Issues of Cybersecurity in Electric Power Systems

N.I.Voropai, I.N. Kolosok[*], E.S.Korkina, A.B. Osak

Melentiev Energy Systems Institute of Siberian Branch of Russian Academy of Sciences, Irkutsk, Russia

***Abstract* — The study deals with the cybersecurity concept of cyber-physical electric power systems (EPSs) as a strategic issue of national importance, which affects all strata of society. The link between the cybersecurity of EPSs and Russia's energy security and information security is analyzed. Data on the number of cyberattacks on control systems of industrial enterprises, power plants, and substations for several years are provided. The consequences of cyberattacks for the operability of the EPS physical subsystem and its facilities are analyzed. Areas of research to counteract external cyber threats are outlined. The key findings of the EPS cybersecurity study carried out at the Energy Systems Institute of Siberian Branch of the Russian Academy of Sciences (ESI SB RAS) are summarized.**

***Index Terms* — Electric power system (EPS), cybersecurity, cyber threats, cyberattacks, counteraction, consequences, key research findings**

I. Introduction

The electric power system (EPS) is an essential infrastructure that provides the population and the economy with electricity with the required reliability, adequate quality, and at an affordable price. With the growing consumer demands for the reliability of energy supply and quality of energy resources, EPSs are developing based on innovative, intelligent technologies in the context of digitalization and computerization of their production processes. Modern electric power systems and their facilities are complex systems consisting of two closely interconnected layers: physical (process) and information-and-communication subsystems. These subsystems of the present electric power systems, and even more so of the prospective ones, are getting comparable in complexity and responsibility in terms of ensuring the proper operation of EPSs.

Digitalization of the electric power industry implies not only the acceleration of information processing in a digital form but also an increase in efficiency of production processes using the next-generation equipment meeting the IEC standards and the development of new software for control of newly built digital substations, single-area electrical networks, and others. Under these conditions, it is getting increasingly more appropriate to treat EPSs as complex cyber-physical systems (CPS), in which the information-and-communication subsystem can operate inadequately due to internal defects (errors in algorithms, and others), and also can be exposed to unauthorized external actions, i.e., cyberattacks [1-6, and others].

The analysis of events that occur in the process of unfolding of several system accidents in different countries [7] proved the reciprocal influence of failures and disturbances in physical and information-and-communication subsystems (ICS) of EPSs. Invalid information on the current state of EPS and its loss due to cyberattacks on the ICS can lead to the generation and implementation of wrong control actions and the development of emergencies in the physical subsystem. In turn, the failure of a physical infrastructure element can result in an emergency state of the electrical part and contribute to the malfunction of the information-and-communication infrastructure control system.

This paper covers the basic concepts and definitions related to the EPS cybersecurity, analyzes the effects of cyberattacks on the performance of the physical subsystem of the EPS and its facilities, presents the areas for research to counteract external cyber threats, and discusses the key findings of the EPS cybersecurity studies carried out at the ESI SB RAS.

II. Basic concepts and definitions

Nowadays, cybersecurity is considered a strategic issue of national importance affecting all strata of society. In December 2016, the USA and Russia published almost simultaneously two official documents: "Joint US & Canada electric grid security and resilience strategy" [8]

[*] Corresponding author.
E-mail: kolosok@isem.irk.ru

http://dx.doi.org/10.38028/esr.2020.02.0003
Received February 22, 2020. Revised March 30, 2020.
Accepted June 02, 2020. Available online October 21, 2020.

and the updated "Doctrine of information security of the Russian Federation" [9]. Similar work is being done in the countries of the European Union, China, and others. The recognition of the cybersecurity importance is evidenced by the significant number of corresponding national strategies. However, these documents show noteworthy differences in the definition of cybersecurity and other key terms.

In [10-12], the authors study the connection between the EPS cybersecurity, on the one hand, and Russia's energy security (ES) and information security (IS), on the other hand. The authors of [11] note that the rapid spread of the computer environment, the development of information technology, and the trend towards the intelligent energy industry make cyber threat one of the most important tactical and strategic threats to energy security, i.e., they consider cybersecurity as an additional threat to energy security that is relevant in today's context.

On the other hand, since there is still no clear-cut definition of the "cybersecurity" term, it is often considered synonymous with information security. According to ISO 27032:2012 [13], cybersecurity is based on five components: application security, information security, network security, Internet application security, critical information infrastructure protection, but is not synonymous with any of them.

Information security is about ensuring confidentiality, integrity, and availability of information needed to meet user needs. Cybersecurity is a broader concept, it is construed as a set of tools, strategies, and technologies that can be used to protect the cyber-environment, resources of the organization, and the user [14]. The cyber-environment is understood here as connected computing devices, infrastructure, applications, services, telecommunications systems, the totality of transmitted and/or stored information, as well as maintenance personnel. Thus, approaching the EPS cybersecurity issue from the standpoint of the CPS, we should emphasize that it is aimed at protecting not only the data and facilities of the information-communication subsystem but also the data and facilities of physical infrastructure, the operation of which can be disrupted due to cyberattacks on the information subsystem.

At present, it is common to have all cyber threats divided into *external and internal ones*. Causes and sources of external threats are located outside the company's computers, usually in the global network: they are viruses, spam, remote hacking, DOD/DDOS attacks, and others. Internal threats depend solely on corporate personnel, software, and hardware. For energy companies, internal threats are no less dangerous than external ones. This issue becomes especially relevant when automating back-office processes in energy companies, for example, when digitalizing the document flow [15]. In Russia, the share of external attacks only slightly exceeds 20%, as estimated by the developers of corporate security systems; the rest of them are hence internal.

