Cyber Security of Russia's Energy Infrastructure as a Component of National Security

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

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

Abstract. Energy infrastructure is regarded as one of the critical infrastructures of the Russian Federation, and cyber security of Russia's energy infrastructure - as a component of national security. The definition of critical infrastructure is given. Cyber physical systems (CPS) are considered, one of these applications is Smart Power Grid. Cyber physical security is defined as cyber security of CPS. The structure of the cyber security concept is considered and its important components are described as information and physical security. It's analyzed the approach to cyber security of Smart Power Grid, adopted abroad, and standards for the critical infrastructures protection. Methodical approach to ensuring of Russia's energy infrastructure cyber security is proposed.

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. We mean under that the set of power plants and energy systems, including energy transportation magistrals. Energy security (ES) is an important part of Russia's national security and can be defined as the protectability of citizens, society, state and economy from deficit threats in supplying basis needs of energy resources with its acceptable quality [1].

Until recently, when considering the ES threats is not considered a problem of cyber security , which are exacerbated by the spread in Russia of the Smart Power Grid concept, which implies the integration of advanced technological infrastructure and modern information technologies. The main achieved results should be observability, controllability, automation control electrical power system (EPS), providing high reliability and strong economic performance [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]. The problem of cyber security becomes particularly acute in connection with the development of the concept of Cyber-Physical Systems (CPS), which are now considered an important factor for the development of ICT and economic recovery and at the same time critical from the standpoint of national security.

This article discusses the state of work in this field, the experience of their solutions in other countries, particularly in the United States, the necessity of special measures aimed at preventing threats, including those caused by the specifics of Russia.

II. CYBER PHYSICAL SYSTEMS (CPS)

This term is still not enough widespread in our country, although these systems are being developed in Russia, including the energy sector. CPS term was proposed in 2006, CPS is now included in the priority lists of innovations in United States and several European countries. CPS predecessors considered embedded real-time systems, distributed computing systems, automated control systems of engineering processes and objects, wireless sensor networks. CPS - is a system consisting of various natural objects, artificial subsystems and the controllers which together form a whole.

CPS novelty and fundamental difference from the existing embedded systems or process control systems on which they are similar in appearance, is that CPS integrate cybernetic beginning, computer hardware and software technologies, as well as qualitatively new actuators embedded in their environment and are able to perceive it changes, respond to them, educate themselves and adapt.

CPS technical prerequisites are: 1) increase the number of devices with embedded processors and data storage: sensor networks operating in all extensive technical infrastructure; medical equipment; smart homes and so on; 2) integration that allows to achieve the greatest effect by combining the individual components in large systems: the Internet of Things, World Wide Sensor Net, Smart Building Environments, the defense systems of the future [5].

One of the areas of development and application of CPS believe Smart Power Grid. The current energy systems are only conditionally be called cyber physical - they were created at a time when the prevailing wasteful use of energy, and communications were quite primitive. Nevertheless, existing regulatory systems already include elements of CPS, as they provide dynamic management of power generation facilities in accordance with the unruly and time-varying loads. While not

all tasks of complex are automated and solved by operators, who are guided by their own experience of data evaluating obtained through feedback channels. However, given that the CPS considered critical from the point of view of national security, even at this stage it is necessary to pay great attention to security issues of CPS, as an important element of the energy infrastructure. In fact, it may be considered cyber physical security of critical infrastructures as cyber security of critical CPS of these infrastructures.

III. Definition and the concept of "cyber security"

According to the standard T-REC-X.1205 - ITU-T [6], cyber security is treated as a set of tools, strategies, principles of security, security guarantees, guidelines, risk management approaches, actions, training, experience, insurance and technologies that can be used to protect the cyber environment, resources, organizations and users.

Cyber environment is connected computing devices, personnel, infrastructure, applications, services, telecommunications systems, as well as the totality of transmitted and / or stored information.

Cyber security is an attempt to achieve and maintain the security properties from the resources of the organization or user against relevant security threats in the cyber environment.

- According to ISO 27032: 2012 [7], cyber security is based on:
- Applications Security
- Information Security;
- Network Security;
- Internet Security and
- Critical Information Infrastructure Protection,

but – isn't their synonymous (Fig. 1).

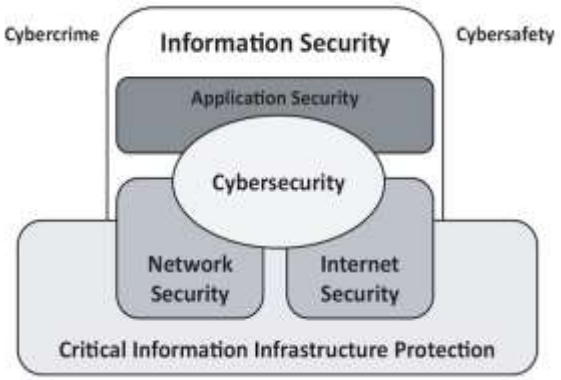

Fig. 1. Definition of cyber security according to ISO 27032: 2012

IV. Protection of key information systems of critical infrastructures objects.

Currently, cyber security is increasingly seen as a strategic issue of national importance, affecting all sectors of society. National cyber security strategy (NCSS) serves as a means increased security and reliability of the information systems of the state.

