The Current State of Cyber Security in Russia’s Energy Systems and the Proposed Activities for Situation Improving

Aleksei Massel
Melentiev Energy Systems Institute of SB RAS
Irkutsk, Russia
amassel@gmail.com

Liudmila Massel
Melentiev Energy Systems Institute of SB RAS
Irkutsk, Russia
massel@isem.sei.irk.ru

Abstract. This article discusses the current state of cyber security in the Russia’s energy systems and the necessity of special preventing measures aimed at threats, including those caused by the specifics of Russia. It is proposed cyberattacks ontology, including, in addition to attacks specifically aimed at energy facilities, unintended attacks as a result of cyber negligence. It's developed the technique of threats analysis and risk assessment of violation of information and technology security of energy complexes. The authors suggest to develop an expert system to support proposed technique that could be used to audit of energy enterprises in terms of cyber security.

Keywords : Cyber security, Information and Physical Security, Cyber Physical Systems (CPS), Smart Power Grid, Critical infrastructure protection.

I. INTRODUCTION

The energy infrastructure is one of the types of critical infrastructure in Russia. Energy security (ES) is an important part of Russia's national security [1], but until recently, when considering the ES threats is not considered a problem of cybersecurity , which are exacerbated by the spread in Russia of the Smart Power Grid concept [2].

It is clear that the successful implementation of this concept requires more attention to the problems of both modern Information and Communication Technologies (ICT) and to the problems of cyber security as complication of modern information and communication technologies increases the vulnerability of the created systems [3-4]. This article discusses the current state of cyber security in the Russia’s energy systems and the necessity of special preventing measures aimed at threats, including those caused by the specifics of Russia. It is proposed cyberattacks ontology, including, in addition to attacks specifically aimed at energy facilities, unintended attacks as a result of cyber negligence. With this in mind, it's developed the technique of threats analysis and risk assessment of violation of information and technology security of energy complexes. The authors suggest to develop an expert system to support proposed technique that could be used to audit of energy enterprises in terms of cyber security.

II. SPECIFICITY OF CYBER SECURITY PROBLEMS IN RUSSIA’S ENERGY INFRUSTRUCTURE

Common problems of cybersecurity in Russia’s energy infrastructure have been considered in the paper [5], published in the Proceedings of this Conference, and in papers [2-3]. Here we consider specificity of these problems, characteristic for Russia, on the example of cyber attacks.

Here are two definitions of cyber attacks: 1) cyber attack, or attack from cyberspace – the attack, carried out with the help of software and hardware on computer networks or computer systems of the enemy; 2) cyber attack - a deliberate attempts to alter, disrupt or stop the operation of computer systems or networks, as well as programs or information that they contain or transmit [6].

Speaking about cyber attacks should be borne in mind that, in addition to intentional acts, the harm can be cause by unintentional actions (we propose to call them cyber negligence) due to, for example Poor computer competence of staff or disparagement of measures providing cyber security, which may be comparable with damage caused by cyber attacks. It is the latter factors are essential for Russia, and can have serious consequences, given the Russian mentality.

The classification of cyber threats can be based on the following criteria

1) the nature of origin (deliberate and unintentional);
2) the direction of implementation (internal and external);
3) the object of the impact (user and administrator workstations, tools for documenting and mapping, communication channels, etc.);
4) a method of implementation (information, software and hardware, physical, radio, organizational, legal, etc.);
5) life cycle (design, commissioning, operation, decommissioning) [7].

Fig. 1 shows the cyber attacks ontology [8] which can be directed as to generating facilities of EPS, so to electricity transmission facilities and objects electricity consumption. The most vulnerable link is the management and control systems of electric power systems (EPS), and vulnerability of management systems will increase as the spread of declared in the Smart Grid conception in Russia multi-agent approach [4].

III. The current state of cyber security in Russia's energy systems.

Among the information and control devices and systems in EPS release:

1. Means of control and management:

ACM (Advanced Control Methods) - Improved methods for monitoring and control.

2. Improved Interfaces and Decision Support – IIDS

Examples of the most commonly used IIDS:

- Outage management system.
- Geographic information system (GIS).
- Work management system.
- Mobile work system.
- Customer Information systems.