The earlier studies on cybersecurity of energy systems introduced the concept of cyber-negligence, which can also be treated as one of the internal cyber threats. Cyber-negligence [16] is the unintentional actions of employees of the organization that can prove harmful. They are due to negligence, poor computer literacy, or disregard for cybersecurity measures, and are comparable in damage to cyberattacks.

As noted in [6], the Dell Security Annual Threat Report published in 2015 by Dell provides the following recorded data on the number of cyberattacks on SCADA systems of industrial enterprises, substations, and power plants: 2012 - 91,676; 2013 - 163,228; 2014 – 675,186. The majority of cyberattacks targeted enterprises in Finland (202,322), Great Britain (69,656), and the USA (51,258), where SCADA systems are widely adopted and, in many cases, connected to the Internet. The authors show that to date, more than 30 countries have developed strategies to combat cyberattacks on energy and industrial facilities.

Therefore, the cyber resilience of energy facilities and EPSs as a whole is a critical and urgent issue to be addressed from the standpoint of the CPS given the interconnection of physical and information-and-communication subsystems [5].

III. Analysis of consequences of cyberattacks for the operability of the physical subsystem of the EPS and its facilities

Below we present some examples of cyberattacks on power facilities that show that such impacts on the ICS can lead to the destruction of physical subsystems and networks.

On December 23, 2015, a successful cyberattack was carried out on Ukraine's power grid [6]. It left about 225 (according to other sources - 600) thousand people without electricity for more than 6 hours. The power supply interruption lasted from 1 to 3.5 hours. Total electricity undersupply was 73 MW / h (0.015% of the daily electricity consumption in Ukraine). Hackers prepared their attack for at least six months. E-mails were sent to utilities, and once they were opened, the BlackEnergy3 malware got downloaded and isolated the infected computers from the control system of the power grid. The operation of the virus makes all information about the information-and-communication subsystem, passwords, and access codes available. After that, it was possible to log in to the SCADA system and shut down 17 substations. Some servers and workstations of automated dispatch management systems of regional EPSs were disabled. At the same time, the company's telephone lines were jammed, which prevented estimating the scale of the outage. Electronic devices used for communication with substation circuit breakers were disabled. Power flow was restored after switching to manual control.

Kyiv blackout [17]. On December 17, 2016, there was an outage of one-fifth of the Kyiv power grid together with the Kyiv pumped-storage power plant, which lasted one hour. The failure of the substation's automatic control completely de-energized the 330 kV Severnaya substation (Novi Petrivtsi village) with disconnection of substation auxiliaries from the power supply. As a result, the 144.9 MW loads of Kyivenergo PJSC and 58 MW of Kyivoblenergo OJSC were disconnected. The Kyiv pumped-storage was also de-energized with auxiliaries disconnected from the power supply, which was announced by the National Energy Company Ukrenergo on its Facebook page.

According to experts of the American company Dragos and Slovak ESET, the attack on a part of the Kyiv power grid was carried out by a team of hackers called Electrum. For this attack, the Electrum team used malware called CrashOverride. The researchers believe that the new software based on CrashOverride can automate massive blackouts. Malicious software includes interchangeable plug-in components. With their help, the malware adapts to different types of EPSs and can be easily reused when attacking the same facility or attack several targets simultaneously.

ESET and Dragos experts emphasize the main difference between the attacks on Ukrainian regional EPSs in December 2015 and that on Kyiv's power system. Whereas in the first case hackers had to access the EPS network and disable it 'manually', in the second case, the attack was fully automated. The CrashOverride malware is programmed to send commands directly via special protocols to the grid equipment to turn the power on or off. The experts claim that this feature allows CrashOverride operators to perform much larger and longer attacks than those during the Kyiv one-hour blackout. The consequences of the CrashOverride attack can be much more devastating than a temporary loss of control over the EPS. ESET experts hold that the malicious program has the potential to cause physical damage to EPS equipment. According to their data, CrashOverride can exploit the known vulnerability of Siemens equipment, in particular, the one found in the Siprotec digital relay. Such relays are installed for protection, monitoring, and control of electric power distribution and supply lines. Siemens has already released an update for the Siprotec relay, but if someone has failed to install it, attackers can physically destroy part of the power grid. Mike Assante of SANS Institute, a USA cybersecurity company, says that switching off a digital relay can cause thermal overloads in power lines. This can lead to sagging or melting of wires, damage to transformers, and live equipment.

Cyberattacks on nuclear power facilities [18].

1. On January 25, 2003, the Slammer network worm crashed the Ohio nuclear power plant's corporate network in the United States, after which it spread to the plant's safety monitoring and coolant systems. The host computer of the power plant was disabled after that. It took six hours to restore the systems.
2. In September 2010, in Iran, about 30 thousand computer systems of industrial facilities were infected with the Stuxnet virus. The virus was introduced into the computer network of the Bushehr nuclear power plant, which paralyzed the plant, resulting in the suspension of Iran's nuclear program. This virus is distributed through the Windows operating system and is aimed at industrial Siemens software and hardware to cause instability of EPS operation. According to available estimates, this is the first virus created to disrupt real infrastructure facilities such as power plants, waste-water treatment facilities, and industrial plants. Such cyberattacks, based on the invasion of a computer virus targeting industrial power plants, introduce new threats into both cyber systems and physical systems [19].
3. On April 27, 2016, in Germany, the computers of the Gundremmingen nuclear power plant (120 km from Munich) operated by the utility RWE were infected with viruses W32. Ramnit and Conficker. The malware was detected on 18 removable media in the computer system of the plant's B unit, in its data visualization software. The infection did not pose a threat to the safety of the nuclear power plant, since the computers controlling the nuclear power plant systems are not connected to the Internet.

