# THE ECONOMICS OF CYBER SECURITY IN THE ENERGY INDUSTRY AND ITS ASSESSMENT METHODS

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

***ABSTRACT***

*In this paper, relevant methods, mechanisms and models for assessing the cyber security economy of energy industry enterprises are presented. Moreover, the author's approach is also presented.*

***Keywords:*** *economics of cyber security, cyber hygiene, economic foundations of cyber attack measures.*

Since the energy industry is a powerful sector, it is important to have a strong information security infrastructure in every country. To date, the use of traditional technologies is not observed in almost all countries of the world, the improvement of digital technologies is driven by the fact that humanity opens the way to technological management in many social and economic factors. Increasingly developing digitalization is escalating the involvement of "intelligent technologies" that cause enterprises in the energy system to acquire the status of "smart". This is interpreted as an innovative energy service activity in the world economic language.

Although intelligent technologies bring lightness and excellence to the core of the industry, its applied intellectual technologies have a different nature to cyber-attacks, which can create unprecedented risks of its own. The main target of a cyberattack on energy industry enterprises is not financial sources, but rather information about the continuous provision of finance. Accordingly, the main data that should be included in the cyber hygiene of energy industry enterprises are energy supply and confidential data of consumers.

The economics of cyber security in the energy industry are measured by the cascading effect, which is caused by the failure of chains in the power supply system. Although the economics of cyber security of energy industry enterprises has not been distinguished as a science, due to its popularity in 2020, attention was paid to this approach at the initiative of energy industry enterprises.

In 2015, the European Network Information Security Expertise Center created a sub-structure of the micro- and macroeconomic foundations of cyber security.

According to it, the macroeconomic foundations of cyber security of energy industry enterprises are based on the fact that new innovative technologies create conditions for the rapid development of new markets in the information technology market. Since information technologies often have the same programming language, if the amount spent on ensuring their cyber security in 2015 was 20.1 billion euros, the damage that could be caused due to its lack of provision was estimated at 640 billion euros.

Most of today's energy industry enterprises have developed the skills to conduct production process management activities based on automated systems, and as a result of the increased demand for the application of cyber measures, the level of employment of cyber security engineers in the energy industry is increasing. Energy industry enterprises have a higher percentage of cyber security than other industries, and it is appropriate to research the factors affecting it.

Table 1.1

Reasons why energy industry enterprises face a cyber attack1

| № | Reasons for a cyber attack | Share in cyber attack | Cyber attack targets and consequences |
|---|---|---|---|
| 1. | Access to information through payment slips | 22% | The confidentiality of the financial details of the electricity payer will be lost |
| 2. | Withdrawing money from payment cards | 19% | Permanent formation of funds against power outages on payment cards |
| 3. | Complete deletion or "randomization" of the data of the dispatching service of electric energy supply | 18% | The formation of an artificial black payment market for the debts of the main payers |
| 4. | Stealing a house with a planned address | 16% | Block all means of communication, leaving the apartment without lights, and remove the item in question |
| 5. | The case is considered as a "clown hacker", that is, a hacker who practices, mocks, and has immoral reasons | 10% | Forming a business card among his colleagues in terms of hacking activities |

1 https://www.ifap.ru/pr/2008/080908aa.pdf

This table is the information presented in the foundation of the “Global Program of Cybersecurity” of the “International Telecommunication Union” organization, which is formed based on the statistics of 125 countries out of 210. Oscar Arias Sánchez, President of the Republic of Costa Rica with a scientific degree, said, “The world must be in continuous motion. It has to come together. No country can find a complete solution to this problem. Bourdieu explained the economic importance of cyber security under the comment, “if work is carried out on the basis of international principles, allowing the activities of hackers of international importance will achieve strategic coordination of countries at the global and regional level1”.

The main principles of the economy of cyber security of energy industry enterprises were developed in 2016 by the US information technology economist Steve Grobman, and the principles of the “Global Cyber Security Program” were formed through its charter2. According to it, these principles include:

1. Ensuring the availability of legal measures and experts in their management.
2. Ensuring constant readiness of technical measures and processes.
3. Formation of organizational structure and mechanisms.
4. Increasing the cyber hygiene capacity.
5. Establishing cyber cooperation.