The first strategy of cyber security began to appear at the beginning of the previous decade. One of the first countries that began to perceive cyber security, as a matter of national importance were the United States of America. In 2003, the United States has been published National Strategy for Cyber Security (National Strategy to Secure Cyberspace). In 2005-2011 years twelve countries - members of the European Union published their national strategies of cyber security.

In Russia strategy of cyber security is not explicitly formulated, but it's developed "Main directions of state policy in the field of security of automated control systems of production and technological processes of critical infrastructure objects of the Russian Federation"

These "Guidelines" developed in order to implement the main provisions of the National Security Strategy of the Russian Federation (RF) until 2020, according to which one of the ways to prevent threats to information security of the RF is to improve the security functioning of information and telecommunication systems, critical infrastructure and high-risk facilities in the RF.

Critical facilities of the RF infrastructure is the object, the violation (or termination) of functioning which leads to loss of control, destruction of infrastructure, irreversible negative changes (or failure) of the economy of RF or its subject, or its administrative-territorial unit or leads to a significant deterioration in the security of life of people living in these areas for the long term. Energy systems, of course, are one of the critical infrastructures.

By CIGRE Working Group the B5.38, August 2010 were formulated **requirements for cyber security in the energy sector** (The Impact of Implementing Cyber Security Requirements using IEC 61850), the main of which are listed below:

- AC – Access Control – for protection against unauthorized access to the device, or information;
- UC – Use Control – for protection against unauthorized copying and use of the information;
- DI – Data Integrity – for protection against unauthorized changes;
- DC – Data Confidentiality – for protection against unauthorized access;
- RDF – Restrict Data Flow – for protection against publication of information in the unauthorized sources;
- TRE – Timely Response to Event – monitoring and logging of security-related events and timely actions in the aftermath of a responsible task and in critical situations for security;
- NRA – Network Resource Availability – for protection against attacks "denial of service".

Cyber security problem in the energy sector is compounded by the fact that among the main tasks of cyber security

ensuring in the Smart Grid main task is to ensure the ***availability***, while ensuring the ***integrity*** and ***confidentiality***. This means that the subjects who have the right to access to information, should be able to exercise their right to freedom, but at the same time, the system must be safe and to protect against cyber threats.

Cyber security could be compromised in the following circumstances:

1. the vulnerability of information resource on the support (lack of quality cryptographic protection);
2. the vulnerability of information channels;
3. the vulnerability of the medium or device of information transmission (eg, inappropriate control of access to the room).

In the field of cyber security are considered the security of information resources, means of information transmission, storage tools and are defined requirements for both information security and physical security.

The main objectives of ***physical security*** (protection) of any object:

- Monitoring of access control;
- Monitoring of CCTV;
- Preventing unauthorized access;
- Measures to prevent the consequences of an accident (fire, earthquake, catastrophes);
- Precautions to reduce the impact on security during emergency.

V. EXISTING APPROACHES TO PROVIDING OF CYBER SECURITY IN THE SMART GRID ABROAD

February 15, 2011 in the University of Maryland, Baltimore County (UMBC) hosted a conference, "Cyber Security in Smart Grid», organized by the Faculty of Computer Science and Electricity. At the conference was submitted report of the National Institute of Standards and Technology NISTIR 7628, called "Instruction to ensuring of cyber security in intelligent networks" (developed in 2010). In 2011, developed an approach to security based on NISTIR 7628, under the title «OpenWay Security», this approach was developed by two major companies: ITron and Cisco, with the support of NETL and NISTIR [8-9].

Fully document is called: «Guidelines for Smart Grid Cyber Security» (Guidelines for Cyber Security Smart Grid) and consists of an introduction and three volumes:

- Volume 1: «Smart Grid Cyber Security Strategy, Architecture, and High-Level Requirements».
- Volume 2: «Privacy and the Smart Grid»
- Volume 3: «Supportive Analyses and References».

At this document it is interest the consideration of risk as a product of the interaction of threats, vulnerabilities and their consequences. It is noted that cyber security should be directed not only to intentional actions of malefactors, but also on random errors, in this sense, defining the human factor.