On August 14, 2003, most of the Midwest and North-East USA and Ontario, Canada experienced a power outage that in some regions lasted up to 4 days and affected about 50 million people. In total, 61.800 MW of electrical load was disconnected [20]. According to experts, the reasons for this large-scale shutdown are not directly related to malicious activities of cybercriminals; they were caused by errors in the cyber system software [20].

The above incidents show that external cyber threats are the most common causes of emergencies at power facilities (all but the last example). The following section will provide an overview of studies in Russia and abroad on counteracting external cyber threats. As for internal cyber threats, for the information-and-communication subsystem, as noted in [21], until recently, this aspect has not been associated with the issue of cybersecurity of cyber-physical EPSs. Further, the fourth section of this paper provides a brief overview of the research findings in this area.

IV. Areas of research to counteract external cyber threats

In general, the problem of countering deliberate external cyberattacks is formulated as follows. First of all, one shall identify the most vulnerable points of the information-and-communication subsystem of the EPS in both its components: compiling information for monitoring of operating conditions and control over them (data collection and processing, system state estimation, and others);

development and implementation of control actions (identification, transfer, execution). The most vulnerable point of the given subsystem is identified by simulating cyberattack scenarios that vary depending on the location of their application (data transfer channels, state estimation algorithms, algorithms for developing control actions, and others). Specific measures are envisaged for each of the most vulnerable points or groups thereof to prevent severe consequences for the EPS [22 - 24, etc.].

One of the most common cyberattack scenarios is the false data injection into the EPS state estimation procedure [22]. The state estimation procedure [25] is one of the most important ones in the operational control of the EPS. The results of its calculations serve as the basis for maintaining the current operating conditions of the EPS, planning repair conditions, and making projections. The system state variables, parameters, and topology can be corrupted. The main goal is to make it difficult to identify false data injection by conventional algorithms. We consider the consequences of cyberattacks of this type for the operation of algorithms of electricity market management, algorithms of optimal power flow, and others. To understand "the inner workings" of the mechanism of the data corruption impact on the state estimation and to develop measures to counteract it, researchers model the false data injection process. Thus, in [26, 27], the false data injection scenario is formalized as a combinatorial problem on the graph by minimizing the number of the most affected vulnerabilities. In [28], optimization models based on mixed-integer programming of undetectable and unidentifiable attacks aimed at inputting false data into algorithms of the EPS state estimation are presented. In [29], a semi-Markov model of the false data injection cyberattack is proposed.

Cyber-initiated attacks aimed at information processing, protection, and control systems can be divided into four categories: blocking, imitation and modification, gathering, and privacy [23]. By way of illustration, let us detail the lists of the first two categories of attacks. Blocking attacks are denial of service; jamming during data transmission; sending Trojan horses (malware to trick the recipient) and the like. Imitation and modification attacks include a technique for injecting knowingly incorrect data (fuzzing); masquerading an attacker or malicious program to gain privileges by falsifying information (spoofing); reordering and mixing data (tampering); data cloning; replaying valid data, i.e., making such data resent or delayed.

Each type of cyberattack has negative consequences for the composition and content of data, which is why measures should be implemented to prevent them [23]. Possible consequences of cyberattacks may include loss of data, violation of their confidentiality, integrity, and plausibility. Potential measures to counter the cyber-attacks include antivirus programs, security protocols, passwords as barriers, data duplication, data filtering, time synchronization control for operations, the use of digital signatures to confirm data ownership, and some others.

In terms of countermeasures against cyberattacks, it is important to assess the probability of the success of the attack. For this purpose, two Bayesian graphical models of cyberattacks are presented in [30] for EPS vulnerability assessment. The ultimate goal of any cyberattack on the ICS is to disable physical elements of the cyber-physical EPS. From an attacker's point of view, substations, control centers, data transmission channels, and corporate monitoring centers are considered as potential objects of attack (vulnerability points). The identification of vulnerability points in the information-and-communication subsystem of these objects is precisely aimed at achieving the ultimate goal of a cyberattack. Different combinations of such vulnerability points produce 14 possible cyberattack scenarios. It follows from the above that an important task is the development of complex cyber-physical models (CPM) for the identification of vulnerable points of cyber-physical infrastructure and assessment of the reliability of cyber-physical EPSs and reliability of power supply to consumers [29-31, and others].

Along with computerized cyber-physical models for studies of cybersecurity of EPSs, another important direction is the development of reference physical models. One of them is presented in [32] and includes four interconnected layers: a layer of physical EPS based on the RTDS simulator with multiple ports for connecting physical measuring, protection, and control devices; a sensor layer including the above physical devices; a communication layer implemented using physical channels of data concentration, data transmission, and required protocols; a layers of applications, including, as one of them, monitoring of EPS voltage stability in real-time. In [33], the authors employ the same methodology of building a cyber-physical model (CPM) of EPS based on the application of the RTDS hardware/software simulator and real devices of protection, automatics, and other elements.

In [24], the authors study the impact of the "denial of service" cyberattack on control systems of distributed generation plants, which is aimed at causing instability of the EPS as a whole with the risk of cascading accident development. The research proposes the use of robust control of distributed generation units as a measure to counteract the cyberattack.

