FRONTLINE MARKETING MANAGEMENT AND ECONOMICS JOURNAL
(ISSN – 2752-700X)
VOLUME 03 ISSUE 11 Pages: 1-9
SJIF IMPACT FACTOR (2021: 5.277) (2022: 5.694) (2023: 6.834)
OCLC – 1276793382
Publisher: Frontline Journals

Journal Website: https://frontlinejournals.org/journals/index.php/fmmej

Research Article

INFORMATION SECURITY MECHANISMS OF ORGANIZATIONAL AND ECONOMIC ACTIVITY OF ENERGY INDUSTRY ENTERPRISES OF WORLD COUNTRIES

Submission Date: November 01, 2023, **Accepted Date:** November 05, 2023,
Published Date: November 09, 2023
Crossref doi: https://doi.org/10.37547/marketing-fmmej-03-11-01

Koraboev Eldor Alijonovich
Head of "Spirituality and Enlightenment" department at Tashkent University of Information Technologies, Uzbekistan

ABSTRACT

In this paper, the necessary measures for cyber security in the organizational and economic activities of energy industry enterprises are described. Moreover, the economic aspects of their implementation plan and mechanisms are analyzed, as well as the introduction of a model into the national economic cyber protection infrastructure is recommended.

KEYWORDS

Information security of energy industry, cyber economy, cyber hygiene in the digital economy, activation of organizational and economic mechanisms.

INTRODUCTION

The desire of the world countries to use "smart technologies" in the era of Industry 4.0 is more confident about the expected profit, rather than the prediction, taking into account the high risks in relation to information security. As the participation of information technology as a

FRONTLINE MARKETING MANAGEMENT AND ECONOMICS JOURNAL
(ISSN – 2752-700X)
VOLUME 03 ISSUE 11 Pages: 1-9
SJIF IMPACT FACTOR (2021: 5.277) (2022: 5.694) (2023: 6.834)
OCLC – 1276793382
Publisher: Frontline Journals

means of the basic conditions of human existence has grown to the level of "economic boon", the indicator of its illegal ownership, i.e. control through cyber activities, is increasing year by year. The fact that developed enterprises prioritize the use of innovation, investment, and intellectual technological activities as the priority tasks of the values of sustainability makes it possible for their protection to be weak. This situation increases the need for further improvement of information security and its participation in the organizational and economic mechanisms of every enterprise.

The application of business models and digital technologies to production and service activities will further increase the demand for energy consumption. However, the operation of energy and energy systems consisting of various components in harmony with integrated "smart technologies" will implement large-scale information exchange, which in turn will increase the level of information security risk.

In the case mentioned above, in 2023, a strategy and program project was developed by the European Socio-Economic Committee of the UN for the purpose of "Ensuring integrated cyber resilience in smart energy systems", and these documents are aimed at digitalization of the energy industry. Intellectual technologies automatically implement the plan to ensure the sustainability of energy products based on various components with the help of digital technologies of energy enterprises. Roadmaps, economic resources, innovative approaches, and proposals for conducting such activities are all in the master intellectual control system, so the information available on it is worth a lot of money on the black market. It is observed that smart technologies are coordinated in the digital system of electricity market participants, consumers, energy system operators, and all generating enterprises.

An information security attack on energy industry enterprises is based on taking control of systems or data ownership by damaging physical machines and equipment. Moreover, one of the main reasons for a cyber attack is the artificial lowering of service prices by damaging the company's reputation in the consumer market. Every additional piece of digital technology in an enterprise serves to increase the risk of a tool being used as a cyber attack tool. However, increasing production efficiency and creating additional value without innovative technologies

FRONTLINE MARKETING MANAGEMENT AND ECONOMICS JOURNAL
(ISSN – 2752-700X)
VOLUME 03 ISSUE 11 Pages: 1-9
SJIF IMPACT FACTOR (2021: 5.277) (2022: 5.694) (2023: 6.834)
OCLC – 1276793382
Publisher: Frontline Journals

is considered ineffective. The main risks of these relative differences are the components of the energy system, i.e., digital and intellectual technologies such as transportation, energy distribution and transmission networks, energy concentration centers, energy consumption flows, and participating in the processes that generate it. The number of financial extortion attacks on energy companies increased by 35% in reported cases worldwide, while malware and software wipers increased by 53% .