Examples of potential risks:

- Increased complexity of the network increases the number of vulnerabilities to potential attacks and unintentional errors.
- Networks interconnected with other networks, which can also take a few "smart" network domains, increase the probability of cascade accidents.
- A large number of interconnections software components increase the vulnerability of software code that simplifies the implementation of attackers in the code of malicious code and vulnerabilities.
- With the increase of network nodes increases the number of entry points into the system for intruders.
- ***Using of the modern technologies - a new risks.***

Let’s illustrate the last point on the example of multi-agent technology. In the developed concept of Smart Power Grid in Russia is widely declared multi-agent approach to the construction of power system control. The problem of reliability and security of multi-agent control system (MACS) is the contradiction between the basic principles of MACS organization (its openness to large heterogeneous data streams from heterogeneous sources and opportunities to connect new types of agents) and requirements to security of the control system, especially in relation to the intentional cyber attacks. MACS is fundamentally vulnerable from the point of cyber-security, and it's the need in new ways to ensure its security and stability with respect to the poor quality and unfriendly data. To do this, it must be protected in relation to possible cyber attacks and be able to work effectively in a very large-scale income data streams of different quality and reliability. Otherwise vulnerable control system may cause major technological accidents.

VI. CRITICAL INFRASTRUCTURE PROTECTION (CIP) STANDARDS

Next, consider the short list of CIP standards, used in the United States. The purpose of these standards is to guarantee that automated systems and communications networks needed for a reliable supply of electricity in the country, reasonably protected from attacks from various credible sources of threats, as well as to maintain the viability and effectiveness of such protection.

CIP includes 11 standards; each standard specifies requirements for the protected object. Already mentioned the names of these standards provide insight into the breadth of the different areas in which cyber threats may arise, for example: CIP-001 - "Reports of suspicious activity"; CIP-002 - "Critical IT-resources"; CIP-003 - "Management in the field of cyber security"; CIP-004 - "Personnel and its Training"; CIP-005 - "Protection of electronic perimeter"; CIP-006 - "Physical Security"; CIP-007 - "Management of systems protection"; CIP-008 - "Incident Management" and others.

VII. METHODICAL APPROACH TO ENSURING OF CYBER SECURITY OF RUSSIA'S ENERGY INFRASTRUCTURE

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. One of the priority issues of cyber security of critical CPS in energy sector is to develop as national standards (taking into account international experience and the specifics of Russia), and methods for ensuring of cyber security, which should become part of the standards, the law approved at the state level.

These techniques should, in particular, determine:

1. The procedure for threat analysis and risk assessment, including criticality of supported by information and telecommunication technologies, targeted functions of Smart Power Systems and the protection cost of IT-recourses and IT-systems.

2. The level of detail analysis of threats, depending of the orientation on the category of decision-makers: senior manager; specialists responsible for the safe operation of IT systems; managers of functional departments of power systems.

3. The composition and the procedure for collecting data for threat analysis and risk assessment (data on threats, threatening events and weaknesses (vulnerability) of the analyzed systems).

4. The order of testing and the composition of tests to determine of the weaknesses (vulnerabilities) of analyzed systems, up to the organization of artificial cyber attacks in order to determine the reliability and vulnerability assessment of existing protection systems.

5. The composition of the recommended measures to improve the reliability of the analyzed systems; a list of possible cyber attacks and the actions needed to reflect them; regulation of activities in the aftermath of cyber intrusions (in the case of successful cyber attacks) [10]. At present, the technique worked out by the authors in more detail, but a full description is not given here.

It is clear that the list of techniques is not exhaustive, but work in this direction is needed primarily for awareness by energy specialists the scale of cyber threats and implications for energy systems, if they would implemented.

VIII. CONCLUSION

The article discusses the structure of cyber security concept and related terms: critical facilities, Cyber Phisical system (CPS) and critical infrastructures protection. It's analyzed the approach to cyber security of Smart Power Grid, adopted abroad, and standards for the protection critical infrastructures. It's noted that punctual use of foreign standards in Russia is impossible due to the specific of Russia's energy systems and the Russian mentality. It's proposed 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 techniques to ensure cyber security of energy infrastructure.

ACKNOWLEDGMENT

This work was partially supported by RFBR grants №13-07-00140, №15-07-1284 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] L. Chernyak. Cyber physical systems at the start. - Open Systems, № 2., 2014, [Online]. Available: URL: http://www.osp.ru (Date of treatment 9.04.2015).

[6] ITU-T Recommendations, [Online]. Available: http://www.itu.int/ITU-T/recommendations .

[7] ISO standard of Information technology. Security techniques. Guidelines for cybersecurity, ISO/IEC 27032:2012.

[8] Information security of Russia National Security, [Online]. Available: http://www.scrf.gov.ru/documents/6/113.html.

[9] Security standards NERC CIP, [Online]. Available: http://www.slideshare.net/CiscoRu/nerc-cip.

[10] 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.