Methods to Analyze Critical Facilities in Energy with Regard to Cyber Threats

Daria A. Gaskova[1], Aleksei G. Massel[2]

Melentiev Energy Systems Institute of Siberian Branch of the Russian Academy of Sciences,
Lermontov str., 130
Irkutsk, Russia
[1] *E-mail: gaskovada@gmail.com*

[2] *E-mail: amassel@gmail.com*

Abstract

The article describes the methods proposed by the authors used for the analysis of critical facilities in the energy sector, taking into account cyber-threats. The authors focus on to an approach that enables analyzing and simulating the entire chain of events "Vulnerabilities – Cyber-threats – Energy Security Threats – Consequences." This approach can be used in the development of an intelligent system to support decision-making on the identification of critical energy facilities in strategic planning from the point of view of cybersecurity violations.

Keywords: Critical facilities, cyber-threats, semantic modeling.

1. Introduction

At a time of informatization in all areas of modern society the need to protect of information, information systems and databases, data transmission networks and hardware-software complexes of the organization was focus area in many countries and primarily in the United States [1]. Security violation and infliction of damage can be caused both by malefactor's attacks to IT-resources of the organization and deliberate or negligent acts of employees [2]. The state of such protection is commonly referred to as Cybersecurity, which is based on: Applications Security, Information Security; Network Security, Internet Security and Critical Information Infrastructure Protection according to the standard ISO 27032: 2012, but – isn't their synonymous. The latter is included in many countries worldwide in the priority research of critical infrastructure, as their failure or destruction can trigger disastrous consequences in the fields of defense, economy, and health and nation security [1].

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 [3], which involve Bayesian networks, Markov processes, Petri nets and Ontology-based Modeling [4].

Energy is regarded as a main critical infrastructure and energy security (ES) is important part of national security [1, 5]. A key feature of the cybersecurity breach lay in possibly disrupting normal functioning, down to destruction, both intangible and physical objects by influencing them from the cyber environment.

The identification of critical facilities (CF), in particular in the energy sector, is a major task in critical infrastructures investigation. In 2012 EMERCOM of Russia approved the "Methodology of entities assignment of state and non-state property to critical facilities of the Russian Federation national security". Thus, the methodology for formation of the register of gas transmission network CF has been provided [6] using the methodology approved. It focuses on gas, being the energy system, and its transportation.

In July 2017, Federal Law № 187-FZ "About the Security of the Critical Information Infrastructure of the Russian Federation" was adopted. Under this law, the critical information infrastructure (CII) consists of information systems, information and telecommunication networks, and industrial control system among other in energy. The detection of the facilities in critical information infrastructures is performed with the facility significance by categorizing based on social, political, economic, environmental significance, as well as significance from the point of view of the country's defense, state security and law and order.

Currently in Russia Smart Grid develops within the framework of the digital energy conception, which is part of the "Digital Economy of the Russian Federation" program. It aims at improving the level of reliability and automation of various processes in the energy sector.

Even though the strategy of cybersecurity in Russia has not yet been adopted, in the Strategy of scientific and technological development of the Russian Federation one of the priority directions of Russia's development for the next 10-15 years is counteraction to threats (technogenic, biogenic, sociocultural, terrorism, extremism) and also cyber threats [7]. Notably the state apparatus stresses the need to involve the scientific community in the implementation of directions.

The energy infrastructure is understood to be both a Big Complex Strategic-scale System (BCSS) and a Cyber-Physical System (CPS) considering that energy sector is transforming to the Smart Grid at normative-legal, software-hardware, and organizational levels. The key feature of critical infrastructures is their strong interdependence. Interdependencies can be classified into cyber, geographic, physical and logical interdependencies. Cyber-interdependence includes all interdependencies between (information) infrastructure components that are linked through information and communication relations. Interdependencies based on proximity are classified as geographic. If there are physical relations to other infrastructures then infrastructures are physically interdependent. All other relationships can be classified as logical interdependencies [4].

The authors present methods for analyzing critical infrastructures by the case of energy, which used to simulate extreme situation (ExS) in the energy sector caused by the cyber threats activities on the analyzable energy facility (EF) in this article. Future directions for research aim at the development of methods for identifying critical facilities by analyzing their resistance to the implementation of cyber threats.

