Identification of Critical Objects in Reliance on Cyber Threats in the Energy Sector

Aleksei Massel and Daria Gaskova

Information Technologies in the Energy Sector Melentiev Energy Systems Institute of SB RAS Irkutsk, Russia
amassel@isem.irk.ru, gaskovada@isem.irk.ru

Abstract: The article describes the identification of critical facilities being a significant trend in researching critical infrastructures, particularly in the energy sector. Cyber threats are believed to be important contemporary threats to energy security in Russia. The authors formulated the risk-based approach to support decision-making in the identification of critical facilities in the energy sector in terms of cyber threats. The novelty of the study lies in the development and application of a fractal stratified model of the relationship of risks, energy facilities, and technologies. This author's approach allows one to identify all the hidden relationships of the influence of cyberthreats on energy objects.The results of the proposed approaches are used and supported by an intelligent decision support system.

Keywords: intelligent system; risk management; cyber threats; risk-based approach; critical infrastructures; energy facilities

1 Introduction

Any military actions are primarily targeted at destructing civil infrastructure which might cause the damage comparable with the blows hitting military forces.

Scientific research and applied developments on complex problems on safeguarding of population, infrastructure units, and life activity environment were described by A. Kondratjev, N.A. Makhutov and S. A. Timashev.

In fact, the problems of ensuring the safety of population and technosphere objects are multidisciplinary [1], and their solution assumes the acquisition of new data on all components through fundamental research carried out in proper areas [2].

Critical infrastructures include complex technological systems, which are believed to be unique technogenous objects. Modeling and investigation of the safety of such systems are reported in the paper by [1]. As a rule, the study of the security of such systems is intended at developing the methods on system analyses, representation and processing of information on the objects. Such information reflects knowledge of experts, collected data and knowledge, mathematic models and others by applying methodologies of investigations, as well as the proposed information environment.

Modeling is executed via recognizing alternative solutions for reducing risk of reliability and safety violations. To add, because such systems bear risks for population and environment, it is vital to consider malfunction of the systems, which might result in the origination of extreme situations and cascade accidents.

The conception of risks is based on the identification of the current status of the elements of the system and conditions of origination and development of extreme, accident and disastrous situations qualitative and quantitative description of the scenarios and consequences of achieving limit conditions causing accidents and disasters [2].

1.1 Management of Risks

The design of critical information infrastructure is aimed at ensuring reliability and safety, and the sources of risk are represented by catastrophic failures and equipment errors, natural impacts on the facility, or deliberate actions of operators. An important component of the information and technological process of modern production are information flows, making IT risk management a priority area of risk management.

IT risk management integrates technologies used to identify, analyze evaluate the incidents and threats, as well as implement security enhancements [3].

Four major components of risk management, indicated in the literature, are [4]:

- risk identification,
- risk analysis,
- risk-reducing measures,
- risk monitoring.

For the purposes of information security risk assessment, the qualitative risk analysis is usually carried out in the Information System [4]. Qualitative methods are provided as descriptions and recommendations; these approaches include scenario analyses, surveys, and audits.

IT risk management of corporate information technologies plays an important role in many aspects of the modern organization functioning, and the key task of such management is risk analysis [3], [4], [5]. This task becomes especially urgent in the context of energy security (ES), under conditions of preparing infrastructure projects both for reorganization and expansion of energy network to meet the national electricity needs [6] and low-carbon energy transition projects. In most cases, they are based on renewable energy sources [7] requiring the introduction of new technologies. This problem is aggravated by the underestimation of the safety of introduced new technologies represented by intelligent information systems, technical equipment, and devices. Thus, the current tendency is to enter service-oriented and cloud-based corporate technologies in industrial production [8], [9]. Control systems based on these technologies include online data analysis and processing, real-time monitoring of devices; they are capable to be flexible and integrated. However, the absence of adequate management of cybersecurity risks can have serious consequences not only for the enterprise itself but also for the environment within a city, region or nationwide.