3. Integrated Communications

Integration of communication systems provides two main functions:

- Open communication standards, such that information can be recognized by a wide range of users (senders and receivers).
- Media support, which provides the necessary infrastructure to transmit information accurately, safely and securely at the desired speed and with the necessary bandwidth.

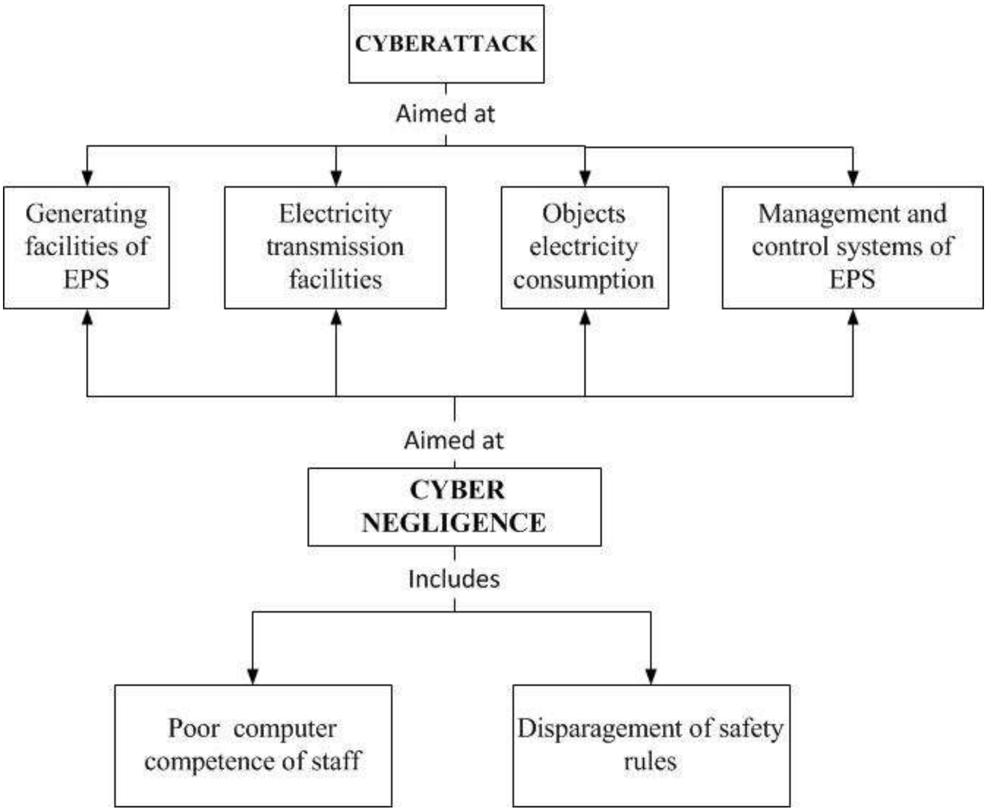
CYBERATTACK
Aimed at
Generating facilities of EPS
Electricity transmission facilities
Objects electricity consumption
Management and control systems of EPS
Aimed at
CYBER NEGLIGENCE
Includes
Poor computer competence of staff
Disparagement of safety rules

Fig.1. The ontology of cyberattacks

The current state of automated process control systems (APCS) in the energy sector is characterized by the following figures (according to the company Positive Technologies):

- Since 2010, 20 times increased the number of detected vulnerabilities (Fig. 2).
- Every fifth vulnerability persists longer than a month.
- 50% of the vulnerabilities allow an attacker to run code execution.
- For 35% of the vulnerabilities have exploits (special programs for cyber attacks using these vulnerabilities).
- More than 40% of Internet-accessible systems can be hacked by hackers-fans.
- One-third of the systems available from the Internet are in the USA.
- Quarter of vulnerabilities is related to the lack of necessary updates of security.
- 54% of Internet-accessible systems in Europe and 39% in North America are vulnerable
- 50% published in the global network systems from Russia are vulnerable.