In recent years, cyber security has been seen as a risk category in economic terms. Describing and defining the ways of risk management in reflecting its economic content is widely used in the cyber-economic audit system. In particular, cyber-attack mitigation - risk mitigation, cyber-attack denial - risk denial, cyber-attack acceptance - risk acceptance, as well as cyber-attack mitigation and risk mitigation, etc. In 2020, the US National Institute of Technology and Standards (NIST) managed to identify the risks of financial loss of the use of intelligent technological components in the generation of manufacturing processes of digital and intelligent technologies after the US scientist Marco Yanceti proved that the experience of following the task of ensuring the utmost secrecy of the design process in the case of mitigating a cyber-attack on energy industry enterprises is effective. In this, a 2-stage analysis of intellectual technology tools causing financial losses and the reasons for their easy defeat of cyber-attacks was performed (Table 1.3).

Table 1.3

Technical and economic losses of a cyber-attack on energy industry enterprises, 2022

Generation process	Financial loss (USD)	Transmission process	Financial loss (USD)	Distribution process, distribution, and consumption of energy resources	Financial loss (USD)
Machine control equipment	24 billion	Optical transformers	5 billion	Improved infrastructure of smart meter accounting	18 billion
Technological management systems	33 billion	Protective equipment	2 billion	Automation tools, feeders	4 billion

FRONTLINE MARKETING MANAGEMENT AND ECONOMICS JOURNAL
(ISSN – 2752-700X)
VOLUME 03 ISSUE 11 Pages: 1-9
SJIF IMPACT FACTOR (2021: 5.277) (2022: 5.694) (2023: 6.834)
OCLC – 1276793382
Publisher: Frontline Journals

Registration equipment	17 billion	Phase measuring equipment	7 billion	Individual mobility tools	44 billion
System connection interfaces	12 billion	Technical service systems	3 billion	Accumulators, solar panels, charging of electric cars, smart centers, microgrids	4 billion
		Means of automation of station subsystems	5 billion		

When analyzing the above table, the information flows of the information security caused a big loss through the management of the electric energy carried out through individual mobility tools, i.e. personal computers, mobile communication tools, tablets, and similar technologies. This is based on the fact that the personal data of each individual is very open and very common. Technological control systems are the next most financially affected, mainly due to the fact that the users of the related technologies have algorithms at a level that can eliminate the need for a dedicated engineer. Since the control equipment of the workshop is the main control system, this equipment is the target for all hackers. While its encounter with a cyber-attack is a natural and expected process, no enterprise can be indifferent to a major financial loss. Accordingly, revision of the organizational-economic mechanism for cyber-economic protection of energy industry enterprises and taking into account the elements of the mechanism was proposed by the US National Institute of Technology and Standardization (Figure 1.4).

According to Figure 1.4, the activation of the engineering mechanism should be inextricably linked with organizational issues. The execution of each cyber attack can be checked against the results, which leads to a comparison with the economic results. Accordingly, it is important to introduce organizational and economic information security mechanisms in enterprises. To date, all organizational-economic mechanisms have the possibility to arrange the confidentiality of information and their electronic flows that do not expose each other through digital document exchange, such as electronic documentation, through organizational-economic mechanisms.