The main essence of the principle formed in connection with legal measures and their management is to capture the cyber-capables and keep the programmers in their environment under constant control. Its economic approach is characterized by ensuring economic security.

Ensuring the constant readiness of technical measures and processes is organized through a strict risk assessment of each cyber activity and the economic losses that may occur as a result.

The formation of organizational structures and mechanisms is considered related to ensuring that hierarchical management has a strong position in relation to information confidentiality. Sometimes a single employee’s link is enough to carry out a cyber attack.

The increase of cyber hygiene potential means that the employees of the enterprise carry out their work while ensuring the confidentiality of the use of each computer and information technology tools.

1 ITU Global Cybersecurity Agenda (GCA). A framework for international cooperation in the field of cybersecurity.

2 Steve Grobman. The Second Economy: The Race for Trust, Treasure and Time in the Cybersecurity War. Apress. 2016 y, 374 p

Establishing cyber cooperation is important because it provides an opportunity to obtain repetitions of cyber attacks between countries, to formulate a cyber strategy, and to ensure a higher level of success of alternative choices.

In the transition to a digital economy, the demand for cyber engineering activities in all countries is keeping pace. The economic cybersecurity engineering strategy was developed by Carnegie Mellon University's Carnegie Mellon University engineering economists Carol Woody and Rita Krellar.

The Economic Cybersecurity Engineering Strategy was developed by Carol Woody and Rita Krellar, engineering economists at Carnegie Mellon University in the United States. It is noted that its mechanism is provided by following six important directions (Fig. 1.1).

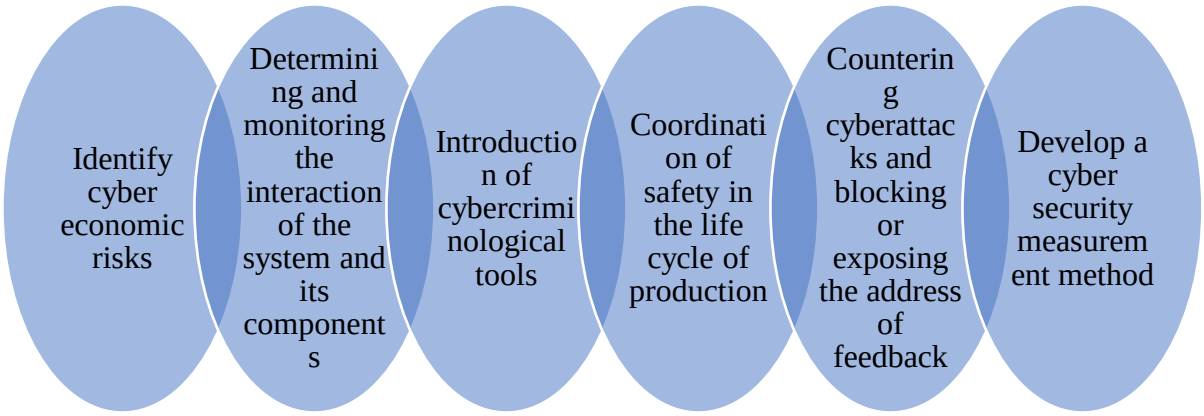


Figure 1.1. Directions for providing economic cyber security1

In identifying the risks of economic cyber threats, the economic cyber security engineering system includes the elimination of threats and strategic mission risks through information technology tools. Cyber risk perceptions drive strategic assurance decisions, and lack of cybersecurity expertise in risk analysis can lead to mistakes by making the wrong choice of assurance.

The analysis of system and component interaction allows to assess the status of components and external influence intersystem monitoring of economic cyber security engineering technologies, to determine its advantages and disadvantages. With confidence, the improvement of the defense system of the strategic mission will be carried out.

1 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 16, 2023, https://insights.sei.cmu.edu/blog/six-key-cybersecurity-engineering-activities-for-building-a-cybersecurity-strategy/

It is not enough to express the introduction of cybercriminological tools through a single comment, but the systematization of all its aspects will fulfill the tasks envisaged in the research:

Cyber threats are required to be distributed among the components through the influence of each interrelated tool.

The assessment system needs to be very transparent. This transparency can only cover a group of cybersecurity and economists.