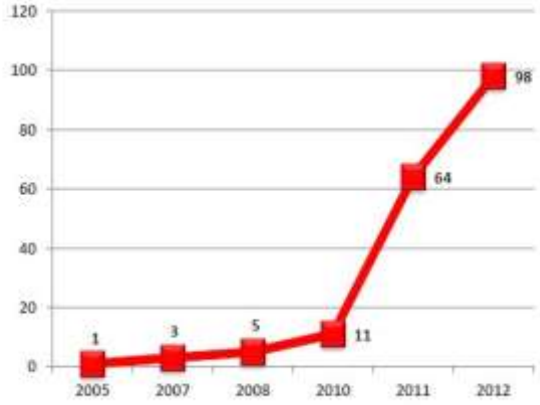

Fig. 2.Dynamics of vulnerability growth in APCS

Dynamics of vulnerability growth is shown in Fig. 2, main types of vulnerabilities are shown in Fig. 3.

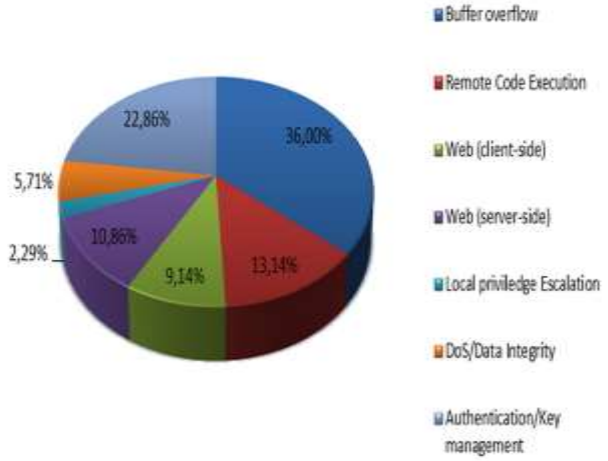

Fig. 3. Main types of vulnerabilities

Fig. 4 shows that the main producers of SCADA (System Control and Data Acquisition in the power) are foreign companies, which is also one of the threats to cyber security.

As for the share of eliminated vulnerabilities, it should be noted that the majority of security flaws (81%) were quickly eliminated by producers - even before information about them became widely known, or within 30 days after the uncoordinated disclosure of information.

A visual representation of how seriously information security problems by different producers of APCS are evaluated can be obtained from information about "closed" vulnerabilities. For example, Siemens has eliminated and released an update for 98% of vulnerabilities, while Schneider Electric eliminated only slightly more than half (56%) of the detected vulnerabilities. The most common drawbacks of safety (found in 36% of cases) related to configuration errors. This includes incorrect password policy (for example, the use of standard engineering passwords), access to critical information and erroneous separation of access rights. A quarter of vulnerabilities related to the lack of security updates.

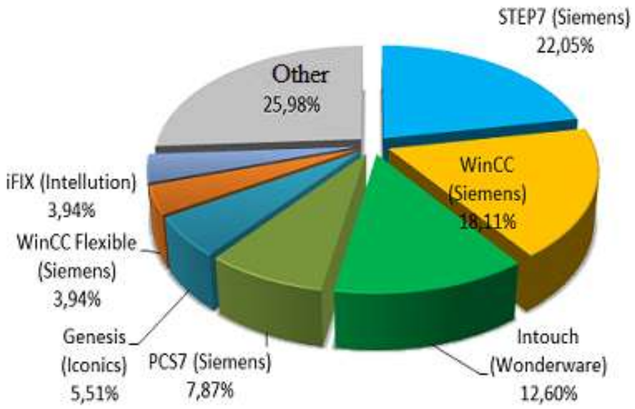

Fig. 4. The main producers of SCADA (according to the company Positive Technologies)

IV. The technique of threats analysis and risk assessment of violation of information and technology security of energy complexes (EC).

1. The procedure for threat analysis and risk assessment (TARA).

Main aspects are:

- criticality of objective functions EC supported by IT-systems
- the cost of protecting IT resources EC

2. Preparation and planning of threat analysis and risk assessment.

It is necessary to install:

- what is IT system or its parts shall be evaluated;
- for some reason it is necessary to assess;
- purpose of the evaluation;
- urgency or priority of work;
- maximum acceptable level of quantifying estimation of residual risk (for example, the maximum time during which is permited a partial loss of system performance due to the events associated with an concret threat)

3. Data collection for threat analysis and risk assessment.

- For the preliminary analysis of the IT-systems security it's necessary to gather information about threats, threatening events and weaknesses (vulnerabilities) of the analyzed system.
- Information about threats and vulnerabilities should help to identify what resources are most at risk from exposure to threatening factors.