The article discusses the critical facilities analysis by applying the assessment of information technology (IT) system protection of energy facilities from cyber threats including EF territorial criterion, the possible impact from nearby critical infrastructures, and the likelihood of cascading failures.

2. Analysis of critical facilities

The research of critical infrastructures is an multicriteria problem, which involves the identification of critical facilities of each infrastructure separately and their mutual influence. The identification of CF is proposed to be performed through three stages:

- (1) stage of identifying vulnerabilities and threats of IT system of EF,
- (2) stage of threat analysis using semantic modeling,
- (3) stage of assessing risk of cybersecurity violations in the critical information infrastructure.

At the first stage (1) determine vulnerabilities of analyzable EF. The stage consists of selection of such EF, description and establishment of interrelations between them and revealing typical vulnerabilities of the IT system of each EF for a target area. Facilities are divided into objects of generation, transportation and consumption of energy. At this stage, methods of ontological modeling, expert system technologies and methods of geovisualization are used.

Ontologies, which proved to be successful tools for energy security research [8], allow to describe the subject area (EF structure, EF assets, etc.), clarify the main definitions, and determine the classification of vulnerabilities and threats. Presently, a common ontological space of vulnerabilities and threats of the EF IT system is actively creating.

The research prototype of rule-based expert system “Cyber” is developing to support the stage. The purpose of developing the expert system expert system is to identify common vulnerabilities of the industrial control system (ICS) of the facility and to associate them with trivial threats.

Application of geovisualization methods allows research engineer in the field of energy to visually determine the location of objects relative to each other, and switch to the mode of displaying the main characteristics of the identified vulnerabilities and threats of each EF with a large number of ones.

At the second stage (2), build threat scenarios for analyzable EF with the application of scenario approach.

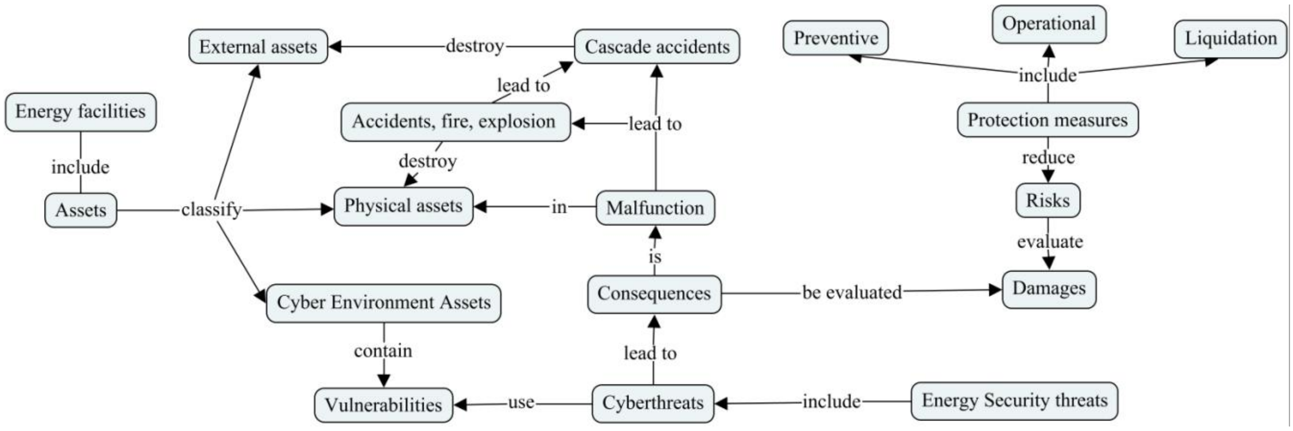

Fig. 1. The ontology of cybersecurity in energy.

In the first place, construct the graphical model of the cyberthreats implementation scenario, which include their impact on the physical level (initiation of ES threats, environmental and economic threats, etc.). The model shows a sequence of concepts that describe an attack propagation and possible consequences from it. At the next item, convert this model into Bayesian network model, add tables of conditional probabilities and calculate the probability of some consequences occurrence.