Since the interdependence of the means is not statically calculated, the protection of trust requires that the digitization be carried out by an individual.

Coordination of security in the life cycle of production requires careful information technology management at each production stage, aimed at ensuring that blocks in their software architecture are not tied to economic blocks. While this includes digital economic systems, it is characterized by the fact that the digitalization of the activities of economic blocs is carried out privately and separately.

Counter-response to cyber-attacks and redirection blocking or exposure needs to be mechanized based on attacker profile maximization and scenarios such as threat modeling, attack tree analysis, development of potential misuse cases.

The development of a cyber security measurement method describes the assessment of the relative priority of cyber attack and cyber hygiene. In this regard, companies keep their valuation methods and models more confidential. Accordingly, research work requires the development of an evaluation method for an economic cyber security strategy.

Nasdaq's (Company) Economic Cybersecurity Index is designed to monitor the economic performance of a company and has a reputation as a unique cyberattack defender in the technology and innovation market, although it is not considered an information technology software company. Its evaluation method is distinguished by its summary of liquidity as a modified index:

$$S_i = \frac{(F_i + E_{i)*} P_{Fi}}{D_i} (1.1)1$$

Where:

$S_i$- economic cyber security index;

$F_i$- a measure of the relative value of a company's outstanding shares;

$E_i$- number of securities holders;

$P_{Fi}$- average value of securities;

$D_i$- the average value of the last traded prices of securities and shares.

1 Nasdaq CTA Cybersecurity IndexSM Methodology. 2015 y https://www.betashares.com.au/wp-content/uploads/2016/10/Nasdaq-CTA-Cybersecurity-IndexSM-Methodology-1.pdf

This index helps in evaluating the 3 effectiveness:

1. Determining the rate of return on securities;
2. Determining the proportional increase in earning income;
3. Profitability of using stocks and securities with reinvestment potential.

Taking into account that all the above-mentioned indices work with large amounts of money, cyber-attacks occupy the highest level of risk from external risks, because its impact and the application of a risk strategy in relation to it are based on abstract management. This has a high impact on ensuring the growth of economic risks. Accordingly, we can achieve the determination of 4 indices using this evaluation method by improving it as follows:

$$S_i = \frac{(F_i+E_i+R_i)*P_{Fi}}{D_i}(1.2)1$$

Where $R_i$- economic risks of the target securities.

The introduction of risk assessment is appropriate to be compared by a cyber-attacker and focused on the formation of targeted cyber defenses, taking into account the risks due to the high probability of implementation based on the plan. Accordingly, we can determine the level of economic risks as the fourth index.

An economical cybersecurity strategy is futile without planning, projecting, and monitoring all possible cybersecurity avenues. This requires ensuring compliance with cyber hygiene standards. As a result of the correct implementation of the strategy based on the cyber compositional approach, the following can be achieved:

1. Planning reliable relationships and designing them consistently
2. Development of requirements and criteria for maintaining confidentiality, integrity and anti-transparency in the system and software, and the activity of the procedure to follow it.
3. Planning economic traps to accept the implementation of cyber attacks and keeping its design secret.
4. Operational security planning, separate maintenance of cyber defense units in the execution of the economic mission.
5. Assessment of economic risks of cyber-attacks and continuous control of sources of external flow of information.

