SCENARIO APPROACH FOR ANALYZING EXTREME SITUATIONS IN ENERGY FROM A CYBERSECURITY PERSPECTIVE

Aleksei Massel, Gaskova Daria
Information Technologies in the Energy Sector, Melentiev Energy Systems Institute of SB RAS, Irkutsk, Russia
e-mail: amassel@gmail.com, gaskovada@gmail.com

***Abstract**: The article describes the approach based on the Bayesian networks for construction of probabilistic scenarios to simulate extreme situations in the energy sector. The paper proves the feasibility of using Bayesian networks to simulate energy security threats caused by the implementation of cyber threats. The main components of the scenario and their interrelations are described. The main stages of modeling extreme situations in the energy sector are determined. The position of the scenario approach in the main stages of identifying critical objects in the case of energy is recognized.*

1. Introduction

Critical infrastructures are regarded as large complex systems of strategic scale on the one part, and as cyber-physical systems on the other. In research of critical infrastructures, a large number of works are based on Simulation modeling, including Agent-based Modeling, Discrete-event Modeling, Dynamic Modeling, Structural Modeling, and Semantic Modeling [1], which involve Bayesian networks, Markov processes, Petri nets and Ontology-based Modeling [2].

Critical infrastructures are deemed to be part of the civil infrastructure, which is a collection of physical or virtual systems and means that are important to the state insofar as their failure or destruction can lead to disastrous consequences comparable to impact on military establishment [3]. Energy security protection is the national security part of the country [4], equally as energy sector is a one of the main critical infrastructure [5].

In the energy sector, the digitalization is primarily reflected in the Smart Grid, which is designed to expand the existing capabilities of generation, transmission and distribution systems, and to provide an infrastructure capable of meeting future needs for distributed generation, renewable energy sources and demand management [6]. The introduction of digital technologies increases the risks of security violation given the current move introducing new more complex solutions into the technological process of the energy facility, coupled with advent of new object business models, which are often undeveloped in terms of security. The above factors are contributing to receive incomplete and unreliable information for decision making, that are exacerbated by the dynamic nature of energy systems and their large physical infrastructure.

Under the "Digital Economy of the Russian Federation" programme approved by Government Order No. 1632-p of 28 July 2017 the main concepts of digital economy is highlighted. The authors consider ones as the whole new level of the Smart Grid in Russia.

The introduction of new information and communication technologies provokes the creation of new risks in the cyber environment of energy facilities.

There are many groups of international safety standards applicable to the energy industry such as CIP, NISTIR, etc. [7]. Since 2018, Federal Law No. 187-fz of 26 July 2017 "On the Security of the Critical Information Infrastructure in the Russian Federation" entered into force in Russia. However, a unified regulatory framework in the field of ensuring the cybersecurity of energy facilities in Russia has not been formed at the moment.

Risk management is traditionally applied for cybersecurity protection [8]. The transition from traditional methods and systems for providing strength, resource and reliability, to methods of risk assessment and management is the results of fundamental and applied research on the problems of technogenic security and risks [9].

The energy security threats are traditionally grouped as: (1) economic, (2) social-political, (3) technogenous, (4) natural and (5) managerial-legal [10]. This threat list was supplemented with the cybersecurity threats [11], their implementation possibly provoking serious emergency situations in the energy fraught with a drastic reduction of energy resources to be provided to consumers. The cyber threats are the least studied of these threats groups.

