Research of the impact on the ecology of the state of cybersecurity of the critical infrastructure objects

Volodymyr Mokhor[1], *Oleksandr* Korchenko[2], *Serhii* Honchar[1*], *Maxsim* Komarov[1], and *Alla* Onyskova[1]

[1] Pukhov Institute for Modelling in Energy Engineering of NAS of Ukraine, 15, General Naumov Str., Kyiv, 03164, Ukraine
[2] University of Bielsko-Biala, 2, Willowa Str., Bielsko-Biala, 43-309, Poland

Abstract. The analysis of the impact on the ecology of the state of cybersecurity of critical infrastructure objects and the factors influencing the state of cybersecurity of the information system of the critical infrastructure object is performed. An explanation is given of why cybersecurity violations in automated process control systems can lead to consequences in the industrial sector and environmental impact. The need to develop effective and adequate proposals and measures for cybersecurity of information systems of the critical infrastructure objects is shown. The classification of assets that are the objects of cyberattacks by attackers and the categories of impact on the critical infrastructure objects are given. Approaches to determining the cyber threat risk factor of the critical infrastructure object and the relevance of threats are presented. The method of assessing the degree of possible damage from the implementation of information security threats is considered. The results of this analysis can be used to develop proposals and measures to avoid the effects of cyberattacks on the critical infrastructure objects. The prospect of further research is to develop a methodology for determining the relationship between specific cyberattacks and possible quantitative damage.

1 Introduction

The current stage of development of society is characterized by the introduction of new technologies, which is a sign of the level of economic development of the country. The growing role of the information sphere for the economy of the state is associated with its rapid entry into the communications, transport, energy, financial, defense and other spheres.

Strategically important for the functioning of the economy and security of the state, society and population are the critical infrastructure objects - enterprises and institutions (regardless of ownership) of industries such as energy, chemical industry, transport, information technology and telecommunications (electronic communications), food, health care, utilities. Therefore, given that in modern society cyberattacks are becoming more frequent and tend to have a significant and lasting impact through enterprises on the economy, it is undeniable that reliable protection against cyberattacks actively affects the state of economic, political, social, defense and other components, national security of the state [1].

It is obvious that the disruption of the critical infrastructure objects of the state can lead to emergencies related to deaths, environmental disasters, causing great material, financial, economic damage or large-scale disruptions of cities and towns, etc. In these circumstances, security, including cybersecurity of the critical infrastructure objects of the state, plays an extremely important role.

Unlike traditional IT systems, in Automated Process Control Systems, which operate on the critical infrastructure objects, there is a fairly close relationship between automated systems and physical processes and actuators [2]. Therefore, the violation of cybersecurity in the Automated Process Control Systems can lead to consequences in the industrial sector and environmental impact.

In view of the above, it is necessary to analyze the impact on the environment, and, as a consequence, to develop effective and adequate proposals and measures for cybersecurity of information systems (IS) of the critical infrastructure objects to prevent such impacts.

2 Analysis of previous publications

A significant part of publications, in particular [3-8], is devoted to the study of problems related to the environmental impact of the state of cybersecurity of IS of the critical infrastructure objects.

In [9-12] shows along with the benefits of accurate and economic control of these digital I&C systems comes the challenges of cybersecurity. Especially with the growth of industry-targeted cyber-attacks in both numbers and capabilities, an overall understanding of the current cybersecurity status is important for further cybersecurity research and deployment improvement. Cyber-attacks against critical energy infrastructure have gone from

* Corresponding author: sfgonchar@gmail.com

possible to eventual to actual. With electrical generation sources in the United States changing under a wide range of pressures, the current fleet of nuclear power plants in the United States provides a reliable and sustainable source of electrical generation capacity. However, in order to extend the lifetime of the fleet, modernization upgrades to digital instrumentation and control systems are required. While this produces many opportunities for increased efficiency, it introduces a new level of complexity for securing and reliably operating reactors in the presence cyber-threats. The United States Nuclear Regulatory Commission recently began urging stronger cybersecurity efforts at nuclear power plants. As upgrades at nuclear power plants begin, the implementation of digital instrumentation and control systems to monitor and run the power plant introduces new vulnerabilities that must be addressed. This necessitates a more modern discussion of risk.