1 Author development

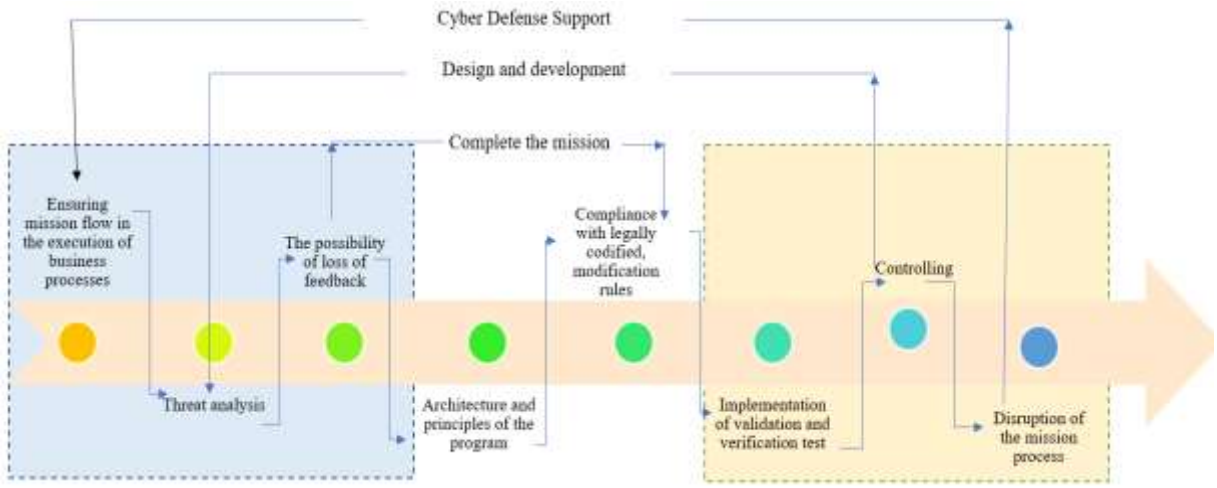


Figure 1.2. An Economic Cybersecurity Valuation Mechanism 1

The life cycle assessment mechanism of economic cyber security production includes 3 stages, and its impact on improving the organizational and economic mechanism of the enterprise is considered high (Figure 1.2).

In the figure above, the functionalization of the main mechanism is described only by threat management. But despite this, subjective threats are also justified by the fact that they require technological maturity.

In 2013, the concept of ensuring the integrity of the cyberspace was revealed by R. Norri of the "Gemalto" enterprise, who justified the need for an expert in the profile of economic cyber audit to register cyberattacks and use its library efficiently. Based on his proposal to use the Compromise Level Index in recording cyberattacks, the collected data, financial resources and the level of damage were analyzed in a summary form. According to him, it is necessary to create its classification in the analysis and control of cyber attacks2

The creation of a cyber economy classification can be changed, expanded and popularized after each cyber attack, and this is mainly the responsibility of the manager of the enterprise's cyber defense system. The classification of the cyber economy mainly covers the weaknesses of each country's economic infrastructure and the sectors and industries that need protection. It is mainly characterized by the provision of participation as technological support in the implementation of economic and financial machinations.

1 Dolan (muallif), Diana Barrero Zalles. Transparency in ESG and the Circular Economy: Capturing Opportunities Through Data. Business Expert Press 2021 y, 176 p

2 Shitova Yu.Yu., Shitov Yu.A. Sovremennые trendы ekonomicheskoy kiberbezopasnosti. Mir novoy ekonomiki [Modern trends in economic cybersecurity. The world of the new economy]. 2019;13(4):22-30. https://doi.org/10.26794/2220-6469-2019-13-4-22-30