An original approach to counteracting cyberattacks is presented in [34] in the form of a package of support for the so-called controlled degradation of the control system of the energy facility in the event of cyber incidents. The essence of the concept is that during an incident, it is possible to consciously give up some functions of information exchange and control, leaving for pre-prepared "limits to degradation" and hence narrowing the environment where a cyber incident may develop. At the level of "maximum degradation" in cases of serious incidents, only the main protection and control functions remain at the stand-alone microprocessor operating condition and the maximum "manual" control mode.

The above analysis of key research findings relevant to the aspect of EPS cybersecurity under examination gives an idea of the state of developments in the world.

V. Key research findings by the ESI SB RAS

The efficiency of EPS control is ensured by the current regularly updated reliable information, optimal control actions developed on its basis, and their reliable execution. Hardware and software tools of SCADA-systems and WAMS, and the state estimation procedure designed to support the dispatch personnel actions in the course of the EPS operational and emergency control, are the components of the information-and-communication subsystem that are critical and at the same time most vulnerable to cyberattacks. Modern cybersecurity methods aim to prevent or reduce the impact of attacks. Attack prevention is ensured at the level of information technology experts through methods of cryptography, authentication, access control, management, and others. If these measures prove insufficient, actions should be taken to reduce the impact of attacks that occurred in the ICS on the reliability of operation of the physical subsystem.

1. Application of statistical methods of information processing in cyberattacks on information collection and processing systems (SCADA and WAMS)

The studies performed at the ESI SB RAS, along with engineering and organizational measures aimed at improving the cybersecurity of electric power facilities, propose employing statistical methods of processing the measurement information coming from SCADA systems and WAMS to analyze the vulnerability of the information-and-communication subsystem and reduce the impact of cyberattacks on the quality of physical subsystem control. First of all, these are the methods of static and dynamic state estimation [25], measurement verification [35], and other information processing methods used in EPS control.

To assess the ability of a complex engineering system to withstand cyberattacks, the concept of system vulnerability level is introduced, the numerical rating of which is a vulnerability index. In [36,37], the concept of the vulnerability index of the state estimation was introduced, with the latter characterizing the degree of exposure of its results to possible errors in measuring information when cyberattacks are directed at the SCADA system. A set of indicators descriptive of the accuracy of state estimation results was used to determine the vulnerability index. Since these indicators are non-deterministic, the apparatus of the fuzzy sets theory is used to estimate the vulnerability index [38]. It is shown that the joint use of SCADA and PMU measurements for EPS state estimation allows increasing the efficiency of methods for bad data detection and accuracy of obtained estimates, thus reducing the vulnerability of the state estimation task to cyberattacks [39].

A method proposed in [40] for processing and verification of information streams of synchronized phasor measurements (SPMs) involves a wavelet analysis of random processes, which allows detecting both systematic errors and interference maliciously created by cyberattacks. The WAMS structure was studied, vulnerabilities were identified, and possible cyberattacks were analyzed. Attacks of false data injection into the information flows of SPM were modeled, the probability characteristics of distorted data and data not exposed to malicious data streams were analyzed. The SPMs were verified using the wavelet theory.

The study in [41,42] suggests the use of dynamic state estimation algorithms and measurement verification for the detection and correction of data distorted due to cyberattacks in the case of low measurement redundancy. Consideration of the dynamics of changes in the EPS state imparts substantially new properties to the state estimation algorithms, including the ability to work under insufficient information, higher robustness to failures and interference, the ability to adapt and predict. The dynamic state estimation offers more opportunities to detect gross and systematic errors in telemetry due to the use of retrospective and predictive information about the parameters of the operating conditions [42].

2. Application of the attack tree technique to analyze the cyber vulnerability of EPS facilities [43,44]

The digital substation (DSS), which is one of the pilot digitalization projects in the electric power industry, was assumed as the object of the cybersecurity study. The study proposes the use of the concepts of "cyber resilience" and cybersecurity indicators to analyze the ability of the DSS to withstand cyberattacks and restore its performance after exposure to them. The structure of the digital substation is studied for the cyber-physical system, and factors influencing the extent of reduction of the digital substation functionality due to cyberattacks are analyzed. Some known cyberattacks were considered, including "denial of service" (DoS-attack), the introduction of viruses and software with "implants", masquerading GPS signals/stream of transient values (SV stream)/MMS and GOOSE messages, traffic overflow, and others, which are direct threats to DSS performance. The consequences for the DSS cybernetic and physical subsystems under various cyberattacks were analyzed, and measures were proposed for these subsystems to counter cyberattacks.

To coordinate DSS vulnerabilities and cybersecurity threats with measures to counter possible malicious attacks, the study employed the fault tree analysis technique used in the reliability theory of complex engineering systems. As a result, a tree of attacks was formed to analyze the DSS cybersecurity. A tree of attacks can be clearly compiled for each substation. This provides an opportunity to analyze the DSS information-and-communication system with respect to the presence of vulnerabilities, to revise the existing protective cyber-measures, and to develop a policy of further steps to improve the cybersecurity of this energy facility.

3. Risk-based approaches to cybersecurity analysis

Theories based on the concept of risk are an important direction in solving the problems of cybersecurity [45]. The risk-based approach takes into account the harm due to damage or destruction of a facility as a result of cyberattacks by using qualitative (complexity of restoration, destruction of the unique natural environment, reputation, etc.) and quantitative (as expressed in monetary terms) indicators, as well as the probability of damage or destruction of a facility with the possibility of cascading emergencies [46].

