 provide for the risk calculation that relies on three, not two, factors, the third factor being the probability of vulnerability [6].

“Information Technology – Security Techniques” (BS 7799), the national standard developed in Great Britain in 2005, determines risk levels based on the sum total of three indicators (asset value; threat level; and vulnerability level). Consequently, the overall risk is proportionate to the contribution by each of the indicators [7].

In 2009, in response to the Russian Federation’s need in information security for banking institutions there has been developed the Bank of Russia’s Standard (RS BR IBBS-2.2-200), which suggests a uniform approach to how banking organizations’ information security systems should be configured. This Standard provides for a two-stage security evaluation using quality and quantity ranking scale [8].

An important step in the evolution of information security systems is the emergence of electronic performance support systems (EPSs), first created by American software developers and experts in the late 21st century. The North American EPSs provide a description of the cyber security infrastructure for electric energy systems [2]. Later, the issues of electricity providers’ IT security systems development were moved upwards to a supranational level: a number of cooperative networks have been set up to maximize the reliability of all the systems, including information ones.

As can be seen from the above, in regulating the information security of their business processes Russia and the world are using their own standards. However, in the light of recent virus-containing cyber attacks in Europe and America, the international standards have proved weak, manifesting the need in further upgrade of information security systems.

Information security risks can be assessed using different methodologies, the two commonest relying on threats and information flows modeling. By applying various tools and methods designed to simulate a business process-related information protection, we have identified and analyzed the most common risks calling for protective measures. In doing the qualitative and quantitative analysis of information system security, we 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.

5. The study into the IT security levels achieved by electric energy providers operating in North Arctic Region: stage one preliminary conclusions

Based on our analysis of the information security concepts being adhered to by 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
the energy providers under analysis operate in are demanding, defined by northern climate. The cold climate requires them to produce enough of 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 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 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 we 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.

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 [2]. ArkhEnergo sees 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 faced repeated malfunction of its antivirus software Symantec [2]. Among the most common power data communication protocols in its use 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-standardization 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 to switch to the antivirus protection software by ESET, a global leader in antivirus software development (Figure 1) [9]. 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 [9, 10]. 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 [2, 9].
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. We mean here not the conventional protection from data leakage but the protection of a process technology from cyber attacks [9]. 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 2 shows some of the viral threats, the most dangerous being information theft (leakage). Yet, in the light of ArkhEnergo’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 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; among others). When designing the information security system it is essential that both the asset to be protected and the process technologies (with all their nuances) 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 [10,11]. Among the producers of such composite systems are InfoTeCS and InfoWatch.

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. We expect this analysis to also define the economic consequences the risks may entail.

Our analysis of IDGC’s information security levels involved the elaboration of a risk prevention action plan (Table 2). Our 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. The primary risk assessment completed, we ranked the risks according to their severity (low, moderate, high) for energy providers’ business processes. Below is the formula we followed when assessing IDGC information security risks:

$$RA = X_1Z_1k_1 + X_2Z_2k_2 + X_3Z_3k_3 + X_4Z_4k_4 + X_5Z_5k_5 + X_6Z_6k_6 = \sum_n X_nZ_nk_n$$ (2)

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 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 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 [11, 12, 13].
Table 2. Characteristics of Information Security Risks of Arkhhenergo

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

6. Final remarks
The findings of our study are indicative of the fact that the economic conditions in which electric energy providers operate continue to be unfavorable. This and the unstable macroeconomic situation have lead to lower levels of contractors’ payment discipline and made borrowed capital much more expensive. Given 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 case in a Smart City environment. That energy providers’ business information security will suffer can be evidenced by the current projections that forecast an increase in the risks the strategically important infrastructure facilities may be exposed to. Once the economic evaluation of the energy providers’ business information security is completed, we will be able 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 our study will involve the development of energy providers’ information security evaluation algorithm. We will also provide a rationale for differentiating the types of information security solutions, based on the security services available.

References
[1] URL: https://minenergo.gov.ru/, last accessed 2017/03/27.
[2] URL: http://www.mrsksevzap.ru/, last accessed 2017/03/27.
[3] Shushkov G M, Sergeev I V 2016 Topical issues of scientific and scientific-pedagogical activity of young scientists (Moscow: IIU MGOU) pp 69 – 76
[4] URL: http://www.ey.com/ru/ru/home, last accessed 2017/03/27.
[5] 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

[6] GOST Information technology. Classification of software tools. Information technology. Categorization of software 2002 (Moscow) p 20

[7] BS 7799-2:2005 Specification of information security management system et al 2005 (England) p 58

[8] RS BR IBBS-2.2-2009 Ensuring information security of organizations of the banking system of the Russian Federation Methodology for assessing the risks of information security breaches et al 2010 (Moscow) p 20

[9] URL: https://www.esetnod32.ru/business/, last accessed 2017/03/27.

[10] URL: http://book.itep.ru/4/7/resources.htm

[11] Voitic A I and Prozherin V G et al 2012 Economics of information security (Saint-Petersburg: NIIT ITMO) p 120

[12] URL: https://infotecs.ru/, last accessed 2017/03/27.

[13] URL: https://www.infowatch.ru/, last accessed 2017/03/27.