In this paper, cyberthreats are considered in the context of a strategic analysis of critical infrastructures. The introduction of new information technologies often carries significant risks and uncertainties, intangible benefits, but provides attractive long-term financial benefits, and can be considered in the framework of strategic project management [10]. Management and control, and possible ways of adapting, if necessary, are provided at the monitoring stage by the project and are favorable to identify potential risks and their adverse effects, as well as developing the ways to eliminate or minimize them.

1.2 Critical Infrastructures

Critical infrastructure is part of civil infrastructure, which makes up a combination of physical or virtual systems and means that are important for the country, as their malfunction or destruction can trigger disastrous consequences in the fields of defense, economy, health safety and nation security [11].

Awareness of the importance of ensuring cybersecurity came first in the west. For example, in 2015, the US Department of Defense prepared the final version of the «Cybersecurity Strategy» [12]. In the US, the Department of Homeland Security allocates 16 critical infrastructures [13].

The investigations of critical infrastructure and, in particular, identification of critical facilities (CF) are a focus area in many countries and primarily in the United States. It can be reasoned by progressively increasing the development of new information technologies and the capacity of modern simulation complexes. Critical facilities of the RF infrastructure are the key objects (or their combinations) of infrastructures, when being affected might violate (or terminate) their functioning, thus causing loss of control, destruction of infrastructure, irreversible negative changes (or failure) of the economy of RF or its subject, or its administrative-territorial unit. The energy systems are surely referred to as the critical infrastructures [11].

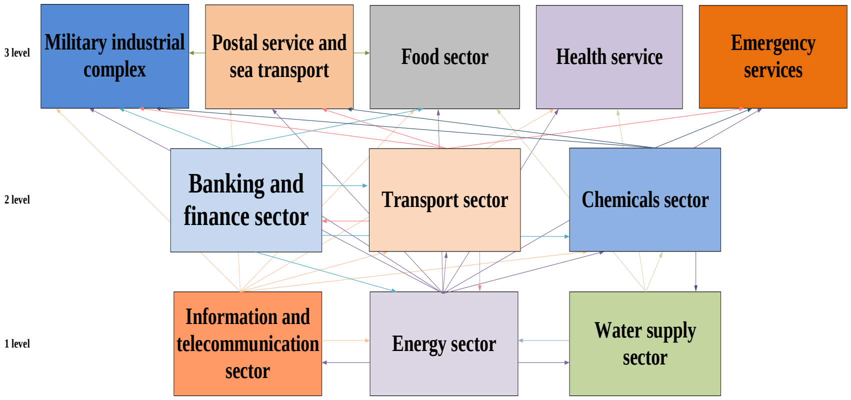

Figure 1
Critical infrastructures

As energy is regarded as critical infrastructure (Figure 1) [11], it is vital to identify critical facilities in the energy sector. In 2012 EMERCOM of Russia approved the «Methodology of attributing governmental and non-governmental proprietary objects to critical objects of the Russian Federation national security». Thus, the methodology for the formation of the list of gas transmission network CF has been provided [14]. It focuses on gas, being the energy system, and its transportation. The authors of the methodology proposed an indicator to locate critical facilities in the gas transportation network, which is determined by the relative gas shortfall to consumers (5% or more) because of the malfunction of these facilities. In this methodology ranking objects by the degree of significance for the country's economy in general and its individual regions is disregarded. The authors propose to perform ranking through the analysis of possible critical situations (CS) and taking into account the risks of the CS.

1.3 Energy Sector

The energy sector combines power plants and energy systems, including energy transporting main lines [15].

Energy security (ES) makes up a significant part in the Russian national security. ES threats are traditionally grouped as: (1) economic, (2) social-political, (3) technogenous, (4) natural and (5) managerial-legal. This threat list was supplemented with the cybersecurity threats [16], their implementation possibly provoking serious emergency situations in the energy fraught with a drastic reduction of energy resources to be provided to consumers [17]. The development of the Smart Grid conception in Russia exacerbates the problem of cybersecurity in energy.