4. Analysis compliance of security policy to regulating documents.

- Documents on the security policy and regulations should contain a description of the means available to protect resources of IT- systems and protection means, which application will reduce the risk

5. Analysis of resources criticality of studied information-technology systems.

- Task of resources criticality analysis is solved, if necessary detailed threat analysis and risk assessment and is based on the preliminary assessment of the resources criticality to determine the main directions of development.
- In cases where a detailed analysis of threats and risk assessment not required you can skip steps 5-7 in described technique and go to from step 3 to step 8.

6. Analysis of the threats to resources of studied information-technology systems.

- For each potential event it's necessary to analyze the threatening factors due to the degree of probability and motivation.

8. The vulnerability analysis of the studied system

- Within each domain, you must identify vulnerabilities (weaknesses), the use of which may damage its individual resources.
- In the analysis of vulnerability should use the list of weaknesses and description of the system obtained in the previous steps.
- For each weak point you need to install the probability of use

9. Analysis of the overall risk of a security breach of information-technology systems.

- Based on the analysis of the vulnerability of the system is required to describe all the possible scenarios of threats (threat scenario consists of one or more events that caused a threatening factor that could lead to compromise of the resource).

10. Assessment of acceptable risk of studied information-technology systems.

- Evaluation of acceptable risk should associate risk with certain resources of researched IT systems.
- Results of acceptable risk are important as a basis for the choice of resources protection means is performed by comparing the options until you select the appropriate measure of protection (or combination of measures).

Currently, under the leadership of the authors an expert system is developed that implements the proposed methodology.

V. Development of expert system to support the proposed methodology.

To implement this expert system were selected software environment CLIPS for developing of Knowledge Base and Inference Engine and object-oriented programming language JAVA for the implementation of the graphical user interface in expert system. The Use Case Diagrams of the developed software, reflecting the main steps of the proposed method, were realized. The design of an expert system is completed and its implementation executes.

VI. Conclusion

As noted in the article [1], it is obvious that punctual use of foreign standards in Russia is impossible due to the specific of Russia's energy systems and the Russian mentality. It was proposed common methodical approach to ensuring of Russia's energy infrastructure cyber security based on the development of national standards for cyber security and a number of special methods to ensure cyber security of energy infrastructure.

In this article the current state of cyber security in the Russia’s energy systems is considered and it’s proposed one of special methods – the technique of threats analysis and risk assessment of violation of information and technology security of energy complexes (EC) is proposed. An expert system is developed that implements the proposed methodology.

Acknowledgment

This work was partially supported by RFBR grants №13-07-00140, №15-07-1284, № 15-57-04074 and Grant Program of the Presidium of RAS №229. The authors are grateful to these organizations.

References

[1] V.V. Bushuev, N.I. Voropai, A.M. Mastepanov, J.K. Shafranik et al, “Energy Security of Russia,” *Novosibirsk: Nauka* , p. 302, 1998.

[2] B.B. Kobets, I.O. Volkova, “Innovative development of electric power based on the concept of Smart Grid,” *M .: IAC Energy*, p. 208, 2010.

[3] L.V. Massel, “The use of modern information technologies in the Smart Grid as a threat of cyber security to Russia’s energy systems,” in *Proc. of the International Conference "Cyber Security - 2013"*, 2013, pp. 56-65.

[4] L.V. Massel, “The problem of Smart Grid creating in Russia from the standpoint of information technologies and cyber security,” in *Proc. of the All-Russian seminar with international participation "Methodical research questions the reliability of large-scale power systems"*, 2014.- pp 171-181.

[5] Massel L.V., Massel A.G. Cyber security of Russia’s energy infrastructure as a component of national safety, *In This Proc*.

[6] Understanding of cybercrime: A Guide for Developing Countries, [Online]. Available: http://www.itu.int/dms_pub/itu-d/oth/01/0B/D010B0000073301PDFR.pdf

[7] N.A. Gaydamakin, Theoretical Foundations of Computer Security, *Ekaterinburg: Publishing House of the Ural University*, 2008,p. 212.

[8] A.G.Massel, “Cyber attacks as a threat to Russia's energy security,” in *Proc. of the International Conference "Cyber Security - 2013"*, pp. 49-56.