Integration of Cyber Security into the Smart Grid Operational Risk Management System*

Alexander V. Olifirov[1][0000-0002-5288-2725], Krystina A. Makoveichuk[1][0000-0003-1258-0463] and Sergei A. Petrenko[2][0000-0003-0644-1731]

[1]V.I. Vernadsky Crimean Federal University, Yalta, Russia
alex.olifirov@gmail.com
christin2003@yandex.ru
[2]Innopolis University, Kazan, Russia
s.petrenko@rambler.ru

Abstract. The article shows that the transition of the electricity industry to technological innovation based on the new paradigm - Smart Grid - leads to an increase in cyber threats. The dependence of operational risks in the electric power company on information security risks was identified, taking into account direct and indirect losses from the implementation of cyber threats. The classification of cyber risks is carried out, approaches to their assessment are investigated, and the interaction of the structural units of the company in the implementation of cyber threats, the assessment of cyber risks and taking countermeasures is considered. It was proposed that power companies include cybersecurity among strategic priorities and report on cybersecurity risks along with information on operational risks. The study noted that for the smart grid, cybersecurity is a strategic priority, and in this regard, it was proposed to ensure proper internal control of the cyber risk management processes, provide stakeholders with full information on cybersecurity incidents to respond appropriately. The authors have proposed to ensure the filling of a vacuum between the leading link operating in terms of business processes and operational risks, and the technical link operating in terms of cyber risks and technical and organizational means of protection against them.

Keywords: Smart Grid, operational risks, cyber risks, operational risk management services.

1 Introduction

Currently, in Russia, in the conditions of digitalization of the economy, there is a certain interest in the actively developing worldwide in the last decade, the direction of the transformation of the electric power industry based on the concept of Smart Grid. Smart Grid is interpreted as the concept of modernization of the electric power industry, as it

is based on the revision of a number of existing basic rules and principles of modernization of the industry.

The principles of developing smart grids are defined through the Smart Grid European Technology Platform [15].

The introduction of the Smart Grid concept provides for the development of smart grid technology and means a fundamental technological reorganization of the electric power industry. A network operating on the basis of the Smart Grid concept is capable of identifying the damaged area itself, de-energizing it and automatically powering consumers who are briefly left without electricity. Controllers with freely programmable logic implement algorithms for configuring consumer power circuits in various emergency situations and provide network automation. However, by providing great opportunities, a smart energy network carries great risks for consumers and owners, which is due to the size of the company and the high cost of risk-prone assets.

Energy companies are characterized by both general risks and specific to one or another type of activity, depending on the scope of their functioning. In the information systems of network companies, risks can be identified and enhanced at any point in the life cycle of these systems, from the decision to develop a system to the commissioning of the system for commercial operation. However, the methods of creating information systems cannot be separated from the main goals of entrepreneurial activity and cannot be unrelated to environmental influences and limitations [3].

The purpose of this article:

1. to investigate in the electric power company the processes of integrating information security (IS) risks (cyber risks) into operational risks (OR);
2. to study the interaction of the departments of the electric power company in the process of risk management during the implementation of cyber threats;
3. define the management of cyber risks as a priority strategic direction for the development of the electric power company in its transition to the new paradigm - Smart Grid.

2 The main part of the study

Information systems are created in order to prevent the operational risks of the electricity company. This risk may be in the form of an increase in the cost of services provided, a decrease in income. Information systems of electric companies should reduce these risks, increasing the effectiveness of managers' actions, based on mathematical models for optimizing risks and methods for managing cyber risks at various levels: enterprise, regional, federal [4, 5, 6].

However, information systems that are designed to prevent operational risks independently carry the risks of increasing cash costs for the system and the deterioration of the company's work associated with putting the system into operation. Figure 1 shows a diagram of the risk flows in various fields that affect the information system of a network company.

Operational risk includes information security risk. The risk of information security includes cyber risk and other risks of information systems.

Cybersecurity should be part of the corporate philosophy, and for this, it should at least be integrated into the business development strategy and the business risk management system (operational risks), by analogy with the approach to managing operational risks in the banking sector (BASEL III) [10, 16].