Engineering systems are commonly designed, constructed, and operate under unavoidable conditions of risk and uncertainty; they are often expected to achieve multiple and conflicting objectives. The overall process of identifying, quantifying, and assessing risks should represent an integral and explicit component of the overall managerial decision-making process [18]. In the energy sector, the decision-making process is deteriorated by the complexity of the target area, difficulty to adequately model the energy facilities, availability of multiple criteria, and large-scale computational experiments [19].

For instance, the electric power facilities are complex structures with a multitude of equipment elements designed both for the main technical process and for ensuring its protection, the safety of maintenance personnel, and consumers of electrical energy. The operating capacity of generators, transformers, transmission lines, engines, electro-technological installations, and things is characterized by a variety of reliability indexes disregarding possible cyber-attacks onto the network or software or employee negligence.

In relation to these reasons, the authors propose to employ a risk-based approach to support decision-making in the identification of critical facilities in the energy sector subject to cyberthreats.

2 Methodology for Identifying the CF

Correct identification of critical facilities in the energy will reduce risks of financial losses in the event of damage or destruction of energy facilities, and also will facilitate the continuous supply of energy products to a consumer. The rapid spread of the computer environment, development of information technologies and the tendency of transition to intelligent energy make the cyber threats the most notable tactical threats of ES. Consequently, in June 2017 a series of cyberattacks have been undertaken in the Russian and international energy, telecommunications and financial companies and organizations. The cryptoware actions, among other things, caused failure in the functioning of the fuel station network. Serious consequences were avoided due to switching to the reserve management system.

In the energy sector, the validity of decisions is exacerbated by the need to process and comprehend large amounts of information belonging to several subject fields. To facilitate this task, the authors suggested developing an intelligent decision support system (DSS). Intelligent DSS is a complex of software tools for data analysis, modeling, forecasting, and decision-making.

In the energy sector, the identification of the CF is to be performed through several stages, as shown in Figure 2.

At the first stage (1) determine the criteria to affiliate the power facility to the CF. Criteria could be related to both the scale of fuel consumption and life quality within the region. A full set of objects is to be determined to solve the task of the CF identification within the country, region, municipality or some other territorial units.

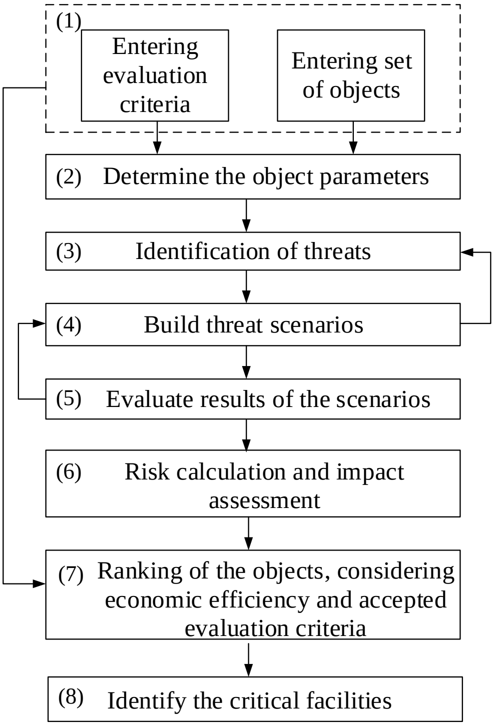
(1)
Entering evaluation criteria
Entering set of objects
(2) Determine the object parameters
(3) Identification of threats
(4) Build threat scenarios
(5) Evaluate results of the scenarios
(6) Risk calculation and impact assessment
(7) Ranking of the objects, considering economic efficiency and accepted evaluation criteria
(8) Identify the critical facilities

Figure 2
Identification of the CF stages

(2) Typify the object, make up its safety certificate and identify the vulnerability of cybersecurity via organizational, institutional, technical, and the operation procedures.

(3) Having information on the object and its vulnerability we establish the links between vulnerabilities and possible cyberthreats, considering the pre-existing preventive measures against security breaches.