However, today, for all its importance, the issue of the environmental impact of the state of cybersecurity of the critical infrastructure objects remains insufficiently studied and researched and is in urgent need of development.

3 The research results

Cyberattacks are aimed at damaging assets. An asset is an entity that is valuable to an individual, organization, or state. Therefore, security programs are aimed at protecting assets from damage.

Assets of the critical infrastructure objects can be classified by type as follows [13]: physical, logical, human.

Consider in more detail each of the types of assets.

Physical assets include any physical components or groups of components that belong to the organization. In the critical infrastructure objects, they include: control systems, physical components of the information transmission network or any other physical objects that are in some way involved in the management processes and analysis of production processes.

Logical assets may include intellectual property, algorithms, expertise, or other information elements that include the ability of an organization or innovation to function. In addition, these types of assets may contain a public reputation, customer confidence, or other measures that, if damaged, directly affect the production process. Logical assets may be presented in the form of personal memory, documents, information contained on physical or electronic media and include test results, regulatory data, or any other information that is treated as confidential or private. Loss of logical assets often causes significant damage to the organization for a long time.

IS of the critical infrastructure objects assets are a special form of logical assets. They contain the logic of automation, which is involved in the implementation of production processes. These processes are highly dependent on the repetition or continuous execution of well-defined events. Therefore, damage to these assets, such as removal or unauthorized modification, may result in loss of integrity or availability directly to the process itself.

Human contain people, knowledge, as well as theoretical and practical skills that they possess and that are related to their production activities. These may include the necessary certificates or important skills needed to act in an emergency.

Assessment of asset losses can be expressed either quantitatively or qualitatively [13].

A quantitative assessment of an asset provides an accurate answer about the financial costs associated with that asset. This may be the replacement cost, the value of the lost sale or other monetary policy measures.

Qualitative valuation of assets is usually expressed more at the abstract level, such as percentages or relative values. Many assets can only be analyzed in terms of qualitative losses.

Losses in IS of the critical infrastructure objects can be classified as direct and indirect.

Direct losses are costs that are associated with the replacement of assets. Damage may occur due to physical damage to the asset, as a result of loss of integrity or availability, interruption of the exact sequence or change in the nature of the process. Logical assets have relatively low direct losses in relation to their usefulness, because the media used to store the asset, as a rule, has a low cost. Minor damage to human assets with a short recovery time can have low direct damage to the organization, even in the case of long-term consequences for the injured person.

Indirect losses are losses caused by loss of assets. These may include losses associated with downtime, recycling or other production costs due to loss of assets.

For physical assets, indirect losses typically include the consequences that arise from the loss of components. Indirect damage from equipment damage may result in repairs, reengineering, or other efforts to regain control of the industrial process. For logical assets, indirect losses are often very large. These include loss of public confidence, loss of business license, loss of competitive advantage from the issuance of intellectual property, such as confidential process, new technologies and so on.

You can correlate the types of losses for each type of assets by sorting the above data by type of assets and the way of expressing their valuation.

The danger of cyber threat in the critical infrastructure objects automated systems from many threats will be determined by assessing the possible consequences of its implementation from the standpoint of impact on the operation of the critical infrastructure objects automated systems, and the severity of such consequences - the risk factor of this threat [14].

Each threat to the cybersecurity of information system circulating in the information system of the critical infrastructure object can be described as follows:

$$n = f\{Z_n, U_n, K_n, H_n, C\} \quad (1)$$

where Z_n is the source of the nth threat to cybersecurity of the information system;

U_n - vulnerabilities due to which it is possible to implement the nth threat to cybersecurity of the information system;

K_n - favorable conditions for the implementation of the *n*th threat to cybersecurity of the information system of the critical infrastructure object of the energy sector;

H_n - consequences of the implementation of the *n*th threat to cybersecurity of the information system of the critical infrastructure object;

C - assets of the critical infrastructure object, which may be damaged in the event of the *n*th threat to cybersecurity of the information system.

The threat to the security of information circulating on the critical infrastructure object will be considered relevant if for the specified object of critical infrastructure with the set structural and functional characteristics and features of functioning there is a probability of realization of the considered threat by the intruder with the appropriate potential and its realization will lead to unacceptable losses from violation of confidentiality, integrity or availability of information.