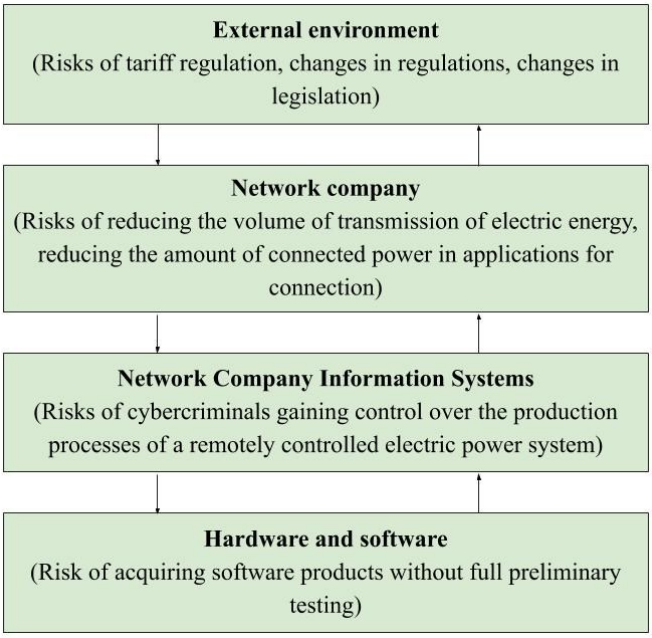

Fig. 1. Risk flows of the electricity company information system

The main goals of specialized standards and recommendations for managing cyber risks include [17, 18, 19]:

- filling a vacuum between the management link, operating terms of business processes, business continuity and sustainability, and the technical link, operating terms of vulnerabilities and technical/organizational means of protection against them;
- identification of organizational and technical measures necessary and sufficient for the proper provision of cybersecurity.

Key terms in this area are [12, 13, 14]:

- cyber risk (cyber risk) - a combination of the probability of an event and its consequences; cyber risk in the electric power industry - the risk of deliberate exposure to employees of the electric power organization, third parties, internal or external information systems aimed at unauthorized receipt, modification, deletion of data and other digital information or the data structure, parameters and characteristics of systems and access modes, through digital infrastructure and technologies communica-

tions, including through the implementation of computer attacks. An additional classification of IS risk sources by types of computer attacks can be carried out: in the context of areas of computer attacks; types of computer attacks; by types of attacked objects;

- cyber risk management is a set of coordinated measures to manage the organization (both components of the information infrastructure and resiliency and cybersecurity tools, and the entire management vertical as a whole) in order to minimize the total cyber risk;
- assessment of cyber risk (in this case, the resulting measure of probability and damage can be expressed either qualitatively - 3/4/5 degrees, or quantitatively - the probability in the average expected the frequency of occurrence of the event in a given time interval (month/year) and damage in monetary terms). One of the main results of the cyber risk assessment process is their prioritization, according to the degree of the potential impact on the company's assets.

In this case, the assessment of cyber risks is carried out using:

- expert assessments (directly (explicitly) or indirectly - using special software and hardware, the logic of which contains some knowledge base about the dependence of a measure of cyber risk on the observed conditions);
- historical information about the likelihood of the vulnerability and damage from its implementation (the disadvantages of the method are the need for a sufficiently large amount of historical data (and for some threats they may simply not exist) and the inability to accurately assess the trend in the event of a changing situation, which we observe in almost all areas of cybersecurity);
- analytical approaches (which are mostly in academic development), for example, with the construction of weighted transition graphs to determine the magnitude of the damage from the implementation of the vulnerability.

Measures aimed at countering cyber risk (reducing the overall risk of an organization) include:

- passive actions:
    - adoption of cyber risk (decision on the acceptability of the observed level of a given cyber risk without any countermeasures);
    - evasion of cyber risk (decision on the transformation of activities that would entail a given level of cyber risk);
- active actions:
    - limitation or reduction of a specific cyber risk (consists of a set of organizational and technical measures that we are used to taking as measures to ensure information security);
    - risk transfer (insurance) is still a rather rare procedure, which gradually gains recognition;

— a set of measures for internal audit and internal and external monitoring of the state of cyber resistance (cybersecurity). First of all, they check the quality of the implementation of measures to reduce cyber risks, their adequacy, their performance of the target function in the course of internal changes in the company, and only then they assess the changing external environment (the emergence of new types of threats and new ways of implementing the already known). In all cases, if a significant discrepancy is found between the current situation and the measures taken, the monitoring subsystem should initiate a partial or full review of the company's policy regarding information security measures [7, 9].

