# Ontological Analysis of Vulnerabilities in the Energy Sector

**Tatiana N. Vorozhtsova[1], Sergey K. Skripkin[2]**

*Melentiev Energy Systems Institute, Siberian Branch of the Russian Academy of Sciences,*
*Lermontov str., 130*
*Irkutsk, Russia*
*[1] E-mail: tnn@isem.irk.ru*

*[2] E-mail: sks@isem.irk.ru*

**Abstract**

The paper presents an ontological analysis of the terminology associated with the concept of vulnerability in the energy sector. The ontology of vulnerabilities is proposed. This ontology reflects the interrelationships between this concept and other cyber security concepts. Classification of vulnerabilities is presented. Possible means of protection for ensuring information security and cyber security in the energy sector are considered.

*Keywords:*Vulnerability, threats. assets, ontology, information security.

## 1. Introduction

The use of information and communication technologies for monitoring the state of energy systems and their control is expanding in the context of the development and implementation of the smart energy concept. This requires a more detailed study of the cyber security problem in different stages of using computer technologies and systems in the energy sector [1]. The notion of "Vulnerability" is directly connectedwith the notion of "Security". The presence of various kinds of vulnerabilities in facilities and information systems leads to the implementation of threats and disruption of energy facilities functioning.

Researchers in Melentiev Energy Systems Institute made an analysis of energy security threats in [2, 3]. Cyber threats are one of the strategic threats to energy security. We previously performed ontological engineering of threats [4]. In this paper,we propose an ontological analysis of possible vulnerabilities at power facilities, their classification, causes and methods of elimination.

The ontology of vulnerabilities is part of the ontology system designed to harmonize research and development of an intelligent system and strategic decision-making support in the energy sector [5,6].

## 2. Vulnerability ontology use

An ontological analysis or ontological engineering is held in order to identify the basic concepts of the domain and their interrelations. The ontological approach provides classification of vulnerabilities, their relationship with other concepts of this subject domain.

Ontologies of vulnerabilities are used for similar purposes in the studies by foreign researchers. For example, the authors of [7] present an ontology of vulnerability designed to provide a structured representation and assessment of vulnerabilities.

Security researchers, software developers, vulnerability coordinators, vulnerability information services and othersuse vulnerability ontologies. A vulnerability ontology is used as a methodological framework for the development of software and tools, including information and management systems. [8]. The vulnerability ontologies are also used to form a security requirements baseline [9].

All these ontologies contain basic concepts related to vulnerability, such as "Asset", "Attacker", "Attack", "Risk", "Countermeasures" and others.

## 3. Basic definitions

In the most general sense, the vulnerability is considered as a weak point or a parameter characterizing the possibility of causing any damage by external means or factors to the described system [10].

Since energy facilities are complex systems, vulnerabilities can be found in physical facilities, control systems, information systems, data transmission facilities and other locations.

Copyright © 2018, the Authors. Published by Atlantis Press.
This is an open access article under the CC BY-NC license (http://creativecommons.org/licenses/by-nc/4.0/).

The ITIL glossary of terms defines vulnerability as a weakness that can be exploited by a threat. Lack of control is also a kind of vulnerability [11].

Vulnerability of an object is the internal properties or weak points of an object that cause its sensitivity to the source of risk, which can lead to the realization of an event and its consequences. The vulnerability of the object depends on the location of the object, its size, the scheme of operation and the degree of life support, the level of protection, strength of the object and other qualities, as well as the nature, degree and means of influence, repetition of events. The property of vulnerability is opposite to the property of stability, this is an inability to resist external influence [12].

In computer security, the term "vulnerability" is used to refer to a weakness of a system that can be used to intentionally disrupt its integrity and cause its malfunction. Vulnerability may be a result of programming errors, deficiencies in the design of the system, weak passwords, viruses, and malicious programs.

The state standard for information technology security defines vulnerability as the weakness of one or more assets that can be exploited by one or more threats [13].