FRONTLINE MARKETING MANAGEMENT AND ECONOMICS JOURNAL
(ISSN – 2752-700X)
VOLUME 03 ISSUE 11 Pages: 1-9
SJIF IMPACT FACTOR (2021: 5.277) (2022: 5.694) (2023: 6.834)
OCLC – 1276793382
Publisher: Frontline Journals

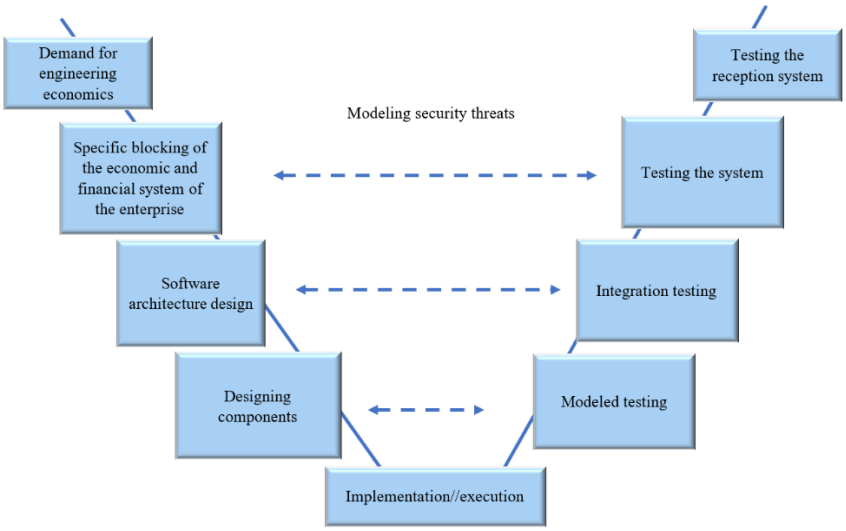

Figure 1.4. A mechanism for using engineering analysis

The mechanism of using the engineering analysis of the energy industry enterprises is considered to have a high risk of penetration through the electronic system of accounting and economic relations because its management is related to the human factor and the connection of the technology used by the human factor (phone, computer, tablet) to the Internet. Cyber resistance of individual technological tools will not be high, because the data flow of social networks is very high and its base is repeated many times. This stifles the free activity of the human factor and causes economic losses as a social and technical problem. In order to apply effective measures against cyber-attacks of integrated intelligent technological energy systems during the production activities of energy industry enterprises, the UN recommended the introduction of the organizational-economic mechanism based on the instructions of the US MTSI (Figure 1.5).

FRONTLINE MARKETING MANAGEMENT AND ECONOMICS JOURNAL (ISSN – 2752-700X)
VOLUME 03 ISSUE 11 Pages: 1-9
SJIF IMPACT FACTOR (2021: 5.277) (2022: 5.694) (2023: 6.834)
OCLC – 1276793382
Publisher: Frontline Journals

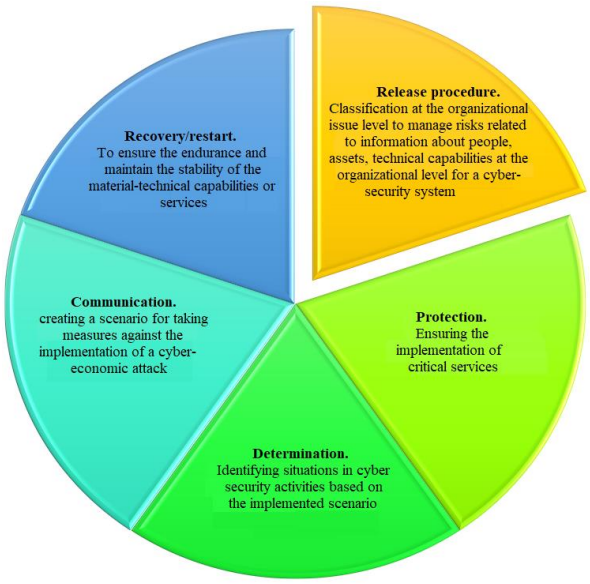

Figure 1.5. US MTSI frame mechanism

According to it, it was promoted as a framework mechanism from the cyber security program of the organizational-economic mechanism. Its interpretation as a framework is determined by the level of development of the energy system of the country's energy infrastructure.

Since the intelligent integrated energy system is considered a critical part of the infrastructure, the effectiveness of framework mechanisms is considered high as a result of the occurrence of cybereconomic attacks.

