Improving the Courses of Educational Programs on Information Security Smart Grid*

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

[1] V.I. Vernadsky Crimean Federal University, Simferopol, Russia

christin2003@yandex.ru
alex.olifirov@gmail.com

[2] Innopolis University, Kazan, Russia

s.petrenko@rambler.ru

Abstract. Global trends directly or indirectly affect the directions of development of the electric power industry in Russia, including the power grid complex. Therefore, it is necessary not only to monitor these trends, but also to strive to respond to them in a timely manner. Smart Grids (SGs) represent a new concept in the development of electric power infrastructure in a digital economy. The widespread use of digital technology is a key factor in providing customers with intelligent electricity services. Existing courses, educational programs in such a situation do not always meet the requirements of the new concept and do not allow the formation of the necessary new competencies. This article provides recommendations for improving educational activities based on the risk analysis of the electricity company and compiling a competency map for an educational program for training personnel in the field of security risk management for SG, methodological approaches to teaching courses are discussed.

Keywords: certified courses; educational program; skills approach; professional competences; Information Security; intellectual power company.

1 Problem statement and its relationship with the most important scientific and practical objectives

Specialists who wish to improve their qualifications and professional level and study, within the framework of certified training courses, information security (IS) problems in the field of innovative electric power, should become owners of professional competencies and the ability to master working methods related to basic principles, conceptual approaches and information technologies used in multilevel information protection

* Copyright 2021 for this paper by its authors. Use permitted under Creative Commons License Attribution 4.0 International (CC BY 4.0).

CEUR-WS.org/Vol-2834/Paper29.pdf

in organizations. These competencies should correspond to the types of professional activities that the certified courses program is oriented to. At the same time, competencies should be consistent with the innovations of an enterprise operating based on the Smart Grid concept. That is, the graduate of the courses must be able and know what the employees of innovative enterprises in this industry know.

In this regard, the problem arises of determining the goals of improving the professional level of students, selecting the content of teaching materials of the educational process, assessing educational results and matching competencies with the modern level of activity of enterprises and organizations in the field of information security in the electric power industry based on the Smart Grid concept.

The aim of the article is to improve the courses of educational programs in information security based on ensuring the completeness and complexity of the competencies of graduates in the field of IS Smart Grid management.

2 Competent approach to training specialists in the field of information security management

First, the research is related to competences and competence-based approach. The concept of a "skills-based approach" (or "competency-based approach") has become widespread in connection with the solution of problems of improving the education of Russia, as well as the transition to the implementation of federal educational standards of higher education. Curriculum on a skills-based approach can be considered as a set of principles, goals of education, selection of the content of education, organization of the educational process and assessment of educational results. The professional competence of an individual can be considered as the goal and result of education.

In this regard, the implementation of the skills-based approach to training specialists in the field of information security management and the study of trends in this area will allow domestic information security specialists to increase their competitiveness in the international markets of information goods and services.

The international vector of development of education in the field of information security management, which is based on the following courses, is of particular interest:

- CISSP (Certified Information Systems Professional);
- CSSLP (Certified Secure Software Lifecycle Professional);
- CISM (Certified Information Security Manager);
- CISA (Certified Information Systems Auditor).

The training materials for these courses have been tested at Bauman Moscow State Technical University, at Financial University under the Government of the Russian Federation when conducting appropriate certification courses for information security specialists [4].

A graduate of the courses should have professional competences: to know the basic methods of information security management, be able to improve methods of information security, have the skills to assess the effectiveness of information security in

organizations. At the same time, the following seven main sections can be distinguished in certified courses [4, 5, 6, 9, 12]:

1. IS management;
2. secure access;
3. network security;
4. cryptographic information security;
5. development of safe programs;
6. modeling and conformity assessment;
7. business continuity and recovery.

In Smart Grid information systems, which are an innovative field, this knowledge and skills, together with their ability to adequately and successfully apply them, can be formed only directly when solving the corresponding problems in the framework of practical activities. They cannot be fully acquired in the course of obtaining education, since in educational institutions there are practically no tasks from the real practice of managing information security of modern companies, including Smart Grid. It should be noted that the threat and risk are determined not abstractly, but relatively specifically protected resources [4, p. 9]. However, this paradox is partially solved by the creation of pilot laboratories, the development of cases, the widespread use of simulation of the main and supporting and auxiliary business processes.