The power company Federal Grid Company of Unified Energy System (FGC UES, PJSC) provides half of Russia's total energy consumption due to the electricity transmitted through its networks. FGC UES, PJSC is one of the largest enterprises in the electric power industry, rendering services in the transmission and distribution of electric energy, in connection to electric networks and in the collection, transmission, and processing of technological information, including measurement and accounting data. This company implements certain elements of the Smart Grid concept. This electric power company has an operational risk management system (hereinafter referred to as the "ORMS"). The goal of the ORMS is to ensure sustainable continuous operation and development of the company by timely identification, assessment and effective management of risks that pose a threat to the effective conduct of business activities and the company's reputation, the health of employees, the environment, and the property interests of shareholders and investors [8, 11].

For the initial analysis of cyber risks, the following approaches can be used [20, 21, 23]:

— calculation of the matrix of consequences and probabilities;
— structured scenario analysis using the method "What if?" (SWIFT);
— root cause assessment method (RCA);
— business impact assessment (BIA);
— failure mode and impact assessment (FMIA);
— protection level assessment (LOPA);
— event tree analysis (ETA);
— causal analysis;
— human factor impact assessment (HRA);
— assessment of latent defects (SA), etc.

For a more in-depth analysis of cyber risks, the following can be used [23-26]:

— Delphi method;
— checklists method;
— brainstorming method;
— method of organizing a partially structured or structured interview;
— preliminary hazard analysis (PHA);
— analysis methods based on Bayesian networks;
— Monte Carlo method, etc.

And to develop a model of cyber threats [1, 27-32] can be used:

- expert assessment methods,
- methods of mathematical statistics,
- Markov methods,
- methods of event-logic approach,
- failure mode, effects and criticality analysis (FMECA),
- fault tree analysis (FTA),
- event tree analysis (ETA)
- bow-tie method, etc.

Electricity company regarding the assessment of risk indicators:

- determines quantitative and qualitative indicators of the propensity for OR for the planned annual period, including IS risk (risk appetite for OR and IS);
- sets the target levels of these indicators: signal (acceptable) level and control (limit) level;
- calculates and substantiates the signal and control values of risk appetite indicators when approving a risk and capital management strategy.

The FGC UES approved a register of 19 key operational risks, assesses their impact on the achievement of the Company's performance targets, annually updates the materiality level and takes measures to manage risks.

The company uses three methods of responding to risks: risk avoidance; risk-taking; reduction or transfer of risk (Fig. 2). The choice of risk response method depends on the significance of the risks.

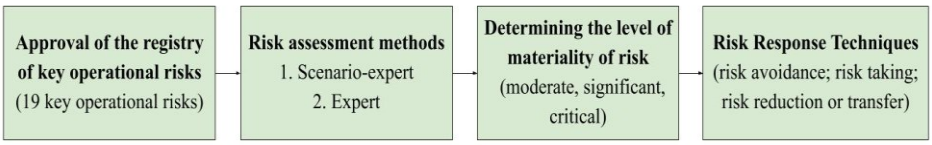

Fig. 2. Risk Assessment and Management Scheme in an Electricity Company

Risks of a critical level are unacceptable for the company and are subject to priority management. Risks with a critical level include “The risk of deviation in the volume of electricity transmission services compared to the set value in the business plan”, “The risk of deviation in the volume of overdue receivables from the amount set in the business plan”.

Risks with a significant level include “The risk of deviations in volumes of technological connections compared to the value set in the business plan”, “The risk of not reaching the level of reliability of electricity transmission services established in tariff regulation”. Risks of a significant level are not critical, but have a significant impact on the activities of the company and are subject to management.

Risks of a moderate level do not significantly affect the company's activities but are subject to periodic monitoring. Risks with a moderate level include “The risk of not

achieving the level of quality of services established by tariff regulation", "The risk of deviation from the value of the indicator of labor productivity increase established in the business plan" [11].