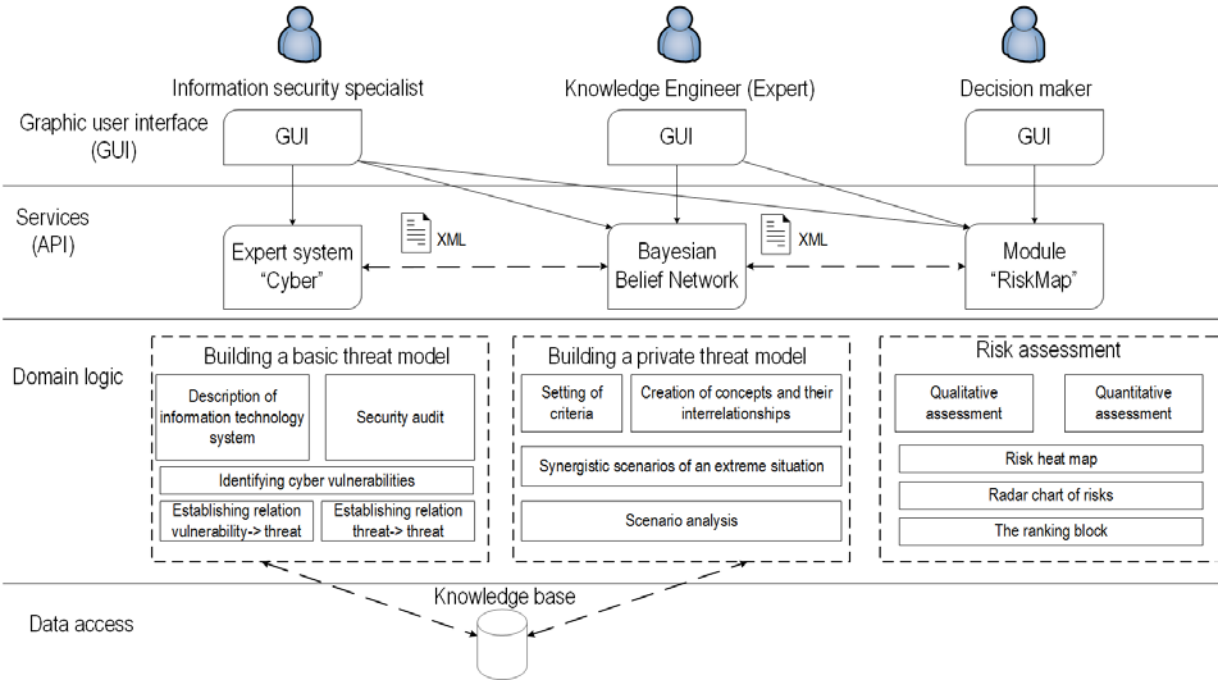

***Fig. 1.** Structure of intelligent system*

2. Intelligent system for threat analysis and risk assessment of cybersecurity violations in energy facilities

Cyber threats could lead to realization of other energy security threats. Since information technologies are dynamic in their development the tendency of constant appearance of new vulnerabilities and ways of their use is undeniable.

The intelligent system is now under development [14] with a view to investigate possible circumstances of energy security violations caused by the implementation of cyber threats. Figure 1 shows the general structure of the intelligent system.

The development objective of the intelligent system for threat analysis and risk assessment of cybersecurity violations in energy facilities focuses on:

- auditing code for security vulnerabilities and the most probable cyber threats (trivial attacks);
- building of probability scenario of extreme situation resulting from cyber threats activities on site;
- extreme situation risk assessing;
- detecting critical facilities using the risk ranking of extreme situation.

The intelligent system includes a set of three main components: 1) the expert system for conducting security audits in an enterprise and identifying critical cyber vulnerability of the information technology system of the facility; 2) the block of Bayesian networks for the analysis of vulnerabilities, threats (cybernetic, threats to energy security and external threats to the environment and objects external to the object under consideration) and the consequences from their implementation, which together lead to an extreme situation; 3) and the block of risks assessment of extreme situation.

The component of the Bayesian networks outlined in this paper is a tool for analyzing possible extreme situations in the energy sector and cybersecurity-wise. The next section of the article presents a scenario approach for analyzing threats leading to an extreme situation in the energy sector and justifying its applicability.

3. Opportunity analysis of using the scenario approach for research critical infrastructures

The original scenario approach arose from social systems studying. The specificity of scenario planning lies in consideration of simultaneously by several alternative option, for each of which internal and external factors are determined, criteria and indicators are established, and risks are estimated [15].

Usually, scenarios represent a probabilistic description of a possible or desirable the development variant of the phenomena and processes under consideration. The reaching of preferred states and situations in the form of course of action requires building development plans and making managerial decisions based on the scenarios analysis [15].