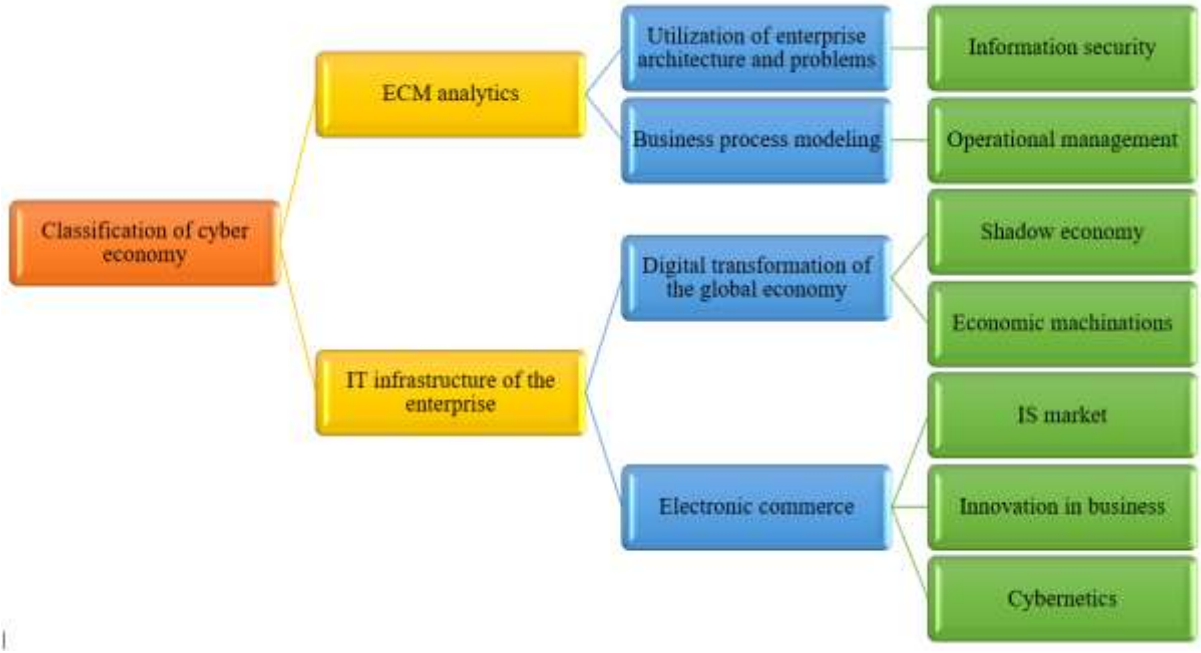


Figure 1.3. Classification hierarchy of cyber economy1

Based on the hierarchy presented in Figure 1.3, the implementation of cyber-economic attacks was observed by the "Gemalto" enterprise, in which it is considered that the corrupt economic system, money laundering and financial fraud schemes operate on the basis of digital technologies. In particular, the concept of the shadow economy is considered to be an economic manipulation model used mainly in tax payments, in which funds are illegally used to conduct sales of services and products and not to be formalized in order to avoid paying taxes. It forms the core of cyber-economic attacks, characterized by the digital concealment of hidden income and tax payment values based on the findings of cyber-economic auditors.

In the analysis of the cyber-economic classification, it is appropriate to study the factors affecting the implementation of cyber-economic activities.

1 Angus Bancroft. The Darknet and Smarter Crime: Methods for Investigating Criminal Entrepreneurs and the Illicit Drug Economy (Palgrave Studies in Cybercrime and Cybersecurity). Palgrave Macmillan, 2019 y, 254 p

Table 1.2.

Factors of origin of cyber-economic attacks 1

| № | Cyber economic attack factors | Cyber attack share (2016-2022) | Evaluation method | The composition of the evaluation method |
|---|---|---|---|---|
| 1 | Monthly salary | | | |
| 1. | Low monthly salary | 22% | $M_s = \frac{M_t - M_r}{X}$ | $M_s$- monthly salary of identified employees who carried out the cyber attack;<br>$M_t$- the value of the salary that the hacker should receive according to the tariff;<br>$M_r$- real time earnings;<br>X- the number of hackers who have carried out a cyber attack. |
| 2. | Low monthly wages will be investigated by the cyber economic auditor | 4% | $M_{sk} = \frac{M_{td} - M_{sr}}{X}$ | Msk- Monthly salary considerations for cyber attack research;<br>Mtd- the value of the wages that the workers should receive according to the tariff and given in the report;<br>Mr- real-time wages (checking through the tax database) values;<br>X- number of employees cyberattacked. |
| 2 | Economic machination | | | |
| 1. | On order from the owner of the enterprise | 14% | $I_m = \frac{I_t - M_t}{T_t - S_t}$ | $I_m$- coefficient of economic machination;<br>$I_t$- economic payments;<br>$M_t$- cost of financial transactions;<br>$T_t$- the value of the material assets of the goods taken into account and its income;<br>$S_t$- tax payments on goods sold. |
| 2. | Collection of money from insurance companies | 15% | $S_m = \frac{I_t - M_t}{B_{tl} - S_{g't}}$ | $S_m$- machination factor through insurance;<br>$B_{tl}$- the cost of damaged goods;<br>$S_tg$- insured object and its coverage percentage (according to the contract). |
| 3. | Financial blackmail | 7% | - | Economically inactive use of credit operations and private funds. |
| 3 | Experience and testing | | | |
| 1 | System robustness testing | 5% | - | To test the systematic attempts and capabilities of hackers |

1 Laxani K. Yansiti M. sifrovoe preimuщestvo. Isskustvo konkurirovat v epoxu isskustnogo intellekta [Digital advantage. The art of competing in the era of artificial intelligence]. Bambora, M.: 2021 g, 319 str, Pavlyuk Yu. Digital vsemonuщiy. 101 instrument dlya povыsheniya prodaj s pomoщyu sifrovыx texnologiy. Eksmo, 2021 g, 208 str.