Analysis of these definitions shows that the main concepts related to the concept of "Vulnerability" are – "Threat", "Asset", "External impact" and others.

## 4. The relationship of basic concepts

Vulnerability is one of the basic concepts that have a direct link to cybersecurity, along with such concepts as threat, risk, countermeasure (means of protection), asset (resource or object of protection), stakeholder (interested person, participant), and others. Figure1 shows the basic concepts associated with the concept of "Security" and the relationship between them. As can be seen from the presented scheme, the concept of "Vulnerability" is associated with almost all other concepts related to security.

As a rule, the vulnerability is associated with the asset, i.e. the asset may have the vulnerability. Accordingly, the threat may exploit the vulnerability to negatively impact on the asset. The assets of the company are a set of its property and money. Assets can be both physical energy facilities – equipment, production facilities, transport flows, communications, and non-physical, for example, management systems, personnel, information, investment funds, software and hardware, and others [14, 15].

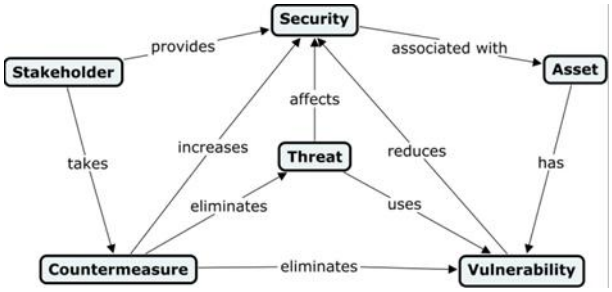


Fig. 1. The relationship of the basic concepts.

The information technologies are widely used in the energy sector, therefore, any of the assets that have vulnerabilities can be subject to cyber threats. The issue of eliminating vulnerabilities and ensuring cyber security is most closely related to the use ofcomputer systems in the control of power systems at different levels.

## 5. Causes and classification of vulnerabilities

There are different causes of vulnerability, for example, design mistakes, deliberate actions during design, incorrect settings or inadvertent user actions. The other vulnerability causes are failures of hardware and software under external impact, the implementation of programs for unwarranted expenditure of resources [16]. Depending on these causes, the vulnerabilities may be classifiedas follows:

- technological or architectural (connection of corporate devices to the unprotected wireless network segments),
- organizational (lack of control over management processes, uncontrolled information flows, impact through contractors),
- operational (weak passwords, unsupported versions of system software, the use of insecure control protocols).

A more detailed classification of vulnerabilities involves the following attributes: the degree of premeditation, the stage in which the vulnerabilities occur, the level in the information system, the type of subsystem, a result of the impact and the object of impact as well as the level of risk.

According to the degree of premeditation, vulnerabilities may be created intentionally or unintentionally. Vulnerabilities can arise in the stages of design, coding or operation. They can exist at the operating system level, in applications, databases or in communication networks. The vulnerability can be in a cryptographic, password or integrity subsystem. The presence of vulnerabilities may result in:

- input and output errors,
- denial of service,
- unauthorized access to data,
- violation of information integrity,
- control violation.

According to the risk level, vulnerabilities are classified as follows:

- high – the possibility of direct access to information with root permissions,
- medium – the ability to access to information which consequently allows you to get access to the site,
- low – the ability to collect information about the system.

## 6. Ontology of vulnerabilities

The result of the performed ontological analysis is the development of ontology, as the main means of formal representation of knowledge domain. Fig. 2 shows the vulnerability ontology.


Fig. 2. Ontology of vulnerabilities.

The ontology presented in a graphical form is performed by using CmapTools and is aimed at illustrating the basic concepts and relationships between them. This allows us to drill down into the basic concepts at the next level, for example, to analyze assets that have vulnerabilities.

As the assets are owned or used by the stakeholders, the relevant requirements or rules for compliance with cybersecurity (countermeasures) are formed for them. Similarly, an analysis of the likely threats, that exploit the vulnerabilities,makes it possible to envisage countermeasures against identified or possible intruders.