The development scenario of a complex system includes models, which contain significant factors that can be formalized with an acceptable degree of accuracy [16]. In case of extreme situations in the energy sector, the scenario is a pessimistic assessment of the main

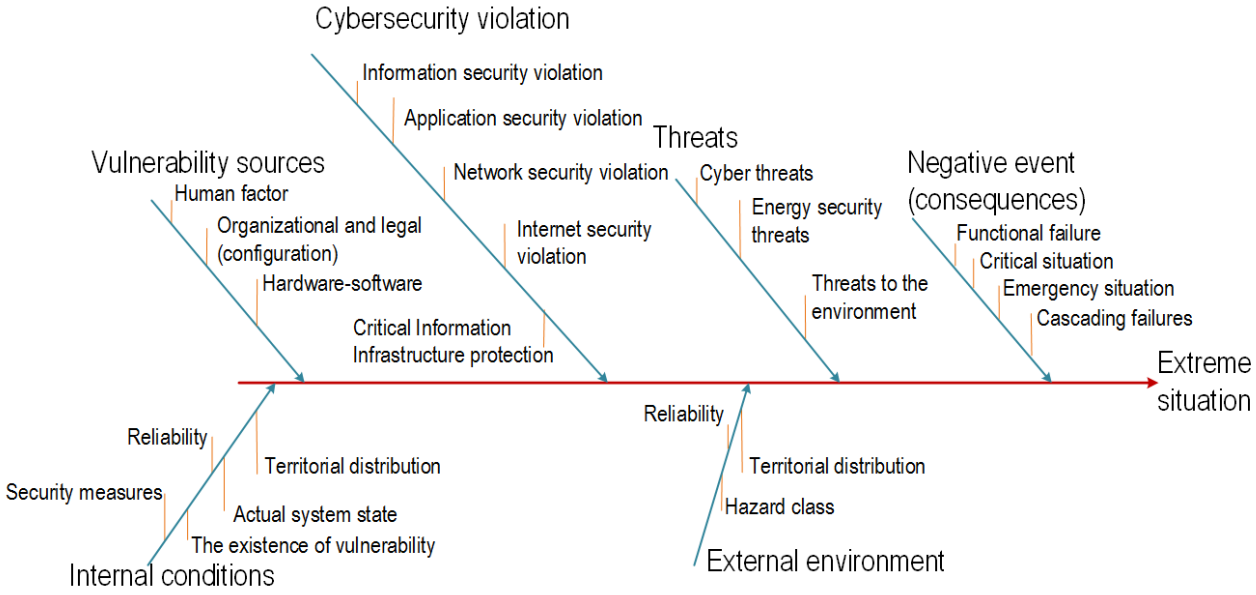

Fig. 2. *Extreme situation caused by the implementation of the cyber threat at the energy facility (in Cause and Effect Diagram notation)*

quantitative characteristics of energy facilities under implementing the threats chain: “cyber threats-energy security threats-threat to the external environment (and / or cascade accident)”.

The advisability of using sign-oriented graphs to generate scenarios of complex systems is justified in [16]. One also describes the requirements for the mathematical device for modelling activities under the scenario approach:

- the possibility of constructing computationally effective analysis algorithms;
- low requirements (sensitivity) to the completeness and accuracy of the initial data;
- the possibility of a relatively simple software-system implementation.

The Bayesian network is proposed to construct such models. The Bayesian network is a graphical model of probabilistic and cause-effect relations between sets of variables, which is a directed acyclic graph whose vertices represent variables, and the edges show conditional dependencies between variables [17].

The Bayesian networks were formerly used to analyze threats to energy security [18]. The Bayesian network is a suitable tool for implementing a scenario approach in the framework of strategic planning. The application of Bayesian networks allows building models of extreme situations using either Bayesian probabilities in case of numerical values based on the expert’s knowledge and

experience or frequency probabilities in the presence of statistical data, which often absent from free access.

Scenario analysis of risks using for investigation of complex systems is characterized by the absence of a “mass” nature of events in the scenario, and is aimed at studying unique situations and relationships [16].

4. Scenario approach

The proposed scenario approach promotes the research of extreme situations that might emerge on complex technological objects of power engineering. This approach also allows analyzing and generating scenarios of negative events leading to extreme situations and consequences from them. The results of scenario analyzing use to further justify decision-making and choose measures to ensure both the cybersecurity of the local facility and the energy security of the territory under consideration in the context of targeted (cyberattack) or accidental (cyber negligence) impacts on the information technology system of the energy facility.