(4) Build threat scenarios for each object or simulate some critical situations involving several objects, e.g. cascade failure.

(5) Evaluate results of the scenarios. An expert selects either most probabilistic scenarios or those meeting criteria for evaluation. It is also feasible to identify

frequently-involved objects in various scenarios and the most vulnerable assets in the scenarios for one object.

(6) Calculate and visualize the risks for each object on a risk map to be further analyzed by experts.

(7) Perform a ranking of energy facilities based on the calculated risks, considering economic efficiency and accepted evaluation criteria.

(8) Finally, identify the CF and make further decisions to ensure preventive countermeasures from the CS.

3 Risk-based Approach

The authors offer the risk-based approach to support the decision-making to ensure cybersecurity in the energy sector. This approach considers harm from damage or demolition of the object using quantitative and qualitative parameters, as well as probability for further damage or destruction of the object components, tailored to extent of damages and cascade failure. The formula of risks consists of three components (1),

$$R = \{T, V, D\}, \tag{1}$$

T – threat, V – vulnerability, D – damage by threat realization.

Threats are defined through the probability of event occurrence triggering critical situations. Cyberthreats might cause the subsequent implementation of the other ES threats. Cyberthreats might initiate scenario events; and final events are responsible for the consequences and determine the damage. The risk-based approach is aimed at developing scenarios for threat implementation leading to critical situations in the energy sector.

A scenario is represented by the set of conditions leading to a threat implementation and threats proper. In this context such conditions could be:

- an event is the threat realized, i.e. with a 100% probability of occurrence.
- consequences are threats to energy security or estimated losses of the energy facility assets.
- operating conditions of the information technology system affecting the threats involved in the scenario.

It is reasonable to apply the Bayesian networks to build cyber threat implementation scenarios using conditional probability.

The approach involves a description of the facility information technology system and further assets detailing. The asset contains vulnerabilities, which can be both critical and not dangerous. The vulnerability criticality level is proposed to be determined following risk management standards [20], and using expert ranking. Vulnerabilities are classified in the work [21]. The authors offer in this work classification is made by subject area: general vulnerabilities, vulnerabilities related to information systems, and the ones specific to the energy sector.

Previously, the methodology for analyzing threats and assessing the risk of information technology security violations of the energy complexes was proposed [22]. In this methodology, the risk-based approach involves the risk analysis at various levels of the energy facility. The transition from the upper levels to the lower ones is accompanied by detailed elaboration and refinement of both the risk assessments and the representations about the object, its information technology system, and its domains. Having got the estimates received at detailed levels establishing feedback will allow adjusting the results obtained at the upper levels. This approach can be projected in the case of risk analysis and vulnerability assessment of several objects. The risk ranking of the objects is proposed to be implemented using risk scales, and on this basis to determine the critical objects. The solution of this task is specific and requires a lot of elaboration and detailing of the energy infrastructure under investigation. At this stage, we only assess risks of its facilities, rather than entire energy infrastructure.

This model is formulated through the fractal approach [19]; it will be described in the next section.

The asset vulnerabilities are determined from the databases and vulnerability banks, e.g. [23].

Damage is estimated for each consequence as the economic efficiency of the scenario. Economic efficiency is understood as the ratio between available risk assessments of the onset of critical situations, expressed in monetary units, and the cost of selected countermeasures with the evaluation criteria on hand.

4 Fractal Stratified Model of Interaction between Energy, Risks and Technologies

The fractal approach represents the subject field as a collection of information layers and their reflections from any layer to each one [19]. In this case, the energy (E) can be stratified into several levels and affiliate each level with the category of risk. Regarding ontology of the fuel and energy complex (FEC) of Russia such levels are: energy systems (Es), energy objects (Eo), and information technology systems (Ei), taking into account their subspecies (2).

$$E = \{Es, Eo, Ei\} \tag{2}$$

Therefore, as follows from (3), the risks (*R*) are stratified into groups (R_g), species (R_k), subspecies (R_s) and risks (*r*).