## 7. The removal of typical vulnerabilities

Traditional information security tools to address vulnerabilities include [17]:

- Configuration management. The configuration of IT infrastructure components, including information security features, must meet the enterprise information security requirements because standard features can be dangerous if configured incorrectly. Monitoring should be carried out periodically.
- Update management. System and application software updates must be installed and monitored regularly.
- Change management. Introduction of major changes to information systems should be accompanied by testing of implemented information security mechanisms. The most significant changes are those concerning architecture of the system, its functions, information security tools and others.
- Vulnerability management. It is necessary to monitor vulnerabilities and assess possible attacks aimed at exploiting the identified vulnerabilities in the existing infrastructure, use the assessment of risks and consequences from the impact on the IT infrastructure. It is necessary to determine the causes of inefficiency of the existing vulnerability management process.

## 8. Methods or means of protection

Cyber threats and cyberattacks in the energy sector are mainly related to corruption and loss of information in different stages of its acquisition, transmission and processing [18]. Information security system is a set of controls, performers, used equipment, as well as objects of protection. This system includes:

- measures – a set of actions aimed at the development and practical application of methods and means of protection,

- equipment – means of protection, control, and management to ensure the protection of information,
- methods – the procedure and rules for the application of certain principles and remedies.

There is the following classification of information security:

- technical means, which include noise generators, network filters and other devices that block the channels of information leakage or allow them to be detected. The advantages of technical means are associated with their reliability, independence from subjective factors, high resistance to modification,
- software including programs for user identification, security system testing, etc. The advantages of the software are versatility, flexibility, reliability, ease of installation, the ability to modify and develop. The main drawback is the high sensitivity to accidental or intentional changes, possible dependence on hardware.
- organizational means consist of organizational and technical (preparation of premises, laying of cable system meeting the requirements of limited access to it, etc.) and organizational and legal (legislation and work rules, established by the management of a particular enterprise). Organizational tools make it possible to solve many diverse problems. They are easy to implement, quickly respond to unwanted actions in the network, have unlimited possibilities of modification and development. The main drawback is the dependence on subjective factors, including the overall organization of work in a particular unit.

Only a reasonable combination of all means can provide the least probability of cyber threats impact on the operation of energy facilities, and protect the process from failures.

## 9. Conclusion

The issues of cybersecurity of the energy industry, as the main object of critical infrastructure,are becoming increasingly moreacute in the present stage of the industry development. This is due to the introduction of modern digital technologies and intelligent networks. New computer technologies for measuring and transmitting data, monitoring operation and control systems increase vulnerability to cyber threats of both individual energy facilities and the entire power system.

The performed ontological analysis makes it possible to study all relationships between the concept of "Vulnerability" and other concepts related to cybersecurity in the energy sector, take into account possible influencing factors, identify possible sources of hazards and provide appropriate measures to prevent cyberattacks on energy facilities.

Detection of vulnerabilities is a periodic process, and its frequency should depend both on the criticality of the information processed in the IT infrastructure and on the characteristics of the infrastructure itself.

The elimination of the identified vulnerabilities is a process of continuous improvement of the information security system. Its implementation will help to address current vulnerabilities and to reduce the likelihood of new ones.

## Acknowledgements

This research was done in the framework of the basic research program of SB RAS III.17.2.1, reg. № AAAA-A17-117030310444-2, and partially supported by RFBR grants №16-07-00569, №16-07-00474.