The focus of production of something new in the electric power industry is shifting in modern conditions to the creation of innovative smart grids. The introduction of the Smart Grid concept provides for the development of smart grid technology and means a fundamental reorganization of the electric energy services market [2, 10]. Federal Grid Company of Unified Energy System (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. PJSC FGC UES provides half of the total energy consumption in Russia at the expense of electricity transmitted through its networks. This company controls 142 thousand km of high-voltage transmission lines and 944 substations with a total capacity of over 345 gigawatts [13].

Electricity company in terms of risk indicators assessment:

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

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

The company uses three methods of risk response: risk avoidance; risk acceptance; reduction or transfer of risk (Fig. 1). The choice of a method for responding to risks depends on the significance of the risks.

A network operating on the basis of the Smart Grid concept is able to detect the damaged area itself, de-energize it and automatically power consumers who are briefly left without power. Controllers with freely programmable logic implement algorithms for configuring power supply schemes for various emergencies and provide network automation.

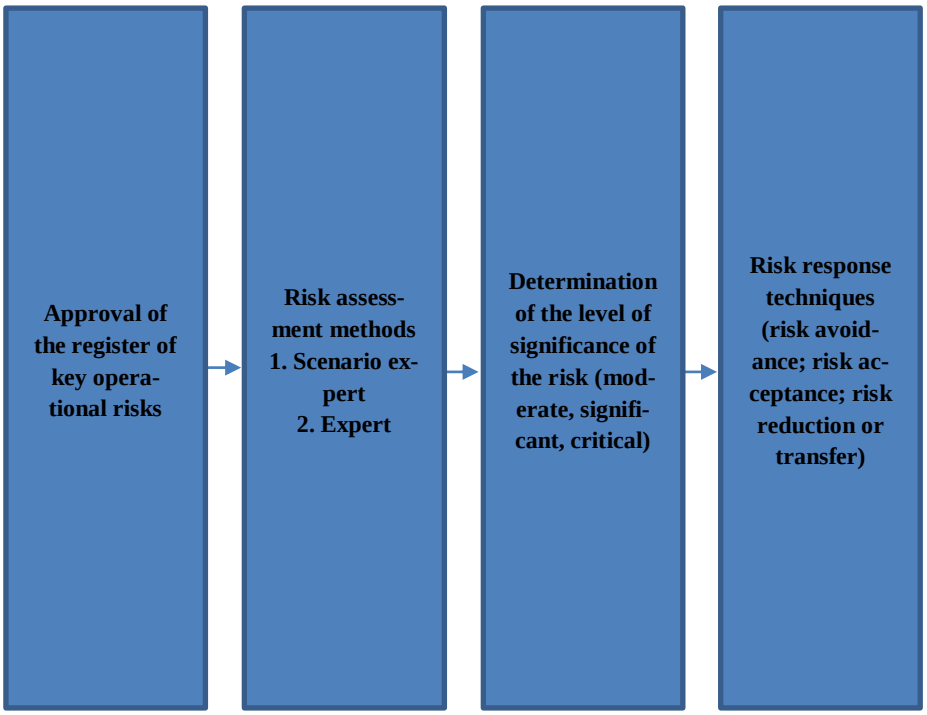

Fig. 1. Risk Assessment and Management Scheme for an Electricity Company

Energy companies are characterized by both general risks and specific ones inherent in one or another type of activity, depending on the scope of their operation. Risks in the information systems of network companies can be identified and increased at any point in the life cycle of these systems, from the decision to create a system (purchase, development of hardware and technical means) and ending with the implementation of the system.