The operational risk management system in an electric power company consists of the following elements:

1. a specialized unit of the organization that performs operational risk management procedures - operational risk management services (ORMS);
2. a specialized unit of the organization that performs IS risk management procedures (IS service);
3. divisions - owners of the company's business processes and divisions providing the organization's business processes (hereinafter referred to as competence centers), using information technologies and carrying out risk identification, collecting information and informing about the identified risk, assessing the identified risks inherent in the processes of competence centers (in within its competence), the development and implementation of measures aimed at reducing the negative impact of operational risks and IS risks, as well as monitoring the level of operational risk and IS risk in their processes;
4. classifiers used in the operational risk and information security management system;
5. an event database containing information on events of operational risk and IS risk and losses from all types of risks;
6. benchmarks of the electric power company and a system of measures aimed at improving the quality of the information security management system and reducing the negative impact of risks;
7. an automated information system, the volume, and functionality of which is determined by the nature and scale of the operations and current processes of the electricity company.

Cyber risk integration processes in the operational risk management system can be represented as follows:

1. The information security service ensures the identification of IS incidents (IS risk events) and the identification of sources, threats, and vulnerabilities of the threat (attack) implementation, the identification of business processes, systems affected by the incident, produces an immediate response to the incident in accordance with the procedure established by the company and transmits information about the incident to the business unit and to the ORMS.
2. Units of the electric power company respond to the incident: they suspend business processes, block accounts, etc. and transmit the consequences of the incident to the ORMS.
3. The operational risk management system determines the extent and degree of impact of the incident (IS risk event) on other risks and business processes, classifies the incident according to the operational risk methodology and reflects it in the event database.

4. The operational risk management system, together with the business units and the operational risk management system, determines incident losses (IS risk events); defines measures to minimize other risks depending on the realized risk of information security.
5. The business unit provides information on losses in the information security system.
6. The information security system determines the effectiveness of measures to ensure an immediate response to an incident (IS risk event).
7. The ORMS, structural units and the information security service organize events aimed at minimizing the consequences of the implementation of IS risk (cyber risk) and other types of risk.
8. The information security service evaluates the effectiveness of measures to minimize the risk of information security (cybersecurity risk) and the level of residual risk.

To implement the processes of integrating cybersecurity into the company's operational risk management system, the bow-tie method can be used [2] (Table 1).

Table 1. Analysis of the causes and consequences of the risks of the electricity company

Analysis of the threats and measures to reduce the probability of an event				
Danger and threat	Measures to reduce the probability of an event	Is the barrier new or existing?	Barrier Performance: B - high C- average N- low	The responsible party for the reliability of this barrier
Threat No. 1 (description)				
Risk of breach of confidentiality, unauthorized access	Measure No. 1. Administrative mechanisms to contain, prevent, detect, and mitigate risks (staff training, data encryption, system testing, polygraph testing, knowledge of the Criminal Code)	Existing	C	Department of Internal Control and Risk Management
	Measure 2. Technical and logical mechanisms for containing, preventing, detecting, and neutralizing risks (password system, system log, public key infrastructure, secure protocol, secure OS)	Existing	B	Department of Internal Control and Risk Management
	Measure 3. Physical protective equipment (physical barriers screens and means of access)	Existing	B	Department of Internal Control and Risk Management
Impact analysis and mitigation measures				
Effects	Prevention and mitigation measures	Is the barrier new	Barrier Performance: B - high	The responsible party for the reliability of this barrier

		or existing?	C- average N- low	
Consequence No. 1: (description)				
Violation of the confidentiality of the system, unauthorized access to the system, the consequences of which is the implementation of the operational risk of deviation of the volume of electricity transmission services in comparison with the set value in the business plan	Measure 1. Implementation of measures aimed at minimizing the consequences of the implementation of IS risk (cyber risk): administrative, technical, logical recovery mechanisms - procedures for the quick recovery of system files, antivirus tools, etc.	Existing	C	Department of Internal Control and Risk Management, Information Security Service
	Measure No. 2 Ensuring the functioning of the system for responding to a violation of the confidentiality of the system, unauthorized access: taking action against employees who committed a cybersecurity incident, entering the incident in the event database	Existing	C	Department of Internal Control and Risk Management, Information Security Service
	Measure No. 3 Implementation of measures aimed at minimizing the consequences of the implementation of a new IS risk (cyber risk) in the business unit of the electric power company (the consequences of deviating the volume of electricity transmission services compared to the set value in the business plan)	New	B	Department of Internal Control and Risk Management

The main advantages of using the “bow-tie” method are the ability to understand the reasons for the onset of risks and the consequences of their implementation. This method makes you think of ways to manage operational risk, taking into account the cyber risks that make up their composition and helps determine the factors for subsequent mathematical modeling of the company's operational risks. A bow-tie analysis is used to study risk based on a demonstration of a range of possible causes and consequences.