Hereupon, build a probabilistic model of security threats realization using information about vulnerabilities and threats, obtained from previous stage.

The third stage (3) involves assessing the risks and consequences of each scenario using a risk-based approach. The approach considers harm from damage or demolition of the object using quantitative and qualitative parameters, as well as further damage or destruction probability of the object components, with consideration for extent of damages and cascade failure. The risk assessment is based on the received threats probabilities, the developed risk classification and the expected consequences, which are evaluated by economic efficiency and evaluation criterion.

A prototype “RiskMap” was developed for qualitative analysis of the risks of violating the cyber-security of the energy facility. The prototype includes a heat risk map and radar chart. Heat map reflects the degree of risk significance and allows visually to assess the number and names of risks by three categories: admissible, moderate, critical. The radar chart illustrates the types of risk.

Identifying security threats is an iterative process, and preventing and responding to computer attacks is a long and cyclical task. The primary stage is the identification of trivial attacks and attacks of low complexity.

When reviewing this problem, ontologies as semantic modeling tools were used. The metaontology of the fuel and energy complex (FEC) was analyzed [9] to study the energy sector. The main aspects of cybersecurity in accordance with standard ISO/IEC 27032: 2012 are reflected in the ontology of cybersecurity [10]. To reflect the interconnection of cybersecurity threats and other threats of energy security, the ontology was built (Fig. 1).

The work considers three assets categories: 1) the cyber environment assets including software and hardware, information and telecommunications components of the energy facility information technology system; 2) physical level assets of energy facilities; 3) external assets toward the object considered which can be damaged by the cyber threats implementation.

The first assets type mostly includes the components of the industrial control system, such as automated operator and dispatcher workstations, SCADA systems (software and servers), intelligent actuators and sensors, technological network and industrial protocols, corporate network and routing.

The second type is related to assets of physical components under the control of ICS (machine/device) likes of generators, transformers, turbines, and others.

Assets of the third type represent an environment external to the object considered and can be ecological objects or territories, energy consumers, other energy or other infrastructures facilities that are territorially or functionally related.

In research of intelligent energy systems, two interrelated areas are allocated: the technological infrastructure and the information and telecommunications infrastructure [11].

Components of power management systems and their main vulnerabilities and cyber threats are considered in [12]. Electric power management systems include two levels: the physical component of control system, and supporting infrastructure, which includes software, hardware and communications networks.

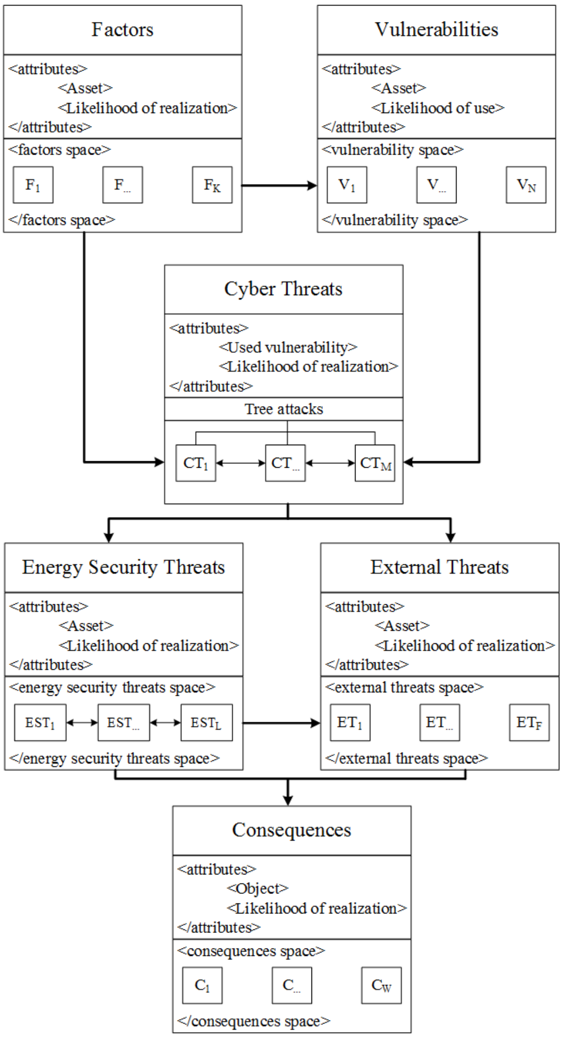

Fig. 2. The structure of the extreme situation scenario.