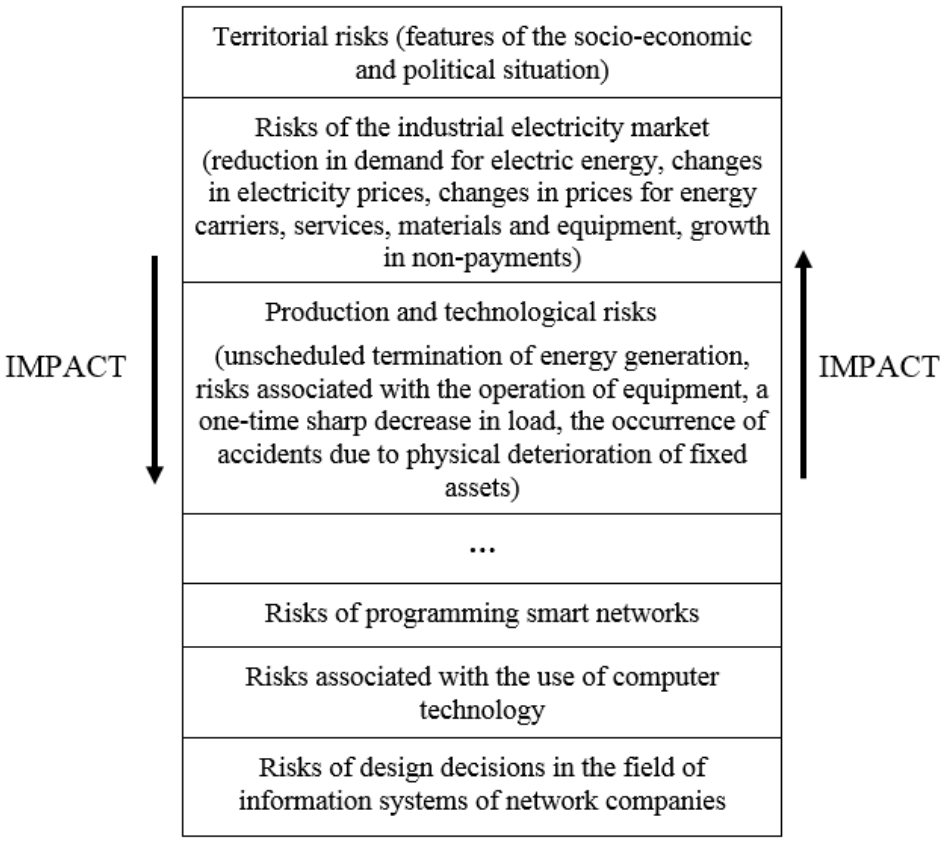

Fig. 2. The scheme of the relationship of risks of enterprises of the electric power industry

Nonetheless, 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]. To effectively use information systems, an entrepreneur must understand the socio-economic risks and limitations of technology development, implementation and use of systems (Fig. 2).

Information systems are created to prevent a company's business risk. This risk can be in the form of an increase in the cost of services provided, a decrease in income. Business information systems should reduce risks by increasing the effectiveness of managers' actions, based on mathematical models of risk optimization and cyber risk management methods at various levels: enterprise, regional, federal [8, 10, 11].

3 Map of competencies of specialists in the field of information security of an intellectual network

The shortage of specialists in the field of information security, who in the digital economy are ready to solve the key tasks of the coming decade, is focused on innovative products and the creation of new markets and the globalization of companies. Systems for training specialists for information security management should begin to train specialists with knowledge and competencies in several subject areas who can work with both internal and external risks, both operational and IT risks (cyber risks) and are able to anticipate future transformations. Changes in the set and nature of competencies are one of the key aspects of the change in the qualification structure of the operational risk management system of an electric utility company and its information security service.

It is possible to identify the relationship between the level of human capital and information security of a high-tech innovative company, which can be expressed in the number of patents obtained, the creation of new competencies, the introduction of new information security practices, etc.

The main subject of the study is the need to analyze exactly what competencies and qualifications are needed to ensure the information security of companies and how this will affect the training system for its personnel. For the world's leading electricity companies, innovation is an important source of income. Estimates show that the transition to an innovative development option based on smart energy will be accompanied by a significant decrease in the commissioning of new power plants and related network facilities for generating capacity. As a result, the reduction in investment is the most significant systemic economic effect. The second largest effect is the reduction in the fuel costs of power plants. New technologies bring energy companies not only new opportunities but also create new threats and risks. Therefore, the introduction of a new system of smart metering devices (Smart Meters), allowing remote transmission of energy consumption data of a client, has opened up many new ways of theft of electricity [7]. In addition to the previously known forms of theft based on various mechanical influences on the meter, smart meter vulnerabilities allow an attacker to compromise real energy consumption data at the software level. Thus, the effect of the introduction of innovation also brings additional annual economic losses to energy companies from theft.

The competency clusters and processes are identified on the basis of the analysis of the interaction scheme of the power company divisions in the operational risk management system and their IS risks (cyber risks), based on expert estimates and taking into account the competence clusters used in the practice of leading companies from the standpoint of information security of the smart energy network [1].