In [47-49], researchers propose a methodological approach to threat analysis and risk assessment of cyber-security risks in electric power infrastructure based on semantic modeling. The approach includes a system of cyber-security ontologies and a fractal stratified model of the ontology system, a technique for analyzing cyber threats in electric power infrastructure, a technique for modeling scenarios of emergencies in electric power infrastructure as caused by cyber threats, and a technique for assessing cyber-security risks in electric power infrastructure.

The architecture of an intelligent system was developed for threat analysis and assessment of cybersecurity risks in electric power infrastructure. It implements a methodological approach based on the integration of the expert system, Bayesian belief networks, and a visual risk assessment component. This methodological approach was used to develop a technique for cyber threat analysis and risk assessment. The proposed methodological approach allows developing a classification of assets and facilities of the electric power infrastructure to assess potential vulnerabilities in terms of the significance of the facilities and the level of their protection.

In [50, 51], to reveal possible operational failures of the EPS under cyberattacks the authors perform an analysis of cybersecurity risks of the ICS and their impact on control functions, as well as the related consequences for the physical subsystem of EPS.

The information-and-communication infrastructure of the EPS was examined and the cybersecurity properties of SCADA and WAMS, which are part of the infrastructure, were analyzed. An algorithm was developed to assess control risks in the event of cyberattacks on SCADA systems and WAMS. SCADA and WAMS systems were treated as assets, and control losses followed by the EPS malfunctioning were considered as damage.

The algorithm consists of two stages: the first stage is the assessment of control risks for each materialized cyber threat; the second stage is the determination of the resulting risk value.

To assess the risks of losing EPS control, a hierarchical fuzzy system was proposed, which includes four fuzzy inference systems. Factors such as the attacker's capabilities, intentions, and goals were used to assess the probability that the threat will be triggered. Combinations of factors, such as the attacker's capabilities and ICS vulnerabilities, served as the basis for assessing the probability of a threat event as a result of adverse action. A combination of these probabilities was used to determine the total probability of the threat materialization. Combinations of the probability of threat materialization and levels of impact (consequences) on SCADA systems and WAMS determine the risk value for the EPS control.

4. Ensuring serviceability of the emergency control and relay protection systems in the context of cyberattacks

In the context of EPS operation under cyberattacks, it is essential to provide the cybersecurity of automatic control systems, including relay protection (RP) devices, the operation and emergency control automatics (ECA) systems, and the automated process control systems (PCS). To this end, the studies performed at the ESI SB RAS [52-55] examined not only the problems of hacker attacks but also the entire array of problems related to the adequate operation of cybernetic systems in EPSs.

The key elements of RP and ECA systems, as noted in [29], as applied to main facilities, i.e., digital substations that can be exposed to cyberattacks with severe consequences, are communication networks, process buses, facility buses, digital systems of RP, ECA, monitoring and control devices, and external digital channels. The researchers propose identifying critical functions of protection and automatic systems and duplicate them on a non-digital basis as the "last tier" of protection, thus excluding the very possibility of cyberattacks on them [53, 54]. Other RP and ECA systems should be able to operate not only in integrated digital information systems but also in a stand-alone isolated condition during the period of a cyberattack or its threat, as well as during the EPS restoration. This "last tier" proposal is practically consistent with the concept of the "controlled degradation" studied in [34].

The research in [53, 54] suggests creating a simulation subsystem at the energy facilities that would automatically simulate the operation of automatic control devices, verifying the adequacy of their work based on information from the emergency event recorders (EER), automatic remote control, and other sources. Given that the hardware and software base of such a simulation subsystem would differ from the hardware and software base of the implementation of RP and ECA devices, in case of cyberattacks, there would be different behavior of real and simulation subsystems observed, which would make it possible to identify cyberattacks as well as to identify potential errors in software algorithms.

The factor of potential algorithm errors realized in the form of software for digital RP and ECA systems is of grave importance and forms internal cyber threats for the information-and-communication subsystem. In [21], this problem is illustrated by case studies of large-scale blackouts of cascade nature in the UES of Russia in recent years. An analysis of the blackouts of August 22, 2016 [55] and June 27, 2017. [7] indicates that the shortcomings of control system algorithms increase the scale of consequences when local accidents become system-wide.

VI. Conclusion

The case studies of real-life cyberattacks on electric power facilities and systems given in the paper testify to the urgency of the

EPS cybersecurity issue. The issue of cyber resilience of energy facilities and EPSs as a whole is a critical and urgent problem that should be addressed from the cyber-physical standpoint in conjunction with physical and information-and-communication subsystems.

Recent years have seen much effort put in the field of EPS cybersecurity. Analysis of the current state of research indicates a strong interest in this problem and demonstrates significant results in identifying vulnerabilities of the information-and-communication subsystem of the EPS and developing cyber-physical models of the EPS to study the consequences of cyberattacks.

The studies performed at the ESI SB RAS employ statistical methods of data processing to analyze vulnerabilities of the information-and-communication subsystem and reduce the impact of cyberattacks on the quality of control of the physical subsystem of the EPS. The researchers propose applying the methods for verification of the information coming from SCADA systems and WAMS, including the wavelet method, to perform static and dynamic EPS state estimation procedures. The efficiency of cyberattack detection is shown to increase with the combined use of data from SCADA and WAMS. Vulnerability analysis is also performed by building an attack tree for electric power facilities.

The substantiation of measures to counter cyber threats and reduce the negative consequences of their possible materialization involves a risk-based approach for determining the damage from the consequences of materialized cyberattacks. An algorithm was developed to assess control risks under cyberattacks on SCADA systems and WAMS.