The input to the method is information on the causes of hazardous events, barriers and controls that can prevent them.

The output of the method is a table showing the main consequences of dangerous events and the barriers established to minimize and mitigate undesirable consequences.

3 Conclusions

1. Among the sectors of the electric power industry, one of the highest values of the risk indicator has information security risk (including cyber risk).
2. Electricity companies do not include cybersecurity among strategic priorities. There is no information on cybersecurity risks in their reports. In general, the share of companies that do not consider ensuring cybersecurity a strategic task, according to the survey, is 82%. And for the smartwatch, cybersecurity is a strategic priority.
3. Lack of proper internal control over the cyber risk management processes leads to the fact that cybersecurity incidents are not properly recorded in the cyber risk events database, stakeholders do not have full information, and appropriate measures are not taken.
4. For the electricity industry, operating on the basis of the smart grid concept, by analogy with the banking sector (Basel III), it is necessary to integrate cyber risk management into the company's operational risk management system.
5. This will make it possible to reflect the share of losses from cyber risks in the smart grid in the total structure of losses from operational risks in the reports of electric power companies and to establish the statistical dependence of operational risks on cyber risks.
6. Integration of cybersecurity will also help to better organize the interaction of structural units of the company for risk management, taking into account the fact that cyber risk manifests itself in a computer network, and its economic evaluation is carried out in a functional unit based on the results of operations.
7. The operational risk management system of the electricity company operates at strategic, tactical and operational levels. Therefore, cybersecurity should be integrated into the business development strategy at all levels of management, to make it part of the corporate philosophy.
8. The integration of cyber risk management into the company's operational risk management system requires a scientific synthesis of the systematization and optimization of cyber risk management processes according to internal capital adequacy assessment procedures (ICAAP) in case of their economic feasibility (Basel II). In this case, mandatory internal processes are implemented: significant risks are identified, risk appetite is established, economic capital is calculated, daily, monthly, quarterly and annual reports are compiled (indicating the volumes of significant risks), stress testing is carried out and the organization of the functioning of the risk management service is specified with ensuring the full implementation of the functions of risk policy and risk reporting.
9. It is necessary to organize proper internal control of the cyber risk management processes, in which all cybersecurity incidents are properly recorded in the cyber risk event database, stakeholders receive full information and take appropriate measures.
10. To implement the processes of integrating cybersecurity into a company’s operational risk management system, the “bow-tie” method can be used, which makes you think of ways to manage operational risk taking into account the cyber risks

included in it, and helps determine factors for the subsequent mathematical modeling of operational and information risks electricity company.