This is due to the fact that in automated systems of the critical infrastructure object there is a very close relationship between automated systems and physical processes and actuators [14]. Therefore, information security breaches in these systems can have consequences in the industrial sector.

Given the above, the risk of threat in automated systems of the critical infrastructure object from many threats will be determined by assessing the possible consequences of its implementation from the standpoint of impact on the operation of automated systems of the critical infrastructure object, and the severity of such consequences - the risk factor of this threat [14].

The relevance of the *n*th threat to cybersecurity of the information system in general can be described as follows:

$$A_n = f\{P(H_{nu}|K_n); H_n\} \quad (2)$$

where $P(H_{nu}|K_n)$ is the probability of realization of the *n*th threat using the *u*th vulnerability, provided there are favorable conditions for this K_n; H_n - the consequences of the implementation of the *n*th threat to cybersecurity of the information system of the critical infrastructure objects.

The probability of a threat can be determined based on the analysis of statistical data on the frequency of information security threats (occurrence of security incidents) in automated systems of the critical infrastructure objects and / or similar systems.

In the absence of such statistics, the relevance of the threat is determined by assessing the feasibility of the information security threat, which in turn is determined by assessing the level of security of automated system of the critical infrastructure objects and the potential of the intruder required to implement the threat.

The hazard ratio can be determined by assessing the extent of the consequences of the breach of confidentiality, integrity or availability of information in automated systems of the critical infrastructure objects.

The relevance of information security threats is determined in relation to the threats for which the following is determined by the expert method:

- opportunities (potential) of the intruder are sufficient to realize the threat to information security;
- in the automated system of the critical infrastructure objects there are potential vulnerabilities that can be used in the implementation of a certain threat to information security;
- structural and functional characteristics and features of the functioning of the automated system of the critical infrastructure objects do not exclude the possibility of using the methods necessary to implement a particular threat, i.e. there is a scenario of threat realization;
- the implementation of the threat to information security will lead to a violation of confidentiality, integrity or availability of information, which may result in unacceptable negative consequences, causing significant harm.

Sources of information on the initial data on information security threats and their characteristics can be basic and standard models of information security threats, defined by regulations for different classes and types of automated systems.

Let's estimate the probability of realization of the threat to information security. The probability of information security threat will be understood as an indicator determined by an expert, which characterizes the value of the probability of realization of a certain (*n*th) information security threat in the automated system of the critical infrastructure object with specified structural and functional characteristics and features. For this purpose it is necessary to enter gradations of this indicator concerning the nth threat which can be described as follows:

$$P(R_n) = f(K_n; S_n; q_n; \omega_n) \quad (3)$$

where K_n - the presence or absence of favorable conditions for the implementation of the *n*th threat;

S_n - the presence or absence of the necessary statistics on the facts of the *n*th threat (the occurrence of incidents of cybersecurity violation of the information system);

q_n - the presence or absence of potential intruders of motivation to implement the *n*th threat, internal and / or external destabilizing factors, i.e. the model of the intruder and the threat model of the information system of the critical infrastructure object of the energy sector;

ω_n - the possible frequency of the *n*th threat.

In the absence of the necessary data to assess the probability of implementation of information security threats or doubts about the objectivity of expert assessments in determining the gradations of the probability of information security threats, the relevance of the *n*th information security threat is determined by assessing its feasibility.

The possibility of implementing the *n*th threat to information security can be assessed based on the level of security of the automated system and the potential of the intruder required to implement this threat to information security in the automated system of the critical infrastructure object with specified structural and functional characteristics and features. Therefore, the possibility of realizing the *n*th threat can be described as follows:

$$W(H_n) = f(X_n; Y_n) \quad (4)$$

where X_n - the level of protection of the automated system of the critical infrastructure object for the implementation of the *n*th threat; Y_n - the potential of the intruder required to implement the *n*th threat, i.e. the threat model.

It is obvious that when putting an automated system of the critical infrastructure object into operation, a high level of protection from the intruder with a given potential must be provided.