The cyber economic attack shares presented in the above estimation method were generated from reports within the Global Cyber Security Program. Also, the evaluation table did not reflect the logistical diversion of medical drugs, embezzlement of pension funds, as well as cyber-attacks on payment cards, because these attacks were mainly carried out through communication.

In the organizational and economic activities of energy industry enterprises, information security mechanisms have high confidentiality and create a border based on research through relevant annual reports, strategic and cooperative programs and projects in the world experience.

## REFERENCES

1. ITU Global Cybersecurity Agenda (GCA). A framework for international cooperation in the field of cybersecurity.
2. Steve Grobman. The Second Economy: The Race for Trust, Treasure and Time in the Cybersecurity War. Apress. 2016 u, 374 r
3. 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 16, 2023, https://insights.sei.cmu.edu/blog/six-key-cybersecurity-engineering-activities-for-building-a-cybersecurity-strategy/
4. https://www.ifap.ru/pr/2008/080908aa.pdf
5. Nasdaq CTA Cybersecurity IndexSM Methodology. 2015 y https://www.betashares.com.au/wp-content/uploads/2016/10/Nasdaq-CTA-Cybersecurity-IndexSM-Methodology-1.pdf
6. Dolan (author), Diana Barrero Zalles. Transparency in ESG and the Circular Economy: Capturing Opportunities Through Data. Business Expert Press 2021 u, 176 r
7. Shitova Yu.Yu., Shitov Yu.A. Sovremennie trendi ekonomicheskoy kiberbezopasnosti. Mir novoy ekonomiki [Modern trends in economic cybersecurity. The world of the new economy]. 2019;13(4):22-30. https://doi.org/10.26794/2220-6469-2019-13-4-22-30
8. Angus Bancroft. The Darknet and Smarter Crime: Methods for Investigating Criminal Entrepreneurs and the Illicit Drug Economy (Palgrave Studies in Cybercrime and Cybersecurity). Palgrave Macmillan, 2019 u, 254 r

9. Laxani K. Yansiti M. sifrovoe preimuщestvo. Isskustvo konkurirovat v epoxu isskustnogo intellekta [Digital advantage. The art of competing in the era of artificial intelligence]. Bambora, M.: 2021 g, 319 str, Pavlyuk Yu. Digital vsemonuщiy. 101 instrument dlya povisheniya prodaj s pomoщyu sifrovix texnologiy. Eksmo, 2021 g, 208 str.

10. Mukhammadkhuja Sobirkhuja ugli Saitkamolov. Legal fundamentals of sustainable development of energy industry enterprises, Turkish Journal of Physiotherapy and Rehabilitation, 45360-45374, 2022

11. Saitkamolov Muxammadxudja Sobirxudja ugli. (2022). Sovremennie tendensii razvitiya energetiki [Modern trends in energy development]. Texasskiy jurnal mejdissiplinarnix issledovaniy, 6 , 222–230. Polucheno s https://zienjournals.com/index.php/tjm/article/view/1087.

12. Saitkamolov Mukhammadkhuja Sobirkhuja ugli. “Modern Tendencies in the Development of the Energy Industry”. Texas Journal of Multidisciplinary Studies 6 (March 27, 2022): 222–230. Accessed November 7, 2023. https://zienjournals.com/index.php/tjm/article/view/1087.

13. Nargiza I. Raqamli iqtisodiyotda blokcheyn texnologiyasi hamda uning ishlash mexanizmlari [Blockchain technology and its working mechanisms in the digital economy] //International Journal of Contemporary Scientific and Technical Research. – 2023. – S. 220-223.

14. Iminova N., Xamidullayev B. Development prospects of the postal service in the fourth industrial revolution //International Journal of Advance Scientific Research. – 2023. – T. 3. – №. 10. – S. 52-60.