References

1. Sergei Petrenko, Big Data Technologies for Monitoring of Computer Security: A Case Study of the Russian Federation, Springer International Publishing AG, part of Springer Nature 2018, e-book, 271 p. DOI: 10.1007/978-3-319-79036-7
2. GOST R ISO / IEC 31010-2011. “Risk management. Methods of risk assessment”. (In Russian).
3. OlifirovA.V. Modeli upravleniya riskami ekonomicheskih informacionnyh sistem // Informacionnye sistemy i tekhnologii v modelirovanii i upravlenii: sbornik materialov vserossijskoj nauchnoprakticheskoj konferencii. – YAlta: Gumanitarno-pedagogicheskaya akademiya (filial) FGAOU VO «KFU im. V.I. Vernadskogo. 2017.– S. 465-470. (In Russian).
4. Olifirov A.V. Strategicheskoe razvitie regional'nyh finansovyh informacionnyh sistem i tekhnologij // Informacionnye sistemy i tekhnologii v modelirovanii i upravlenii: sbornik materialov vserossijskoj nauchno-prakticheskoj konferencii (23-24 maya 2016 g.). Gumanitarno-pedagogicheskaya akademiya (filial) FGAOU VO «KFU im. V.I. Vernadskogo» v g. YAlte; Sankt-Peterburgskij gosudarstvennyj elek-trotekhnicheskij universitet "LETI". 2016. – S. 238-244. (In Russian).
5. Kobec B. B., Volkova I. O. Innovacionnoe razvitie elektroenergetiki na baze kon-cepcii Smart Grid. — M.: IAC Energiya, 2010. — 208 s. (In Russian).
6. Risk-menedzhment. Metody ocenki riska: uchebnoe posobie / V. M. Kartvelishvili, O. A. Sviridova. – Moskva: FGBOU VO «REU im. G. V. Plekhanova», 2017. – 120 s. (In Russian).
7. Barabanov A. V., Dorofeev A. V., Markov A. S., Cirlov V. L. Sem' bezopasnyh informacionnyh tekhnologij [Tekst] / Pod red. A. S. Markova. - Moskva: DMK, 2017. - 221 s. (In Russian).
8. Ghansah I. Smart grid cybersecurity potential threats, vulnerabilities and risks // Public Interest Energy Research, Prepared for California Energy Commission, 2012. DOI: 10.1016 / j.jesit.2018.01.001
9. Olifirov, A.V., Makoveichuk, K.A., Zhytnyy, P.Y., Filimonenkova, T.N., Petrenko, S.A. Models of Processes for Governance of Enterprise IT and Personnel Training for Digital Economy / 2019 Proceedings of 2018 17th Russian Scientific and Practical Conference on Planning and Teaching Engineering Staff for the Industrial and Economic Complex of the Region, PTES 2018 c. 216-219 DOI: 10.1109/PTES.2018.8604166
10. Petrenko, S.A., Makoveichuk, K.A. Ontology of cybersecurity of self-recovering smart Grid / CEUR Workshop Proceedings 8th All-Russian Scientific and Technical Conference on Secure Information Technologies, BIT 2017; Moscow; Russian Federation; 6-7 December 2017. - Volume 2081, 2017, Pages 98-106.
11. Integrirovannyj godovoj otchyot Publichnogo akcionernogo obshchestva «Federal'naya setevaya kompaniya Edinoj energeticheskoj sistemy» za 2018 god [Elektronnyj resurs]. – Rezhim dostupa: < https://report2018.fsk-ees.ru/?/ru/59-information-on-the-report >. Data obrashcheniya: 11 oktyabrya 2019. (In Russian).
12. Homeland Security Presidential Directive - 7, Critical Infrastructure Identification, Prioritization, and Protection, December 17, 2003. Available at: https://www.dhs.gov/homeland-security-presidential-directive-7 (Accessed 07 November 2019).