## References

1. Massel L.V., Voropai N.I., Senderov S.M., Massel A.G., Cyber security as one of the strategic threats to Russia's energy security *J. Cyber security issues.* **4** (17). (2016) 2–10.
2. *Energy security of Russia: problems and solutions* / N.I. Pyatkova [and others]; ed. By N.I. Voropai, M.B. Cheltsov; Melentiev Energy Systems Institute SB RAS. (Novosibirsk: Publishing House of SB RAS, 2011).
3. *Ensuring Russia's energy security: selecting priorities* / S.M. Senderov, V.I. Rabchuk N.I. Pyatkova, S.V. Vorobiev; ed. by S.M. Senderov, Melentiev Energy Systems InstituteSB RAS. (Novosibirsk: Publishing of SB RAS, 2017).
4. T. Vorozhstova, N. Pyatkova, Ontology Engineering threats to Energy Security, in *Proceeding of International Workshop "Critical Infrastructures: Contingency Management, Intelligent, Agent-based, Cloud Computing and Cyber Security" (CI:CM/IACC/CS – 2017)* (ИСЭМ СО РАН, 2017) pp. 24–26.
5. Massel L.V., Massel A.G., Technologies and tools of intelligent decision-making support in emergency situations in the energy sector, *J. Computational technologies.* V.18. (2013) 37–44.

6. Vorozhtsova T.N., Ontological model of knowledge space for situational management in energy, in *Proceedings of XX Baikal all-Russian conference "Information and mathematical technologies in science and management"*. V.3. (Irkutsk. MESI SB RAS, 2015) pp. 85–88. (in Russian).
7. B. Khazai, T. Kunz-Plapp, C. Buscher, A. Wegner., VuWiki: An Ontology-Based Semantic Wiki for Vulnerability Assessments. [online] available: https://link.springer.com/content/pdf/10.1007%2Fs13753-014-0010-9.pdf.
8. H. Booth, C. Turner., Vulnerability Description Ontology (VDO). A Framework for Characterizing Vulnerabilities. Reports on Computer Systems Technology / [online] available: https://csrc.nist.gov/CSRC/media/Publications/nistir/8138/draft/documents/nistir_8138_draft.pdf.
9. G. Elahi, E. Yu, N. Zannone, A Modeling Ontology for Integrating Vulnerabilities into Security Requirements conceptual Foundations, in *Proceeding of International Symposium "Rule Interchange and Applications"*(2009) pp. 99-114. [online], available: https://link.springer.com/content/pdf/10.1007%2F978-3-642-04840-1.pdf.
10. Wikipedia. [online] available: https://en.wikipedia.org/wiki/Vulnerability_(computing).
11. Terms dictionary ITIL in Russian. Edition 2.0. [online] available: http://www.itsmforum.ru/ZAM-test/Russian_2011_Glossary_v2.0.pdf
12. Dictionary of emergency situations. Electronic resource: https://dic.academic.ru/dic.nsf/emergency.
13. GOST R ISO/IEC 13335-1-2006: Information technology. Security techniques and tools. Part 1. The concept and model of safety management of information and telecommunication technologies.[online], available: http://controleng.ru/wp-content/uploads/6822.pdf.
14. Papkov B.V., Cyber-threats and cyber-attacks in the electric power industry: textbook / B.V. Pupkov, A.V. Kulikov, V.L. Osokin. (N. Novgorod: NIMRAS, 2017)
15. Papkov B.V., Cybersecurity issues in the electricity sector / B.V. Papkov, A.L. Kulikov, V.L. Osokin. (M.: Energoprogress, 2017) (Bibliotechka electrical engineering, Supplement to the journal "Energetic"; V.**9** (225)).
16. Osak A.B., Panasetsky D.A., Buzina E.Y., Cybersecurity of electric power facilities as a factor of reliability of power plants. [online] available: https://www.researchgate.net/publication/301551630_Kiberbezopasnost_obektov_elektroenergetiki_kak_faktor_nadeznosti_EES.
17. Papkov B.V., The vulnerability and resilience of electric power facilities, in *Proceedings of Yu. N. Rudenko International Scientific Seminar "Methodological problems in reliability study of large energy systems"ed. by N. I. Voropai, Issue 68. "Research and ensuring the reliability of energy systems"* (Irkutsk: ISEM SB RAS, 2017) pp. 682.
18. Cybersecurity 2016-2017: from the results of the forecasts. [online] available: https://www.ptsecurity.com/upload/corporate/ru-ru/analytics/Cybersecurity-2016-2017-rus.pdf.