However, in the course of operation of automated systems of the critical infrastructure objects new vulnerabilities of systems, increase of potential of the intruder, change of structural and functional characteristics, importance of the processed information, features of functioning of the specified systems and other conditions leading to emergence of new threats to information security can significantly reduce the level of design security of these systems. In this case, in order to maintain the level of protection of automated systems of the critical infrastructure objects during operation, a regular analysis of changes in information security threats should be conducted, and current information security threats should be periodically re-evaluated.

Thus, the level of security of the automated system of the critical infrastructure objects can be determined based on the analysis of the following information:

- whether there are additional threats to information security during operation;
- whether information protection measures can be taken against additional information security threats that have arisen during operation;
- how quickly you can neutralize additional threats to information security that have arisen during operation.

The potential of the intruder to implement a particular threat to information security can be determined on the basis of data provided in the basic and standard models of information security threats, which are determined by regulations for IS of different classes and types.

To assess the degree of possible damage from the implementation of information security threats, the possible outcome of the information security threat in the automated system of the critical infrastructure objects, the type of damage that can lead to the implementation of information security threats, the degree of consequences of the implementation of information security threats for each type of damage.

As a result of the threat to information security, direct or indirect effects on the confidentiality, integrity, availability of information circulating in the automated control system of the critical infrastructure objects are possible [14].

Direct impact on the confidentiality, integrity, availability of information is possible as a result of the implementation of a direct threat to information security. In this case, the objects of the threat are directly information and / or other objects of protection that ensure the receipt, processing, storage, transmission, destruction of information in automated systems of the critical infrastructure objects, as a result of access to which or impact on which the impact on privacy, integrity or availability of information is possible.

Indirect impact on the confidentiality, integrity, availability of information is considered as a result of the implementation of indirect threats to information security. The implementation of indirect threats to information security does not directly affect the confidentiality, integrity, availability of information, but creates the conditions for the implementation of one or more direct threats to information security, which allow to implement such an impact. In this case, as a result of the implementation of an indirect threat, it is necessary to consider the results of the implementation of all direct threats to information security, which can be implemented in the case of the implementation of this indirect threat.

In determining the degree of possible damage, it is necessary to assume that depending on the goals and objectives of the automated system of the critical infrastructure objects, types of information processed, the impact on confidentiality, integrity or availability of each type of information contained in the system may lead to different types of damage. In this case, different owners of information will be characterized by different types of damage.

As noted in [13], the main categories of influence in automated control systems of the critical infrastructure objects are:

- physical impact - includes many direct consequences of accidents of the Automated Process Control Systems. The most important potential consequences are those that can lead to injury and death. Other consequences include loss of property (including data) and potential damage to the environment;
- economic impacts - the consequences of the second order from the physical impacts that are derived from accidents of the Automated Process Control Systems. Physical impact can have consequences for the system, which in turn can cause greater economic damage to the enterprise or organization. On a large scale, these effects can negatively affect the local, regional, national levels, and possibly the global economy;
- social influences - the consequences of the second order, which are derived from the loss of state or public confidence in the organization.

Given the above categories of impacts in automated control systems of the critical infrastructure objects, it is possible to list the consequences of these impacts [13]:

- violation of national security;
- facilitating the commission of an act of terrorism;
- loss or reduction of production;
- injuries or deaths;
- damage to equipment;
- emission (leakage, evaporation) or theft of hazardous materials;
- environmental damage;
- criminal or civil obligations;
- loss of private or confidential information;
- loss of brand image or customer trust.

These consequences may be supplemented by other types depending on the goals and objectives solved by the automated system of the critical infrastructure objects, as well as the type of information that is processed in it.

The degree of possible consequences of the implementation of information security threats is determined by the degree of negative consequences of the violation of confidentiality, integrity or availability of each type of information circulating in the automated system of the critical infrastructure objects.

Thus, the degree of negative consequences of breaches of confidentiality, integrity or availability of information is determined for each type of damage, depends on the goals and objectives performed by the automated system of the critical infrastructure objects, and may have different meanings for different information owners and operators, and is determined by experts.

If two or more types of information are processed in an automated system of the critical infrastructure objects, the degree of possible damage must be determined separately for each type of information circulating in the system. The final degree of possible damage will be determined by the highest value of the degree of possible damage, determined for the confidentiality, integrity, availability of each type of information.