FRONTLINE MARKETING MANAGEMENT AND ECONOMICS JOURNAL
(ISSN – 2752-700X)
VOLUME 03 ISSUE 11 Pages: 1-9
SJIF IMPACT FACTOR (2021: 5.277) (2022: 5.694) (2023: 6.834)
OCLC – 1276793382
Publisher: Frontline Journals

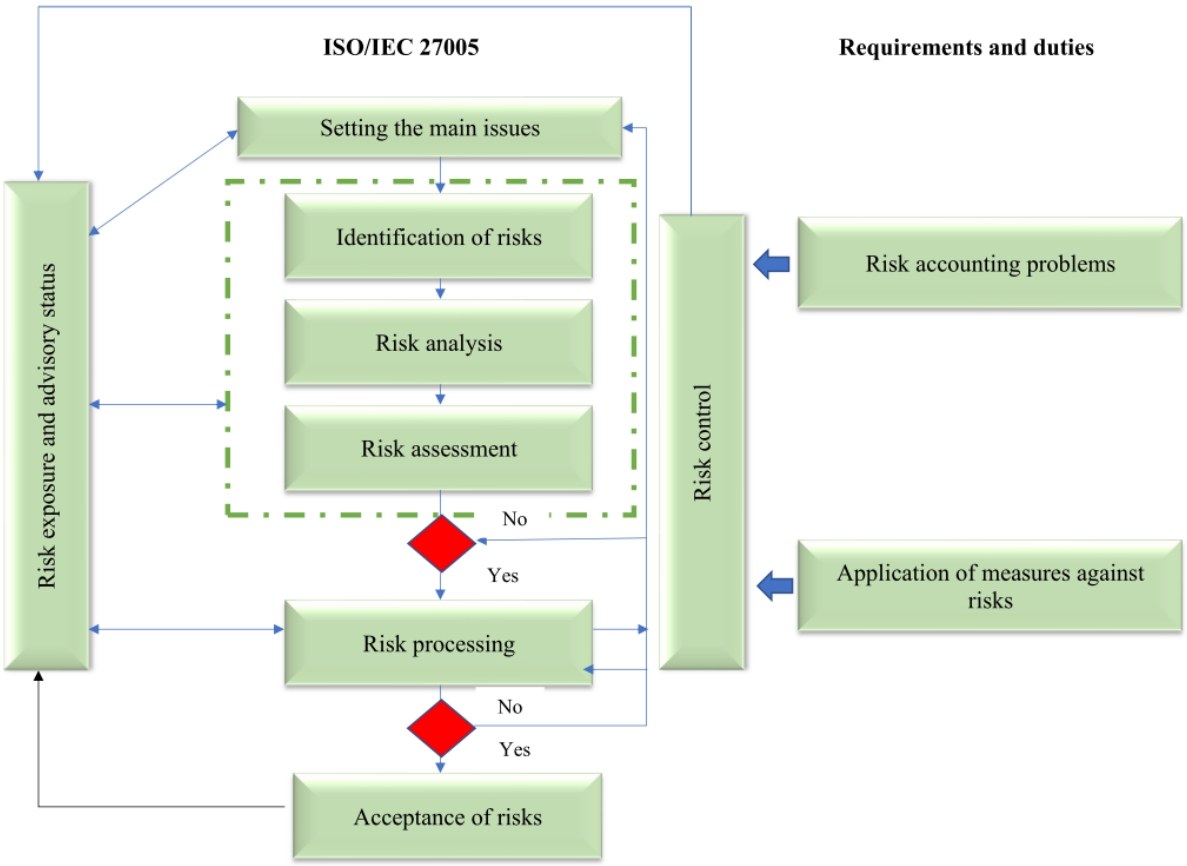

Figure 1.6. Algorithmic methodology of risk management process in cyber security

The methodology recommended above is intended for the risk management process according to the international standard ISO/IEC 27005:2018, using the tasks required in the provision of cyber security. According to it, it is recommended to draw up a strategic plan of measures to mitigate the risks expected due to the use of advanced intellectual technologies in the relevant field and sector and to design it as a socio-economic insurance task.