The main types of threats for these systems are 1) the threat to corrupt the content; 2) the threat to introduce a time delay or denial in the communication with received measurements or control messages, desynchronization, timing attacks. The main consequences from cyber-attacks implementation are loss of load or violations in system operating frequency and voltage, or other negative influence.

In the Russian legislation [13] three levels of ICS are distinguished: 1) the level of operator (dispatching) control (the upper level); 2) the level of automatic control (middle level); 3) level of input (output) of data, actuators (lower (field) level).

Existing approaches to the threats classification don’t reflect an adequate picture of the interdependence of assets, vulnerabilities and threats. The authors propose to establish these relations using the expert system “Cyber” by filling the knowledge base. The knowledge base rules are divided into three main groups: audit rules, rules for associating vulnerabilities and threats, and rules for describing typical threat scenarios that can later be displayed using Bayesian networks as a probabilistic model.

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 [14].

In [15] the Bayesian networks are used to analyze energy security threats. 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 ExS 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.

Both the threat analysis, covering a wide range of parameters and threats in a particular ExS, and weaknesses assessment can be simulated by Bayesian network factored in granularity of analysis of the energy facility information technology system.

Investigation of the possible consequences from the adverse events implementation is the important task in shaping the threats implementation scenarios. The consequences assessment is done by assigning an evidence for one node, and further reviewing the values of its descendants (the consequences of the event).

Figure 2 shows the structure of the ExS scenario.

Risk management is used in many areas and risks are understood as a different notions depending on the research area.

The ISO 31000: 2018 (E) “Risk Management – Guidance” standard issued in February 2018 contains a general approach to managing any risks.

Given that energy is a critical infrastructure and the disruption of its functioning can lead to disastrous consequences, and also active digitalization period, this paper consider risks as a negative event within the framework of risk management of information technology and the accidents and disasters theory.

The formula (1) of risks consists of three components [16]:

$$R = \{T, V, D\}, \quad (1)$$

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

The information technology system assets of the enterprise contain vulnerabilities and they are not highlighted in formula (1) because ones are attributive. Threats are expressed by the likelihood of the negative event occurrence, which lay in using the vulnerability and / or the likelihood of the threat implementation from the initial threat (tree of threats). And damages are a measure of economic evaluation and, as a rule, are expressed in monetary equivalent.

Cyber threats are considered as strategic threats that can cause the realization of energy security threats, the consequences of which are significant social, economic or environmental losses caused by ExS, including accidents or cascading accidents.

The building of the “Vulnerability – Threat – Consequences” threesome is targeted for implementation during the phase of probabilistic models development of private threats model using the Bayesian network. The Bayesian network allows estimating the impact of the vulnerability probability on threats, threats on threats, and threats on consequences.

Farther, it is proposed to display a ranked list of facility critical assets. Critical assets are considered assets, which accounted for the greatest number of threats in the scenarios and the greater likelihood of threats implementation then probability threshold determining by expert.

3. Conclusion

There are numerous methods and approaches to research critical infrastructures that are applied depending on the purpose of the study. In this paper, the authors propose an approach that includes the following steps:

- stage of identifying vulnerabilities and threats of IT system of EF,
- stage of threat analysis using semantic modeling,
- stage of assessing risk of cybersecurity violations in the critical information infrastructure.

Since energy sector is a complex multicriterial structure with a lot of interrelations and interdependencies, the authors use methods of semantic modeling that allow, on the one hand, to simulate the research field and to evaluate the situation plausibility on a qualitative level without performing complex computer experiments on the other.

Farther, the authors use risk management, which is an integral part of the enterprise management process and an approach to assessing the likely losses and damages in the occurrence of ExS, taking into account a bunch of "vulnerabilities-cyber threats-threats-EB consequences."