Every cyber threat, if implemented, leads to destructive ones. The relationship between threats and destructive actions that arise as a result of the implementation of these threats can be represented as a matrix:

$$G = [g_{dn}] \quad (5)$$

where d varies from 1 to D; D - the number of possible destructive actions; n varies from 1 to N; N - the number of cyber threats.

The elements of the matrix (5) become 1 if the nth cyber threat leads to the implementation of the dth destructive action, and become 0 - otherwise.

Let B_d be the coefficient of danger of performing the dth destructive action, where d varies from 1 to D; D - the number of possible destructive actions.

Then, given that in the case of the implementation of the nth cyber threat may be several destructive actions, the risk factor of the nth cyber threat will be determined as follows:

$$B_n = \Sigma B_d g_{dn} \quad (6)$$

where B_d – the coefficient of risk of execution of the dth destructive action, determined by the severity of the consequences of this execution, as an indicator of the criticality of the energy sector; g_{dn} – a coefficient that is defined as an element of the matrix (5).

The analysis of existing information security systems allows to determine the main components of the cyber security system of information systems of the critical infrastructure objects:

- normative-legal;
- organizational;
- technical;
- training, retraining and advanced training of relevant specialists.

Each of the above components, in one way or another, affects the state of cybersecurity of IS of the critical infrastructure objects.

Thus, one of the topical issues is the availability of regulatory framework for cybersecurity of IS of the critical infrastructure objects, bringing the national regulatory framework for cybersecurity of the critical infrastructure objects in line with international regulations; fulfillment of the coherence of the conceptual apparatus used in the existing national legislative and regulatory documents; finalization (if necessary - development) of regulatory documents, requirements, methodologies for threat assessment of facilities that are critical to the life of the state, the general methodology for risk assessment for critical facilities and critical infrastructure in general.

In addition, it should be noted that managers and / or owners of the critical infrastructure objects should be aware of the possibility and likelihood of cyberattacks and the consequences, if any. The implementation of cybersecurity measures requires additional resources, to which the managers of these objects do not always agree, and there is no mechanism that would require these managers to implement the necessary measures. Therefore, without the introduction of this mechanism, all standards, instructions, etc. on cybersecurity of IS of the critical infrastructure objects will be of a recommendatory nature, because the information circulating, for example, in Automated Process Control Systems, does not belong to any type of information subject to protection in accordance with applicable law.

Cyberattacks of an external intruder are opposed by the information protection system of the information system of the critical infrastructure objects, the functions of which must include:

- protection of the network perimeter;
- ensuring the security of interconnections;
- security monitoring and audit;
- detection and prevention of attacks;
- data backup and recovery;
- security analysis and security policy management;
- data integrity control;
- protection against malicious software;
- content filtering and prevention of leakage of confidential information;
- installation of software updates;
- security administration.

According to the results of the analysis of threats and vulnerabilities [13], it can be noted that the protection of such systems should be considered in the following areas:

- protection of information and physical components of IS of the critical infrastructure objects;
- technical information protection of IS of the critical infrastructure objects;
- protection of processes, procedures and programs of information processing of IS of the critical infrastructure objects;
- protection of communication channels of IS of the critical infrastructure objects;
- suppression of spurious electromagnetic radiation;
- management and control of the protection system.

Thus, taking into account the above, it can be noted that the state of cybersecurity of IS of the critical infrastructure objects is influenced by the following factors:

- availability of the necessary and sufficient regulatory framework for cybersecurity of IS of the critical infrastructure objects;
- the presence of sources of cyber threats, their capabilities, type, purpose, motives, interest in cyberattacks;
- the presence of vulnerabilities in cyber defense systems that can be used in cyberattacks;
- the presence or absence of favorable conditions for the implementation of cyber threats;
- the attractiveness of the assets to which cyberattacks are actually directed;
- consequences of the possible implementation of cyber threats;
- the level of professional training of employees responsible for cybersecurity at all levels: organization, enterprise, industry, department, etc.