$$\mathrm{R} = \{R_g, R_k, R_s, r\} \tag{3}$$

Also, the fractal approach is applied to information technologies implementing a risk-based approach. To identify the energy object vulnerabilities it makes sense to use an expert system and databank created for ontologies. The data is further transferred to the Bayesian Belief Networks to construct the threat implementation scenarios. The result of the expert work with the scenario is supplied to the risk assessment and risk maps. This approach is described as set of methods (4):

$$M = \{M_o, M_p, M_b, M_r\}, \tag{4}$$

where M_o is ontology modeling, M_p is structuring personal knowledge structure, M_b is Bayesian Belief Networks technology, M_r is the risk assessment method.

Every information technology is a specific layer. For the user of an intelligent system, work with layers is performed sequentially, but the feedback is possible with any layer passed to refine the data or to reassess them.

Figure 3 presents the fractal stratified model of energy sector risk assessment in terms of the proposed approach.

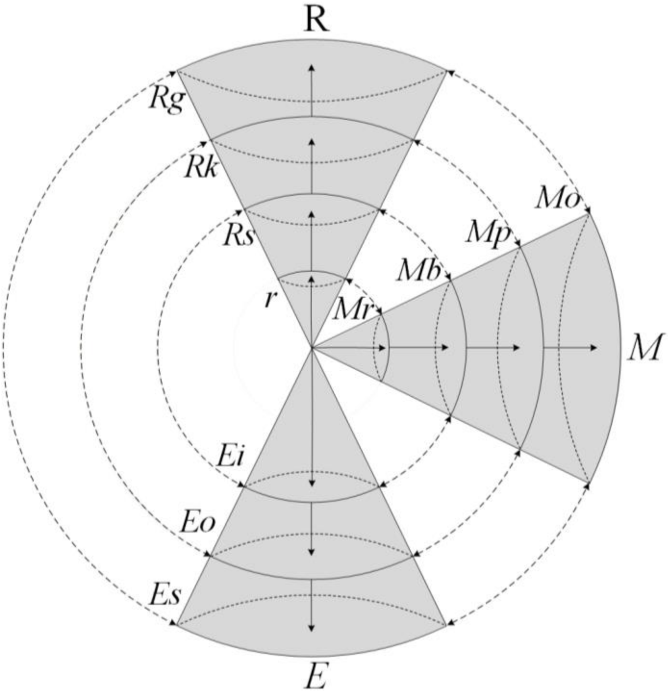

Figure 3

Fractal stratified model of interaction between energy, risks and technologies

5 Intelligent Decision Support System

At present, the structure of the intelligent system given in Fig. 4 is being designed. It consists of three interrelated components: (1) an expert system for supporting threats vector building, (2) the Bayesian network for modeling threat scenarios, and (3) the module for assessing the risk of cybersecurity violations, which includes visualization as a risk map. Besides, the researched prototype for the system described above has been made. The intelligent system is intended to support decision-making in the CF identification in the energy sector cyberthreats considered. It is being designed using a risk-based approach.