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

1. a specialized subdivision of the organization that carries out operational risk management procedures - the operational risk management service (ORMS);
2. a specialized unit of the organization that performs information security risk management procedures (IS service);

3. subdivisions-owners of the organization's business processes and subdivisions that support the organization's business processes (hereinafter referred to as competence centers), use information technologies and carry out risk identification, collection of information and informing about the identified risk, assessment of identified risks inherent in the processes of competence centers (within their competence), development and implementation of measures aimed at reducing the negative impact of operational and information security risks, as well as monitoring the level of operational risk and information security risk in their processes;
4. classifiers used in the operational risk and information security management system;
5. an event database containing information on operational risk and IS risk events 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 scope and functionality of which is determined by the nature and scale of the operations and processes of the electric power company.

In Figure 3, which reflects the interaction of company departments in the context of the integration of information security risks, the following conventions are adopted:

1 - the information security service (ISS) 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, makes 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 - business units respond to an 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 determines, together with business units and the operational risk management system, 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 ISS;

6 - the information security system determines the effectiveness of measures to ensure an immediate response to an incident (IS risk event);

7 - ORMS, structural divisions, and the information security service organize activities 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.

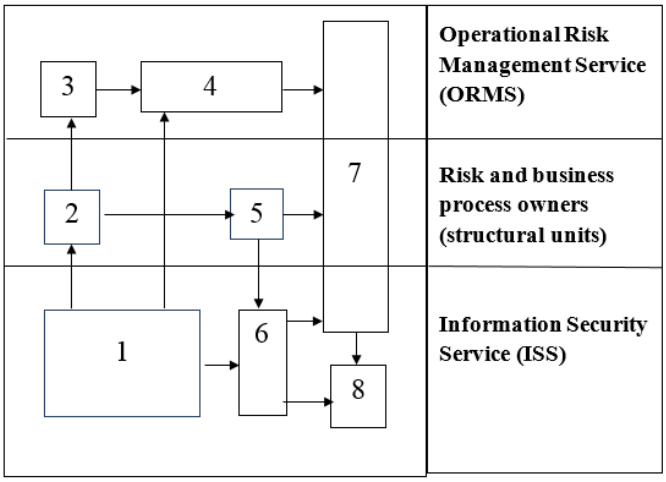

Fig. 3. Information security risk management scheme as part of operational risks

Taking into account the considered scheme and the competency approach proposed in [1], we present a map of the competencies of specialists in the field of information security of an intellectual network.

A. Leadership, organizational and managerial competencies of an information security officer.

A.1. It owns modern models of organization of the company and can independently organize the process of ensuring information security.

A.2. It can act as a qualified customer of research and development.

B. Employee competencies in terms of communication and coordination in the external ecosystem.

B.1. It can maintain effective communication with experts to identify promising areas of development.

C. Technological and special professional and sectoral competencies of employees in the field of intelligent power grids.

C.1. It can determine long-term directions for development (electric power technologies).

C.2. Understands the directions of the development of the professional field can determine new tasks in his field and evaluate the means of solving them.

C.3. It can solve new problems in the professional (technological) field.

C.4. It can solve complex problems in the professional (technological) field.

C.5. It can provide standardization of new technologies and solutions.

C.6. It can solve standard tasks in the professional (technological) field.

C.7. It can learn ways to solve standard problems in the professional field.

D. Cognitive competencies of an employee.

D.1. It can evaluate the achieved level of knowledge, formulate the need for new knowledge in the field of information security, evaluate the methods of their receipt and the results obtained.

D.2. It can determine and develop ways to obtain new knowledge in the field of information security, evaluate the results.

D.3. It can create new knowledge on the subject of activity (including technical and regulatory knowledge).

D.4. Able to independently master new knowledge (including technical and regulatory knowledge).

E. Employee competencies.

E.1. Search and discovery of new business opportunities (identifying business opportunities).

E.2. Search and discovery of new risks: operational, information (cyber risks).

E.3. Assessing the prospects of new business opportunities (evaluating business opportunities).

E.4. Assessment of new operational, informational risks (evaluating of cyber risks).

E.5. Decision making, responsibility for the consequences of decisions (decision-making).

E.6. Identifying and solving problems.

E.7. The ability to think in a new way (innovative thinking).

E.8. Effectiveness of communication with different partners (communication).

F. Vision of the future, long-term forecasting, and determination of long-term strategic goals by an employee.

F.1. It can determine the direction of development of the sphere of consumption of company products and services, as well as infrastructures for 15–20 years and set long-term goals.