The extreme situations are considered as both emergency situations and critical situations in studies on energy security. The definition of a particular situation is based on indicative analysis and 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 an 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. These threats can be eliminated by adopting appropriate preventive and operational measures that will not allow the critical situation to develop into an emergency situation, in which operational and liquidation measures are needed [19].

Figure 2 presents the structure of the extreme situation and the main cause-effect concepts.

The scenario represents the conjunction of the chain of energy security threats that with a certain probability might flow from implementing cyber threats. This model also takes into account the conditions for the onset of negative events and the consequences that lead to damage.

Modeling the extreme situation begins with the identification of cyber vulnerabilities at the energy facility with the involvement of specialists (information security specialist). The objective of this stage is to create “vulnerability-threat” and “threat-threat” chains, that reflecting the trivial (predictable) attacks and behavior of the cybersecurity offender. An expert (a knowledge engineer in energy security) further continues to work with the chains by adding “threats-consequences” part. Subsequently, the concepts are concretized and scenarios are formed using the Bayesian network. Scenario includes the following groups of concepts:

- factors for negative consequences or conditions softening them;
- vulnerabilities of the information technology system of the energy facility;
- cyber threats posed by successful use of cyber vulnerabilities by the attacker;
- energy security threats caused by the implementation of cyber threats;
- threats to the environment caused by the implementation of cyber threats to the investigated facility;
- consequences using for further definition of damage and risk assessment of extreme situation.

Figure 3 illustrates the example of exploiting vulnerability scenario named “Remote code execution”, which is considered on an industrial server.

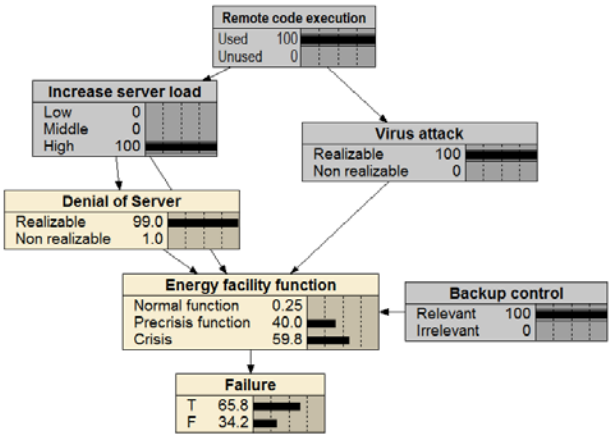

Fig. 3. “*The remote code execution” vulnerability scenario using the Bayesian network in the Netica*

This vulnerability can be exploited in several ways such as conducting a virus attack, embedding web shells, or conducting a Dos attack.

A virus attack can be aimed at either stealing information and disrupting the operation of an industrial server or using its resources for instance by including it in the Botnet network. This usually occurs for the purpose of sending SPAM (so-called black SEO), or to implement DDos attacks on other resources or Mining.

Scenario analysis will enable the expert to identify vulnerabilities that are most likely to be used by an attacker, a chain of threats that will have the greatest impact on the occurrence of negative consequences, and the consequences themselves and their probabilistic assessments. The above factors influence the risk of an extreme situation and the amount of damage from it. The information obtained in the scenario analysis is further suggested to manage risks and to develop protective measure.

5. Conclusions

The article describes some aspects of the energy sector as a critical infrastructure the security of which lies in the national security of the country. The scenario approach is proposed for predicting and analyzing possible failures, accidents and catastrophes as a result of the implementation of cyber threats. The scenario approach is aimed at the analysis of extreme situations in the energy sector as part of the development of intelligent system. The paper considers the main aspects of the extreme situation in the energy sector taking into account cybersecurity. In addition, an example of exploiting vulnerabilities is developed in the “Netica” software environment.

Acknowledgement

This work was partially supported by RFBR grants № 18-37-00271, №16-07-00474, №18-07-00714, №17-07- 01341. The authors are grateful to this organization.