Ensuring cybersecurity of automatic control systems, such as relay protection devices, operation and emergency control automatics, and automated process control systems also proves an urgent task in the operation of EPSs under cyberattacks. To fulfill the task, the studies performed at the ESI SB RAS examined not only the problems of hacker attacks but also the entire array of problems of adequate operation of cybernetic systems in the electric power industry.

The process of digitalization of electric power systems; the use of intelligent technologies and complex engineering, information, and communication equipment have increased the cybersecurity risks of EPSs and energy companies. These point to the need to continue multi-faceted studies in this direction so that the recommendations they are to produce would ensure the required level of cybersecurity of digital intelligent EPSs.

References

[1] Voropai N.I., Gubko M.V., Kovalev S.P., et al. Problems of digital energy development in Russia, Problemy upravleniya. – 2019. – No. 1. – P. 2–14. (in Russian)

[2] Koshcheev L.A. On the use of digital technology in the electric power industry, *Izvestiya* NTC Edinoj energeticheskoj sistemy. – 2019. – No. 1 (80). – P. 47–56. (in Russian)

[3] Jin Wei, Kundur D. Two-tier hierarchical cyber-physical security analysis framework for smart grid, IEEE PES *General Meeting*, San Diego, USA, July 22 – 27, 2012, 5 p.

[4] Khaitan S.K., McCalley J.D. Cyber-physical system approach for the design of power grids, IEEE PES *General Meeting*, Vancouver, Canada, July 21 – 25, 2013, 6 p.

[5] Voropai N.I., Kolosok I.N., Korkina E.S., Osak A.B. Issues of vulnerability and survivability of cyber-physical electric power systems, *Energy Policy*. 2018. No. 5. Vol. 53–61. (in Russian)

[6] Papkov B.V., Kulikov A.L., Osokin V.L. Cyber threats and cyberattacks in the electric power industry: a study guide. Nizhny Novgorod: Nizhny Novgorod branch of the Russian Presidential Academy of National Economy and Public Administration, 2017, 80 p. (in Russian)

[7] Voropai N.I., Efimov D.N., Mayakov D.V., et al. Accident in the Unified Energy System of Siberia on June 27, 2017., *Methodological issues of studies of large energy systems reliability.* Issue 69. Book 2. Irkutsk: ESI SB RAS. – 2018. – P. 208–218. (in Russian)

[8] Joint United States - Canada electric grid security and resilience strategy (https://www.whitehouse.gov/sites/whitehouse.gov/files/images/Joint_US_Canada_Grid_Strategy_06Dec2016.pdf).

[9] The doctrine of information security of the Russian Federation (Approved by Decree of the President of the Russian Federation, No. 646 of December 5, 2016, http://kremlin.ru/acts/news/53418). (in Russian)

[10] Massel A.G. Cyberattacks as a threat to Russia's energy security, Proceedings of the international conference "Cybersecurity-2013". Ukraine, Kyiv, Institute of Special Communication and Information Security, National Technical University of Ukraine, “Igor Sikorsky Kyiv Polytechnic Institute”. 2013. No. 1 (3). P. 49-56. (in Russian)

[11] Massel L.V., Voropai N.I., Senderov S.M., Massel A.G. Cyberhazard as a strategic threat to energy security, *Voprosy kiberbezopasnosti*. No. 4 (17). 2016. – P 2-10. (in Russian)

[12] T-REC-X.1205 – ITU-T: Overview of cybersecurity [Electronic publication]. URL: https://www.itu.int/rec/T-REC-X.1205-200804-I (Accessed on May 16, 2019).

[13] ISO/IEC 27032:2012. Information technology. Security techniques. Guidelines for cybersecurity.

[14] Massel L.V. Adoption of modern information technology in Smart Grid as a threat to cybersecurity of energy systems of Russia / Information technology and security. – Ukraine, Kyiv, Institute of Special Communication and Information Security, National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute", No. 1 (3) 2013. – P. 56-65. (in Russian)

[15] https://iot.ru/energetika/kiberbezopasnost-v-energetike-kak-pobedit-nevidimogo-vraga

[16] Massel A.G., Gaskova D.A. Methods, and approaches to ensuring the cybersecurity of digital energy facilities, Energeticheskaya politika. – 2018. – No. 5. – P. 62-72. (in Russian)

[17] Nekrasov V. Blackout Kyiv: what the cyberattack on Kyiv's power grid is fraught with and who is behind it. *Ekonomichna Pravda*, June 15, 2017. Published 07:20 June 16, 2017. (in Russian)

[18] Fedunenko E., Chernysheva E. Cyberattacks on nuclear facilities. Historical background// *Kommersant newspaper*. No. 10, dated January 20, 2017. (in Russian)

[19] Cherry S., Langner R. How Stuxnet Is Rewriting the Cyberterrorism Playbook, *IEEE Spectrum*, 2010, No. 10, pp. 33 – 34.

[20] U.S.- Canada Power System Outage Task Force, Final Report on the August 14, 2003 Blackout in the United States and Canada: Causes and Recommendations, April 2004. online: https://reports.energy.gov/BlackoutFinal-Web.pdf

[21] Osak A.B., Panaseckij D.A., Buzina E.Ja. Reliability of emergency control automatics and relay protection from a cybersecurity perspective, M*ethodological issues of studies of large energy systems reliability. Issue* 69. Book 2. Irkutsk: SEI SB RAS, 2018. P. 99–108. (in Russian)

[22] Liang G., Zhao J., Luo F., Weller S.R., Dong Z.Y. A review of false data injection attacks against modern power systems, *IEEE Trans. on Smart Grid*, 2017. V.8(4), pp. 1630–1638.