F.2. It can determine the direction of technology development in the field of the company for 15-20 years and set long-term goals.

This map shows what competencies are necessary for the implementation of the processes of an electric power innovation company. At the same time, the distribution of managerial, technological and entrepreneurial competencies is uneven. However, most processes require complex organizational and entrepreneurial competencies in conjunction with a high level of technological and cognitive competencies. This map also shows the place and importance of the company's technological competencies to ensure information security. Therefore, shareholders must approve that part of the money that the company earned from innovations will be spent on the introduction of new information security services.

The processes of changing the composition of the required competencies and qualification structure for managing and ensuring innovative activities in the context of digitalization and information security acquire a special role at the stage of transformation of electric companies.

Conclusion

The considered approach to the formation of competencies allows you to:

– ensure the completeness and comprehensiveness of the composition of competencies, since this composition of competencies, will be associated with the regulation

of information processes and business processes of the company and fully comply with its description;

- represent competencies in educational programs in the form of a tree with a hierarchical multi-level structure and in the chronological sequence of their implementation, according to the chronology of the implementation of relevant processes to ensure information security;
- to supplement, based on the study of new business processes of successful enterprises, a set of competencies of graduates taking into account the focus of the educational program on new specific areas of knowledge and activities.

References

1. Afanasyev G. E. Karta kompetentsiy i perspektivnykh professiy R&D [Map of competencies and promising professions R&D]. Federalnyy spravochnik. Obrazovaniye v Rossii [Federal directory. Education in Russia], 2011, Volume 8. Available at: URL: http://federal-book.ru/files/FSO/soderganie/Tom%208/V/Karta.pdf (Accessed October 11, 2019). (In Russ.)
2. Kobets B. B., Volkova I. O. Innovatsionnoye razvitiye elektroenergetiki na baze kontseptsii Smart Grid [Innovative development of the electric power industry based on the Smart Grid concept]. – M.: IAC Energiya, 2010. — 208 p. (In Russ.)
3. Kartvelishvili V. M., Sviridova O. A. Risk-menedzhment. Metody otsenki riska: uchebnoye posobiye [Risk management. Risk Assessment Techniques: A Study Guide]. – Moskva: FGBOU VO «REU im. G. V. Plekhanova», 2017. – 120 p. (In Russ.)
4. Barabanov A. V.. Dorofeyev A. V.. Markov A. S.. Tsirlov V. L. Sem bezopasnykh informatsionnykh tekhnologiy [Seven secure information technologies]. Pod red. A. S. Markova [Ed. A.S. Markov.]. – Moskva: DMK, 2017. - 221 p. (In Russ.)
5. Conrad E., Misenar S., Feldman J. CISSP Study Guide. 3rd edition. - Boston: Syngress, 2015. 622 p. DOI: 10.1016/C2009-0-61065-5
6. David L. Cannon CISA Certified Information Systems Auditor Study Guide, 4th Edition. 2016. DOI: 10.1002/9781119419211
7. Ghansah I. Smart grid cyber security potential threats, vulnerabilities and risks // Public Interest Energy Research, Prepared for: California Energy Commission, 2012. DOI: 10.1016/j.jesit.2018.01.001
8. 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
9. Paul M. Official (ISC) 2 Guide to the CSSLP CBK 2nd Edition - 2013, 800 p. DOI: 10.1201/b15377
10. Petrenko, S.A., Makoveichuk, K.A. Ontology of cyber security 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. Available at: URL: http://ceur-ws.org/Vol-2081/paper21.pdf (Accessed October 11, 2019).

11. Petrenko, S.A., Makoveichuk, K.A., Chetyrbok, P.V., Petrenko, A.S. About readiness for digital economy / 2017 Proceedings of 2017 IEEE 2nd International Conference on Control in Technical Systems, CTS 2017, p. 96-99. DOI: 10.1109/CTSYS.2017.8109498
12. The Official (ISC)2 Guide to the CCSPSM CBK®, Second Edition.- 2016. DOI:10.1002/9781119419198
13. Integrirovannyy godovoy otchet Publichnogo aktsionernogo obshchestva «Federalnaya setevaya kompaniya Edinoy energeticheskoy sistemy» za 2018 god [Integrated annual report of the Public Joint Stock Company "Federal Grid Company of the Unified Energy System" for 2018]. Available at: URL: https://report2018.fsk-ees.ru/?/ru/59-information-on-the-report (Accessed October 11, 2019). (In Russ.)