References

1. L.V. Massel, A.G. Massel. “Semantic technologies based on the integration of Ontological, Cognitive and Event modelling”, III International Science and Technology Conference “OSTIS-2013” Minsk, 2013, pp. 247-250 (in Russian).
2. M. Rybnicek, R. Poisel, M. Ruzicka and S. Tjoa, “A Generic Approach to Critical Infrastructure Modeling and Simulation”, International Conference on Cyber Security “CyberSecurity” Alexandria, VA, USA, 2012, pp. 144-151.

3. L. Barannik, S. Klementev, “Organization of critical infrastructure security in the U.S.”. No. 8. Foreign Military Review, 200, p. 3 (in Russian).

4. V.I. Rabchuk, S.M. Senderov, G.B. Slavin, “Energy Security in Russia: Problems and Solutions”, Novosibirsk: ESI SB RAS, p. 197, 2011 (in Russian).

5. A. Kondratev “The current trends in research of Critical Infrastructure in foreign countries”. No. 1. Foreign Military Review, 2012, pp 19-30 (in Russian).

6. S. Sridhar, A. Hanh, M. Govindarasu, “Cyber-physical system security for the electric power grid”. Vol. 100. No. 1. Proc. IEEE, 2012, pp. 210-224.

7. L.V. Massel, A.G. Massel, “Cyber security of Russia’s energy infrastructure as a component of national security,” 6th International Conference on Liberalization and Modernization of Power Systems, 2015, pp. 66-72.

8. V.V. Mohor, A.M. Bogdanov, A.S. Kilevoj, “Information Technology. Methods of security. Cybersecurity manual (ISO/IES 27032:2012),” Three-K Kiev, 2013, p. 129, (in Russian).

9. N.A. Mahutov, N.V. Abrosimov, M.M. Gadenin, “Provision of safety - the priority in the sphere of fundamental and applied research”. No. 3. “Economic and Social Changes: Facts, Trends, Forecast”, 2013, pp. 39-61 (in Russian).

10. N.I. Pyatkova, V.I. Rabchuk, S.M. Senderov, M.B. Cheltsov, “Energy Security in Russia: Problems and Solutions”, Novosibirsk: SB RAS, 2011, p. 211 (in Russian).

11. L.V. Massel, N.I. Voropai, S.M. Senderov, A.G. Massel, “Cyber Danger as one of the strategic threats to energy security,” Cybersecurity issues, No. 4 (17), 2016, pp. 2-10 (in Russian).

12. Positive Research 2017. Collection of research on practical safety. 2017. Available at: https://www.ptsecurity.com/upload/corporate/ru-ru/analytics/Positive-Research-2017-rus.pdf (accessed 07.07.2018). (in Russian)

13. “WannaCry in industrial networks: work on mistakes”, Report of Kaspersky Lab, 2017. Available at: https://ics-cert.kaspersky.ru/reports/2017/06/08/wannacry-in-industrial-networks/ (accessed 07.07.2018). (in Russian).

14. A.G. Massel, D.A. Gaskova, “Application of risk-based approach to identify critical facilities in the energy sector with regard to cyber threats”, Proceedings of the 19th International Workshop on Computer Science and Information Technologies. Germany, Baden-Baden. Publisher Ufa: USATU, Vol. 1, 2017, pp. 159-163.

15. K.A. Feofanov, “Scenario capabilities of modern forecasting and management”, Vestnik MSTU “Stankin”, No. 4, 2009, pp. 126-132 (in Russian).

16. V.V. Kulba, V.L Schultz, A.B Shelkov, “Information management. Part 2: Scenario approach”, National Security / Nota Bene, No. 4, 2009, pp. 4-15 (in Russian).

17. D. Heckerman, “A Tutorial on Learning with Bayesian Networks”, Technical Report MSR-TR-95-06, Microsoft Research, March, 1995, p. 57.

18. L.V. Massel, E.V. Pyatkova, “Application of Bayesian Networks for the intelligent support of Energy Security problem researches”, Proceedings of Irkutsk State Technical University, No. 2, 2012, pp. 8-13 (in Russian).

19. L.V. Massel, A.G. Massel, “Technologies and tools for intelligent support of decision-making in extreme situations in energy”, Computational Technologies, Vol. 18, No. S1, 2013, pp. 37-44.