[23] Holstein D.K., Cease T.W., Seewald M.G. Application and management of cybersecurity measures for protection and control, *CIGRE 2016* Session, Paris, France, August 25 – 30, 2016. 9 p.

[24] Srikantha P., Kundur D. A DER attack- mitigation differential game for smart grid security analysis, *IEEE Trans. on Smart Grid*. 2016. V. 7(3). pp. 1476–1485.

[25] Gamm A.Z. Statistical methods of state estimation of electric power systems. - Moscow: *Nauka*, 1976. 220 p. (in Russian)

[26] Yamaguchi Y., Ogava A., Takeda A., Iwata S. Cybersecurity analysis of power networks by hypergraph cut algorithms, *IEEE Trans. on Smart Grid*. – 2015. V. 6(5), pp. 2189–2199.

[27] Khokhlov M.V. Vulnerability of EPS state estimation to cyberattacks, *Methodological issues of studies of large energy systems reliability*. Issue 65. Irkutsk: SEI SB RAS. 2015. pp. 557–566. (in Russian)

[28] Khokhlov M.V. Optimization models of undetectable and unidentifiable FDI-attacks, *Methodological issues in studies of the reliability of large energy systems.* Issue 67. Syktyvkar: Komi Republican Printing Office. 2016. pp. 366–376. (in Russian)

[29] Xiang Y., Ding Z., Zhang Y., Wang L. System reliability evaluation considering load redistribution attacks, *IEEE Trans. on Smart Grid*. 2017. V.8(2).pp. 889–901.

[30] Zhang Y., Wang L., Xiang Y., Ten Ch.-W. Power system reliability evaluation with SCADA cybersecurity considerations, *IEEE Trans. on Smart Grid*, 2015. V.6(4). pp. 1707–1721.

[31] Davis K.R., Davis Ch.M., Zonouz S.A., e.a. A cyber-physical modeling and assessment framework for power grid infrastructures, *IEEE Trans. on Smart Grid*. 2015. V. 6(5). pp. 2464–2475.

[32] Liu R., Vellaithurai C., Biswas S.S., e.a. Analyzing the cyber-physical impact of cyber events on the power grid, *IEEE Trans. on Smart Grid.* 2015. V. 6(5). pp. 2444–2453.

[33] Arhangelskij O.D., Voloshin A.A., Ivanov F.A. On the cyber-physical model for information security research in the electric power industry //https://ennlab.ru/wp-content/uploads/2018/06/Statya-O-kiberfizicheskoy-modeli-dlya-issledovaniy-informatsionnoy-bezopasnosti-v-elektroenergetike.pdf. (in Russian)

[34] Nazarov I.G., Suslov D.V., Nikandrov M.V., Slavutskij L.A. A system of ensuring controlled degradation of the energy facility control system in the event of cyber incidents, *Vestnik Chuvashskogo universiteta*. 2018. No. 1. pp. 146–152. (in Russian)

[35] Gamm A.Z., Kolosok I.N. Detection of gross telemetry errors in electric power systems. – *Novosibirsk: Nauka*, 2000. 152 p. (in Russian)

[36] Kolosok I., Gurina L. Calculation of cybersecurity index in the problem of power system state estimation based on SCADA and WAMS measurements, Proc. of the 9th Intern. Conf. on Critical Information Infrastructures Security CRITIS 2014, Limassol, Cyprus, October 13-15, 2014, Revised Selected Papers. Editors: Panayiotou, C.G., Ellinas, G., Kyriakides, E., Polycarpou, M.M. (Eds.). Security and Cryptology © .2016. pp. 172 – 177.

[37] Kolosok I.N., Gurina L.A. Determination of the index of vulnerability to cyberattacks for the problem of state estimation using SCADA data and synchronized vector measurements, *Elektrotekhnika*, 2017, No. 1, pp. 52-59. (in Russian)

[38] Bogatyrev L.L., Manusov V.Z., Sodnomdorzh D. Mathematical modeling of operation modes of electric power systems uncertainty – Ulaanbaatar: *Publishing house of the printing office of Bauman Moscow State Technical University*, 1999. 348 p. (in Russian)

[39] Kolosok I.N., Korkina E.S. Decomposition of power system state estimation problem as a method to tackle cyber-attacks / The 1st IEEE International Conference ICPS-2018, Saint-Petersburg, Russia, May 15-18, 2018, SF-004928

[40] Kolosok I.N., Gurina L.A. Verification of synchronized vector measurement data in the event of cyberattacks on WAMS, Informacionnye i matematicheskie tekhnologii v nauke i upravlenii. 2017. No. 1 (5). pp. 19–29. (in Russian)

[41] Clements K. A., Krumpholz G.R., Davis P.W. Power system state estimation with Measurement Deficiency: An observability/measurement placement algorithm, *IEEE Trans. on Power Systems*. 1983. Vol. PAS 102, № 7, pp. 2012-2020.