Acknowledgements

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. A. Kondratev, The current trends in research of Critical Infrastructure in foreign countries, *Foreign Military Review*, no. 1, (2012) 19–30 (in Russian).
2. A. G. Massel, Cyber-attacks as a threat to Russia's Energy Security, in *Proc. International Conference "Cybersecurity-2013"* (Kiev, 2013) pp. 49–56 (in Russian).
3. L. V. Massel, A. G. Massel, Semantic technologies based on the integration of Ontological, Cognitive and Event modeling, in *Proc. III International Science and Technology Conference "OSTIS-2013"* (Minsk, 2013), pp. 247–250 (in Russian).
4. M. Rybnicek, R. Poisel, M. Ruzicka and S. Tjoa, "A Generic Approach to Critical Infrastructure Modeling and Simulation", i*n Proc. International Conference on Cyber Security "CyberSecurity"* (Alexandria, VA, USA, 2012), pp. 144–151.
5. L. V. Massel, N. I. Voropai, S. M. Senderov, A. G. Massel, Cyber Danger as one of the strategic threats to Russia's Energy Security, *Cybersecurity issues*, no. **4**(17) (2016) 2–10 (in Russian).
6. A. V. Edelev, S. M. Senderov, I. A. Sidorov, The use of distributed computing to identify critical objects of the Russian gas transmission network, *Information and Mathematical Technologies in Science and Management*, №1. (2016) 55–62 (in Russian).
7. *About the Security of the Critical Information Infrastructure of the Russian Federation, Federal Law no. 187-FZ 01.12.2016, 2017,* [Online]. Available: http://pravo-search.minjust.ru/bigs/login.jsp#id=37A0900E-7D2A-43A3-BBAD-CC3B7F2703E0 (in Russian).
8. L. V. Massel, T. N. Vorozhtsova, N. I. Pjatkova, Ontology engineering to support strategic decision-making in the Energy Sector", *Ontology of Designing*, Vol. 7, no. **1** (23) (2017) 66–76 (in Russian).
9. L. V. Massel, Knowledge management for intelligent decision support of decision-making based on Ontological engineering, in Proc. All-Russian Conference "The distributed information-computational resources. Science – the digital economy" (DICR-2017) (Novosibirsk, 2017) 30–37 (in Russian).
10. T. N. Vorozhtsova, Development of the ontology of cybersecurity in the energy sector, in *Proc. International Conference "Cybersecurity-2013"* (Kiev, 2013) 19–25.
11. L. V. Massel, Ontological engineering and knowledge management to support strategic decisions on Intellectual Energy development, in *Proc. XX Anniversary All-Russian Scientific Conference "Enterprise Engineering and Knowledge Management"* (Moscow, 2017) 59–65 (in Russian).
12. S. Sridhar, A. Hanh, M. Govindarasu, Cyber-physical system security for the electric power grid, in *Proc. IEEE*, Vol. 100, no. 1, 2012, 210–224.
13. *Requirements to ensure the information protection in automatic process control system of production and technological processes in critical facilities, potentially hazardous facilities, and also objects that present an increased danger to human life and the environment*, Order of FSTEC Russia no. 31 14.03.2014, 2014, [Online]. Available: http://fstec.ru/prikazy/864-prikaz-fstek-rossii-ot-14-marta-2014-g-n-31 (in Russian).
14. D. Heckerman, *A Tutorial on Learning with Bayesian Networks, Technical Report MSR-TR-95-06*, (Microsoft Research, March, 1995), 57 p.
15. L. V. Massel, N. I. Pjatkova, Application of Bayesian Belief Networks for the intelligent support of Energy Security problem researches", in *Proceedings of Irkutsk State Technical University*, no.2, (2012) pp. 8–13 (in Russian).
16. A. G. Massel, L. V. Massel, D. A. Gaskova, Cybersecurity of critical infrastructures (on the example of Energy Sector), in *Proc. The 7th Anniversary All-Russian Conference "Information Security Technologies" (BIT-2016)* (Moscow, eds. V.A. Matveev, 2016) pp. 197–199 (in Russian).