13. Homeland Security Presidential Directive - 20/National Security Presidential Directive - 51, National Continuity Policy, May 9, 2007. Available at: https://fas.org/irp/offdocs/nspd/nspd-51.htm (Accessed 07 November 2019).
14. Hughes. R. B. (2009) Atlantisch Perspectief,.Ap:2009 Nr. 1/4, NATO and Cyber-Defense: Mission Accomplished, Netherlands, Netherlands Atlantic Committee. Available at: https://www.atlcom.nl/site/english/nieuws/wp-content/Hughes.pdf (Accessed 07 November 2019).
15. European Technology Platform (ETP) SmartGrids Available at https://www.edsoforsmartgrids.eu/policy/eu-steering-initiatives/smart-grids-european-technology-platform/ (Accessed 07 November 2019).
16. Basel III Available at https://www.bis.org/bcbs/basel3.htm (Accessed 07 November 2019).
17. H. Cam and P. Mouallem, "Mission-Aware Time-Dependent Cyber Asset Criticality and Resilience," in Proceedings of the 8th CSIIRW Cyber Security and Information Intelligence Research Workshop, Oak Ridge National Lab, Oak Ridge, TN, 2013. DOI: 10.1145/2459976.2459989
18. H. H. Willis and K. Loa, "Measuring the Resilience of Energy Distribution Systems, RAND Justice, Infrastructure, and Environment, PR-1293-DOE," July 2014. [Online]. Available at: http://www.rand.org/content/dam/rand/pubs/research_reports/RR800/RR883/RAND_RR883.pdf. (Accessed 07 November 2019).
19. Hollnagel, E., Woods, D. D., & Leveson, N. C. (2006). Resilience engineering: Concepts and precepts. Aldershot: Ashgate. Available at: https://www.researchgate.net/publication/50232053_Resilience_Engineering_Concepts_and_Precepts (Accessed 07 November 2019).
20. Petrenko Sergei. Cyber Security Innovation for the Digital Economy: A Case Study of the Russian Federation, ISBN: 978-87-7022-022-4 (Hardback) and 978-87-7022-021-7 (Ebook) © 2018 River Publishers, River Publishers Series in Security and Digital Forensics, 1st ed. 2018, 490 p. 198 illus.
21. Petrenko, A.S., Petrenko S.A., Makoveichuk, K.A., Chetyrbok, P.V. The IIoT/IoT device control model based on narrow-band IoT (NB-IoT), 2018 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (EIConRus), 2018, pp. 950-953. DOI: 10.1109/EIConRus.2018.8317246
22. J. Park, T. P. Seager, P. S. Rao, M. Convertino and I. Linkov, "Integrating risk and resilience approaches to catastrophe management in engineering systems," Risk Analysis, vol. 33, no. 3, pp. 356-367, 2013. DOI: 10.1111/j.1539-6924.2012.01885.x
23. Petrenko, S.A., Stupin, D.D. (2018). National Early Warning System on Cyberattack: a scientific monograph [under the general editorship of SF Boev] "Publishing House" Athena ", University of Innopolis; Innopolis, Russia, p. 440. Available at: https://elibrary.ru/item.asp?id=36378643 (Accessed 08 November 2019, in Russian).
24. J. Zalewski, S. Drager, W. McKeever, A. J. Kornecki and B. Czejdo, "Modeling Resiliency and Its Essential Components for Cyberphysical Systems," in Position Papers of the Federated Conference on Computer Science and Information Systems (FedCSIS). 2015. DOI: 10.15439/2015F414
25. J. Allen and N. Davis, "Measuring Operational Resilience Using the CERT® Resilience Management Model, "September 2010. Available at: https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=9401. (Accessed 08 November 2019).
26. J. H. Kahan, "Resilience Redux: Buzzword or Basis for Homeland Security," Homeland Security Affairs Journal, vol. 11, no. 2, February 2015. Available at: https://www.researchgate.net/publication/292162477_Resilience_Redux_Buzzword_or_Basis_for_Homeland_Security (Accessed 08 November 2019).

27. J. King, "DTCC's Bodson Discusses Cyber Resilience at World Economic Forum," Depository Trust and Clearing Corporation, 3 February 2016. Available at: http://www.dtcc.com/news/2016/february/03/dtccs-bodson-discusses-cyber-resilience. (Accessed 08 November 2019).
28. J.-P. Watson, R. Guttromson, C. Silva-Monroy, R. Jeffers, K. Jones, J. Ellison, C. Rath, J. Gearhart, D. Jones, T. Corbet, C. Hanley and L. T. Walker, "Conceptual Framework for Developing Resilience Metrics for US Electricity, Oil, and Gas Sectors, SAND2014-18019," September 2015. Available at: http://energy.gov/sites/prod/files/2015/09/f26/EnergyResilienceReport_%28Final%29_SAND2015-18019.pdf. (Accessed 08 November 2019).
29. John R. Davis Jr. Major, (2015) Joined Warfare Center, "Continued Evolution of Hybrid Threats", Three Sword Magazine, 28/2015, Available at http://www.jwc.nato.int/images/stories/threeswords/CONTINUED_EVOLUTION_OF_HYBRID_THREATS.pdf (Accessed 08 November 2019).
30. Johnson, P. 2017. "With The Public Clouds Of Amazon, Microsoft, And Google, Big Data Is The Proverbial Big Deal." Forbes, Jun 15. Available at: https://www.forbes.com/sites/johnsonpierr/2017/06/15/with-the-public-clouds-of-amazon-microsoft-and-google-big-data-is-the-proverbial-big-deal/#2a37a76b2ac3 (Accessed 08 November 2019).
31. Kaplan, S., & Garrick, B. J. (1981). On the quantitative definition of risk. Risk Analysis, 1(1), 11–27. https://doi.org/10.1111/j.1539-6924.1981.tb01350.x
32. Kang, C. 2017. "Pittsburgh Welcomed Uber's Driverless Car Experiment. Not Anymore." New York Times. Technology, May 21. Available at: https://www.nytimes.com/2017/05/21/technology/pittsburgh-ubers-driverless-car-experiment.html?searchResultPosition=1 (Accessed 08 November 2019).