[42] Glazunova A.M., Kolosok I.N., Syomshchikov E.S. Detection of erroneous data in the measuring information by methods of dynamic state estimation when controlling an intelligent energy system., *Elektrichestvo*, 2017, No. 2, pp.18–27. (in Russian)

43] Voropai N.I., Kolosok I.N., Korkina E.S. Problems of increasing the cyber resilience of the digital substation, Relejnaya zashchita i avtomatizaciya. 2019. Vol. 34. No. 1. pp. 78-83. (in Russian)

[44] Kolosok I.N., Korkina E.S. Cybersecurity analysis of the digital substation from a cyber-physical system perspective, Informacionnye i matematicheskie tekhnologii v nauke i upravlenii, 2019, 3 (15), pp.121-131. (in Russian)

[45] Haimes Y. Systems-based risk analysis, Global Catastrophic Risks, *Nick Bostrom, Milan M. Cirkovic* (ed), Oxford, 2008, pp. 146-163.

[46] Massel L.V., Komendantova N.P. Risk assessment of natural and man-made threats to the resilience of energy, environmental, and social systems based on intelligent information technologies, *Informacionnye i matematicheskie tekhnologii v nauke i upravlenii.* 2019. No. 4 (16). pp. 31-45. DOI: 10.25729/2413-0133-2019-4-03 (in Russian)

[47] Massel A.G., Massel L.V., Gaskova D.A. Cybersecurity in critical infrastructures (the case of energy), Bezopasnye informatsionnye tekhnologii (BIT-2016). Proceedings of the Seventh All-Russian scientific and technical conference. Ed. by V.A. Matveev, 2016. pp. 197-199. (in Russian)

[48] Massel A.G., Gaskova D.A. Methods and approaches to ensuring the cybersecurity of digital energy facilities, Energy Policy. 2018. No. 5. pp. 62-72. (in Russian)

[49] Gaskova D.A., Massel A.G. Cyber threat analysis technique and risk assessment of critical infrastructure cybersecurity breach, *Cybersecurity Isues*. 2019, No. 2 (30). pp. 42-49. (in Russian)

[50] Kolosok I.N., Gurina L.A. Cybersecurity risk assessment of information-and-communication infrastructure of the intelligent energy system, Informatsionnye i matematicheskie tekhnologii v nauke i upravlenii. 2019. No. 2 (14). P. 40-51. DOI: 10.25729/2413-0133-2019-2-04 (in Russian)

[51] Kolosok I.N., Gurina L.A. Assessment of risks of EPS control in the event of cyberattacks on the information-and-communication infrastructure of the cyber-physical system, Methodological issues of studies of large energy systems reliability. Book 1 / Ed. by N.I. Voropai. Irkutsk: *ESI SB RAS*, 2019, pp. 238-247. (in Russian)

[52] Osak A.B., Panasetsky D.A., Buzina E.Ja. The impact of cybersecurity of electric power industry facilities on the reliability of EPS operation, Methodological issues of studies of large energy systems reliability. Issue 67. Syktyvkar: *Komi Republican Printing Office*. 2016. pp. 377–385. (in Russian)

[53] Osak A.B., Panasetsly D.A., Buzina E.Ja. Ensuring serviceability of the systems of emergency automation and relay protection in the context of cyberattacks, Proceedings of the International Conference *"Relay protection and automation of energy systems"*, St. Petersburg, Russia . 2017. 6 p. (in Russian)

[54] Osak A.B., Panasetsky D.A., Buzina E.Ja. Improving the reliability of packaged systems of emergency automatics and relay protection under cyberattacks, Methodological issues of studies of large energy systems reliability. Issue 68. Irkutsk: *ESI SB RAS.* 2017. pp. 274–282. (in Russian)

[55] Voropai N.I., Osak A.B., Smirnov S.S. Analysis of the 2016 system accident in the UES of Russia caused by equipment damage at the Reftinskaya GRES power plant, *Elektrichestvo*. 2018. No. 3. pp. 27–32. (in Russian)

Nikolai I. Voropai is Professor, President of Melentiev Energy Systems Institute of the Russian Academy of Science, Irkutsk, Russia. He is the Corresponding Member of the Russian Academy of Sciences.

He graduated from Leningrad (St. Petersburg) Polytechnic Institute in 1966. N.I. Voropai received his degrees of Candidate of Technical Sciences at the Leningrad Polytechnic Institute in 1974 and Doctor of Technical Sciences at the Siberian Energy Institute in 1990. His research interests include modeling of power systems operation, dynamics performance and control of large power grids; reliability and security of power systems; development of national, international and intercontinental power grids; smart grids; power industry restructuring.

Irina N. Kolosok graduated from St. Petersburg Technical University. Since 1972 she has been with Energy Systems Institute (ESI), Russian Academy of Sciences, currently as a leading researcher. She received the Ph.D (1986) and D.Sc (2004) degrees. Her scientific interests are: real-time control problems, especially in the field of state estimation of electric power systems (EPS), SCADA systems, application of AI-methods for on-line EPS control, EPS cyber security, EPS flexibility, cyber-physical systems.

Elena S. Korkina graduated from Irkutsk Polytechnic Institute on speciality of an engineer-economist in 1978. Since 1987 she has been working at the ESI, SB RAS in the laboratory of electric power system operation control problems. She received the Ph.D in 2009 on "Development of methods for state estimation of electric power systems based on data integration of SCADA and PMU". Her scientific interests are: real-time control problems, SCADA systems, WAMS, EPS state estimation, EPS cyber security, EPS flexibility, cyber-physical systems

Alexey B. Osak graduated power faculty from Irkutsk Technical University in 1998. He is a Researcher, Head of Sector in the Laboratory of control of abnormal operating conditions in electric power systems of the Melentiev Energy Systems Institute of Siberian Branch of the Russian Academy of Sciences.

His research interests are modeling of electrical modes of power systems, justification of the development of electric networks, electric power systems security, control of normal and emergency conditions of electric power systems.