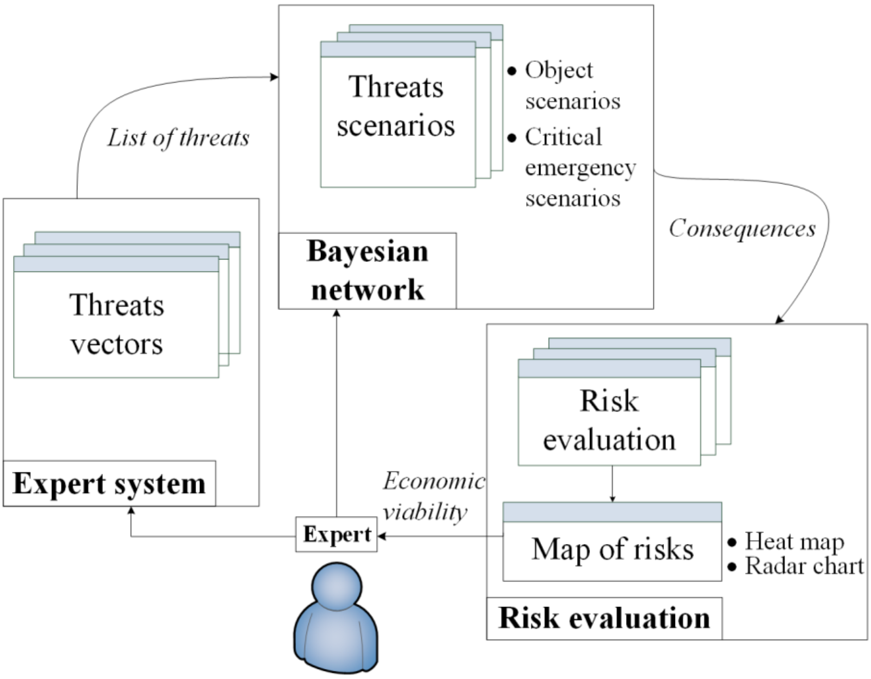

Figure 4
Structure of intelligent system

The expert system serves to obtain data on the energy facility and to make up threats vectors including penetration vector, attack vectors, and cybernegligence. For this purpose, an expert can use information about the information technology system, management, and legal internal standards, as well as the operational functioning of the facility. Having obtained the user information, the templates are filled to identify any relationships between the vulnerability of the object and the threat. The information in templates is wired to the Bayesian network component so that the user could construct the probabilistic scenarios of the extremal situation in energy. The work with a scenario results in locating the impact of cyberthreat group implementation on the energy facility assets, leading to the implementation of other energy security threat groups. Information on the consequences of the implementation of the threat is transferred to the risk assessment component. This component consists of the calculated and visualizing components. The intelligent system work results in the determination of economic efficiency for each energy object considered, and also in the ability to rank objects.

The intelligent system means to support decision-making in the CF identification on the basis of constructing scenarios of possible extremal situations including critical situations and evaluating their significance by the groups of parameters. At present, the energy sector is very much concerned with emergency situations. The definition of a particular situation assumes assessment of the system state or objects through the scale: "norm", "pre-crisis" - a critical situation, "crisis" - an emergency situation. With this in mind, the critical situations are referred to the situations when something threatens a uninterrupted functioning of the technical objects and the objects of life support and/or the life or health threats of individuals or social (professional) groups [16].

The application of the intelligent system allows the expert to build up possible critical situations, based not only on his own experience, but also on those identified by the IDSS for the CF of energy determination, and regarding the scenarios provided by the other experts.

Conclusions

The article reports the energy sector as the critical infrastructure and important part of national security. Because of the lack of any approved methodology to identify CF in critical infrastructures and the trend of introducing modern information and communication technologies in the energy sector, the authors propose to apply the risk-based approach with modeling and analysis of critical situations arising from the implementation of cyberthreats. It is necessary to develop an intelligent system for the risk assessment of cybersecurity violations due to feasible cyberthreats with the risk-based approach and methodology of threat analysis and risk assessment applied.

Acknowledgment

This work was partially supported by RFBR grants №18-07-00714, №19-07-003514, №19-57-04003. The authors are grateful to this organization.

References

[1] Berman A. F., Nikolaychuk O. A., Yurin A. Yu., Pavlov A. I. A methodology for the investigation of the reliability and safety of unique technical systems // Journal of Risk and Reliability. Proceedings of the Institution of Mechanical Engineers. – Vol. 228, 2014 – pp. 29-38

[2] Makhutov N. A, Gadenin M. M. Ensuring the safe operation of technosphere and population facilities using risk criteria // Abstracts of the

XXI International Scientific and Practical Conference on the problems of protecting the population and territories from emergency situations. – 2016 – pp. 137-146 (in Russian)

[3] Rot A. IT Risk Assessment: Quantitative and Qualitative Approach // Proceedings of the World Congress on Engineering and Computer Science WCECS 2008, 2008, San Francisco, USA

[4] Rot A. Enterprise Information Technology Security: Risk Management Perspective // Proceedings of the World Congress on Engineering and Computer Science 2009, Vol. II WCECS 2009, 2009, San Francisco, USA

[5] Allodi L. Massacci F. Security Events and Vulnerability Data for Cybersecurity Risk Estimation // Risk Anal. – 2017 – T. 37 – № 8– 1606–1627pp.