The basic block-building technique is filled with software traps, fraudulent account numbers and account instructions, and similar information to protect it by distinguishing factors related to economic security. To do this, it includes copying the general state of the system, organizing a regular cycle of the algorithm of the most popular products or services in the commercial system by dividing the products and services into categories, creating a risk matrix and its

FRONTLINE MARKETING MANAGEMENT AND ECONOMICS JOURNAL
(ISSN – 2752-700X)
VOLUME 03 ISSUE 11 Pages: 1-9
SJIF IMPACT FACTOR (2021: 5.277) (2022: 5.694) (2023: 6.834)
OCLC – 1276793382
Publisher: Frontline Journals

consequences, mechanizing the target protection system by dividing it into levels.

During the development of Industry 4.0 in line with digital technologies, the socio-economic development of the country, the fact that attention to its economic security is increasingly becoming a central point of focus is mainly determined by the possibilities of modern and advanced information technologies and the scope of their collective use. Accordingly, the ability to distinguish cyber-economic threats, to anticipate them, to organize the careful formulation of countermeasures according to their characteristics, is considered the main and important element of the integrity of the economic infrastructure. The measures proposed above are aimed at improving the cyber-economic protection of the country, increasing cooperation and mobility of state bodies, entrepreneurs, and its population in the information sphere, and serving to prevent the flow of information to a high degree. Organizational-economic mechanisms of activation of strategic measures of economic importance should include objective evaluation of the environment's internal and external information flow, prevention of multi-level struggle against them, and expansion of the scope of direct influence. It is very important for the national energy infrastructure to eliminate the chaotic nature of cyber-economic attacks by using the shortcomings of digital technologies and to develop an organizational-economic mechanism that serves to reduce and mitigate the consequences of the impact of information. After all, it is not a difficult task in the environment of cyber development to find a way to collect all the necessary information of consumers even through a single payment card. Therefore, according to foreign experience, in order to protect the cyber-economic system of energy system enterprises, it is necessary to transform the management digital system systems into the latest world-standard technologies, and then the need to adapt the organizational structure to this situation and maintain the continuity of participation in production while ensuring its proportionality increases.

REFERENCES

1. Recommendations to the European Commission for the Implementation of Sector-Specific Rules for Cybersecurity Aspects of Cross-Border Electricity Flows,

FRONTLINE MARKETING MANAGEMENT AND ECONOMICS JOURNAL (ISSN – 2752-700X)
VOLUME 03 ISSUE 11 Pages: 1-9
SJIF IMPACT FACTOR (2021: 5.277) (2022: 5.694) (2023: 6.834)
OCLC – 1276793382
Publisher: Frontline Journals

on Common Minimum Requirements, Planning, Monitoring, Reporting and Crisis Management., Smart Grid Task Force Expert Group 2. Final Report, 2019- 107

2. ECE/ENERGY/GE.6/2023/3 Европейская экономическая комиссия. Комитет по устойчивой энергетике Группа экспертов по системам экологически чистого производства электроэнергии Группа экспертов по

3. ECE/ENERGY/GE.6/2023/3 Economic Commission for Europe. Committee on Sustainable Energy Expert Group on Clean Electricity Generation Systems Expert Group on Energy Efficiency Nineteenth Session. Geneva, October 3–4, 2023. Item 7 of the provisional agenda. Reliability and cyber resilience of smart integrated energy systems, https://unece.org/sites/default/files/2023-08/ECE_ENERGY_GE.6_2023_3_ECE_ENERGY_GE.5_2023_3_RU.pdf

4. Woody, C., and Creel, R., 2021: Six Key Cybersecurity Engineering Activities for Building a Cybersecurity Strategy. Carnegie Mellon University, Software Engineering Institute's Insights (blog), Accessed October 17, 2023, https://insights.sei.cmu.edu/blog/six-key-cybersecurity-engineering-activities-for-building-a-cybersecurity-strategy/.

5. Fortinet, Global Threat Landscape Report. A Semiannual Report by FortiGuard Labs (February 2023).