4 Conclusions

The analysis of the ecological impact of the state of cybersecurity of the critical infrastructure objects and the factors influencing the state of cybersecurity of the information system of the critical infrastructure object is performed. The method of assessing the degree of possible damage from the implementation of information security threats is considered.

The results of the analysis can be used to develop proposals and measures to avoid the effects of cyberattacks on the critical infrastructure objects.

The prospect of further research is to develop a methodology for determining the relationship between specific cyberattacks and possible quantitative damage.

References

1. *Zakon Ukrayiny «Pro osnovni zasady zabezpechennya kiberbezpeky Ukrayiny»* (Law of Ukraine "On the Basic Principles of Cyber Security of Ukraine"). 2163-VIII (Kyiv, Bulletin of the Verkhovna Rada of Ukraine, 2017).
2. Guide to Industrial Control Systems (ICS) Security: NIST Special Publication 800-82, Recommendations of the National Institute of Standards and Technology.
3. K. Jeong, B. Choi, J. Moon, D. Hyun, J. Lee, I. Kim, G. Kim, S. Kang, Risk assessment on abnormal accidents from human errors during decommissioning of nuclear facilities. Annals of Nuclear Energy. 87(P2), 1-6 (2016). https://doi.org/10.1016/j.anucene.2015.08.009
4. I.V. Blinov, Ye.V. Parus, H.A. Ivanov, Imitation modeling of the balancing electricity market functioning taking into account system constraints on the parameters of the IPS of Ukraine mode. Technical Electrodynamics. 6, 72-79 (2017). doi:10.15407/tech-ned2017.06.072
5. V.O. Artemchuk, T.R. Bilan, I.V. Blinov et al., ed. by A.A. Zaporozhets, T.R. Bilan, *Teoretychni ta prykladni osnovy ekonomichnoho, ekolohichnoho ta tekhnolohichnoho funktsionuvannya obyektiv enerhetyky* (Theoretical and applied bases of economic, ecological and technological functioning of energy objects). (Kyiv, 2017) http://doi.org/10.5281/zenodo.2540527
6. O. Popov, A. Iatsyshyn, V. Kovach, T. Yatsyshyn, I. Matvieieva, Analysis of possible causes of NPP emergencies to minimize risk of their occurrence. Nuclear and Radiation Safety. 1(81), 75-80 (2019). DOI: 10.32918/nrs.2019.1(81).13
7. Wanxia Xu, Jinman Wang, Min Zhang, Sijia Li. Construction of landscape ecological network based on landscape ecological risk assessment in a large-scale opencast coal mine area. Journal of Cleaner Production. 286, 125-523 (2020). https://doi.org/10.1016/j.jclepro.2020.125523
8. G.D. Banks, T. Fitzgerald, A sectoral approach allows an artful merger of climate and trade policy. Climatic Change. (2020). doi:10.1007/s10584-020-02822-2
9. F. Zhang, Nuclear power plant cybersecurity. Nuclear Power Plant Design and Analysis Codes. Chapter 21, 495-513 (2021). https://doi.org/10.1016/B978-0-12-818190-4.00021-8
10. J. Peterson, M. Haney, R.A. Borrelli, An overview of methodologies for cybersecurity vulnerability assessments conducted in nuclear power plants. Nuclear Engineering and Design. 346, 75-84 (2019). https://doi.org/10.1016/j.nucengdes.2019.02.025
11. I. Nash, Cybersecurity in a post-data environment: Considerations on the regulation of code and the role of producer and consumer liability in smart devices. Computer Law & Security Review. 40, 105529 (2021). https://doi.org/10.1016/j.clsr.2021.105529
12. M. Lezzi, M. Lazoi, A. Corallo, Cybersecurity for Industry 4.0 in the current literature: A reference framework. Computers in Industry. 103, 97-110 (2018). https://doi.org/10.1016/j.compind.2018.09.004
13. Industrial communication networks – Network and system security. IEC 62443-1-1. Part 1-1: Terminology, concepts and models.
14. S.F. Honchar, *Otsinyuvannya ryzykiv kiberbezpeky informatsiynykh system obyektiv krytychnoyi infrastruktury* (Estimation of cybersecurity risks of information systems of critical infrastructure objects). (Alpha Advertising, Kyiv, 2019) ISBN: 978-966-288-263-6