[6] Battaglini A., Komendantova N., Brtnik P., Patt A. Perception of barriers for expansion of electricity grids in the European Union // Energy Policy 47 (2012) – pp. 254-259

[7] Schinko T., Komendantova N. De-risking investment into concentrated solar power in North Africa: Impacts on the costs of electricity generation // Renewable Energy 92 (2016) – pp. 262-272

[8] Lojka T., Bundzel M., Zolotova I. Service-oriented Architecture and Cloud Manufacturing // Acta Polytechnica Hungarica. - Vol. 13, No. 6, 2016 – pp. 25-44

[9] Chen J. Zhu Q. Security as a Service for Cloud-Enabled Internet of Controlled Things Under Advanced Persistent Threats: A Contract Design Approach IEEE Trans. Inf. Forensics Secur. – 2017 – T. 12 – № 11– 2736–2750pp.

[10] Jovanovic F., Milijic N., Dimitrova M., Mihajlovic I. Risk Management Impact Assessment on the Success of Strategic Investment Projects: Benchmarking Among Different Sector Companies // Acta Polytechnica Hungarica. Vol. 13, No. 5 (2016) – pp. 221-241

[11] Kondrat'ev "The current trends in research of Critical Infrastructure in foreign countries". №1. Foreign Military Review, 2012, pp. 19-30 (in Russian)

[12] Cyber Strategy // The Department of Defense, 2015 [Online] URL: https://defence.ru/document/61/

[13] Critical Infrastructure Sectors // Official website of the Department of Homeland Security [Online] URL: https://www.dhs.gov/critical-infrastructure-sectors

[14] A. V. Edelev, S. M. Senderov, I. A. Sidorov "The use of distributed computing to identify critical objects of the Russian gas transmission

network”. №1. Information and Mathematical Technologies in Science and Management, 2016, pp. 55-62 (in Russian)

[15] N. I. Voropai. Reliability of power supply systems. - Novosibirsk: Science, 2015 -208 p.

[16] Massel L., Massel A. Cyber security of Russia's energy infrastructure as a component of national security. / Proceeding of the International Conference on Problems of Critical Infrastructures, 6th International Conference on Liberalization and Modernization of Power Systems. Edited by Z. A. Styczynski and N. I. Voropai. 2015. C. 66-72

[17] Nazir S. Assessing and augmenting SCADA cyber security: A survey of techniques / S. Nazir, S. Patel, D. Patel // Comput. Secur. – 2017 – T. 70– 436–454c.

[18] Yacov Y. Haimes. “Systems-based risk analysis”. In: “Global Catastrpphic Risks” Nick Bostrom, Milan M. Cirkovic (ed), Oxford, 2008, pp. 146-163

[19] Massel L. V. “Fractal approach to he structuring of knowledge and examples of its application”. Vol.6, № 2 (20). Ontology of designing, 2016, pp. 149-161(in Russian)

[20] Draft International Standard ISO/DIS 31000 «Risk management – Principles and guidelines on implementation», ISO, 2008

[21] Young A. L., Yung M. Cryptovirology // Commun. ACM – 2017. – Vol. 60 – № 7 (2017) – P. 24-26c.

[22] Massel A., Massel L. The current state of cyber security in Russia's energy systems and the proposed activities for situation improving / Proceeding of the International Conference on Problems of Critical Infrastructures, 6th International Conference on Liberalization and Modernization of Power Systems. Edited by Z. A. Styczynski and N. I. Voropai. 2015, C. 183-189

[23] Data Security Threats Database of the FSTEC of Russia [Online] Available: http://bdu.fstec.ru/