Categorization of objects of critical information infrastructure of water transport

Sergey Sokolov[1,1], *Nikolay* Glebov[1], *Kristina* Natashova[1], *Oleg* Gubernatorov[1]

[1]Admiral Makarov State University of Maritime and Inland Shipping, St. Petersburg, 198035, Russia

Abstract. The transport complex is a complex network with many add-ins and the transfer of large amount of information in real time. Identifying the critical transport information infrastructure is the first step in the process of ensuring security and protecting the availability of critical objects. This paper contains the author's recommendations on the implementation of Russia Federal Law No. 187-FZ regarding the categorization of objects of critical information infrastructure in the field of water transport.

1 Introduction

As international experience shows, damage to critical information infrastructure (CII) of water transport can lead to critical consequences.

In June 2017, shipping giant A. P. Moller-Maersk underwent a major cyberattack - computer systems failure affected all of the company's business units, including container shipping, port and towing operations, oil and gas production, drilling services and oil tankers [1]. Such failures of critical automation systems prove that cyberattacks have a significant impact on critical infrastructure. This can lead to negative social, political, economic, environmental consequences, consequences for the defense of the country, the security and safety of the state. Water transport plays an important role in the transport system of the Russian Federation. Thus, the need to ensure the sustainability of water transport infrastructure against cyberattacks is a key issue at the national level.

Federal Law No. 187-FZ of July 26, 2017 "On the Security of Critical Information Infrastructure of the Russian Federation", which entered into force in 2018, can be considered the newest regulatory legal act regulating issues of information security of sea and river transport of the Russian Federation [**Error! Reference source not found.**]. According to this Federal Law, owners of CII should be connected to the State System for the Detection, Prevention and Mitigation of Computer Attacks (GosSOPKA (Federal SOC)), make a list of CII objects and assign them one of the three categories of significance. Bringing objects into compliance with the requirements of Federal Law No. 187-FZ is an urgent task. The first step is to carry out the categorization of CII objects. In the field of water transport, this stage requires, among other things, a deep study of the organizational side of the issue.

[1] Corresponding author: sokolovss@gumrf.ru

In pursuance of this Federal Law, a system of subordinate regulatory legal acts and methodological documents has been put into effect. Thus, the categorization is carried out by subjects of CII in accordance with the requirements of the Resolution of the Government of Russia No. 127 of February 8, 2018 "On Approval of the Rules for Categorizing the Objects of Critical Information Infrastructure of the Russian Federation, and also the list of indicators of the criteria of significance of the objects of critical information infrastructure of the Russian Federation and their values" (Hereafter - Resolution), which is intended to determine the most significant information infrastructure objects, the disruption of the functioning and operating of which can lead to significant consequences [4].

Categorization of CII objects is the process of comparing each individual CII object with criteria and indicators of significance. In accordance with the law, the subject of CII is obliged to consider each of its objects: to assess the consequences that will follow in case of violation of the activities of this CII object, to compare with the criteria given in this Resolution, and to make a conclusion about the category of significance of this object.

2 The tasks of the categorization process

A. The first task of the categorization process is to classify the organization as a subject of CII.

Who are the subjects of CII? These are state bodies and institutions, individuals and legal entities, individual entrepreneurs, which own CII objects on any legal basis: Information systems (IS), Information and telecommunication networks (ITCN), Automated control systems (ACS), which function in the transport field of activity. There are cases when the CII object belongs to one subject, but for the purposes of economic activity, it is used by another subject of CII. In this case, the assessment of the categorization must be carried out by the subject-owner on the basis of the data that he receives from the economic entity.

How can the economic entity determine whether it is a subject of CII or not? First of all, an organization may apply to the Russian National Classifier of Types of Economic Activity (OKVED). OKVED will clearly indicate whether the company belongs to the list of industries specified in the FZ-187. As for the scope of activities of water transport, this activity is defined under the OKVED 50 class.

One can refer to the list of licenses and other permits, which also define the types of activities for which permission is required in accordance with Russian legislation. By the mentioned types of activities, one can relate his organization to the field of activity prescribed by law. In water transport, the following activities are subject to licensing: the carriage of passengers and goods by inland and sea transport, the handling of dangerous goods in water transport and seaports, the towing by sea transport (except for the own needs of a legal entity or an individual entrepreneur) [7].

Each organization has regulations, the provisions in accordance with which it operates. It also describes the types of activities that can be correlated with the definitions that legislation provides.

This is not an exhaustive list, there are other options. But this one is the most obvious.

B. The second tasks: definition of CII objects.

To do this, it is necessary to make an inventory of information, software and technical resources. After that, it is necessary to determine the purpose of information processing and identify managerial, technological, production and (or) other processes that are implemented in terms of performing functions (powers) or activities of subjects of CII. Based on the purpose of information processing, it is possible to select:

1. Information systems:
   1.1. Coastal information systems;

1.2. On-board information systems;
1.3. Electro-cartographic systems;
1.4. Port technology systems.
2. Information and telecommunication networks;
3. Automated control systems.

3 The categorization commission

Let us proceed to the process that the owner of the CII object must carry out in order to categorize the objects belonging to him - to fulfill the requirements of the Resolution. First of all, in accordance with the Resolution, the subject should establish a categorization commission. It is established by the decision of the head of the CII subject. The commission is headed either by the manager himself or by the person to whom these powers are delegated.

The commission should include:

- employees of CII who are responsible for the main processes taking place in the subject, who are experts in the field of the performed functions, the activities carried out, the field of information technology;
- employees who are responsible for ensuring the safety of CII, including information security.
- in the case when an organization has a state secret protection department, their representatives should also be included in the commission.
- employees entrusted with powers of civil defense and emergency.
- in concern with the Federal body or legal entity that determines the policy, legal regulation in the established field of activity, representatives of this legal entity may be included. That is, if we have a subject that carries out water transport activities, then in concern with the Ministry of Transport of the Russian Federation and (or) the Federal Agency for Maritime and River Transport, their representatives can be included in the commission of the subject.

The commission is established, what to do next? Further, initial data are prepared, which will be considered by this commission. The list of initial data is also given in the Resolution:

- information about the object that is considered for categorization: purpose, architecture, applied software and hardware, interaction with other CII objects, interaction with communication networks;
- processes in the framework of the performance of functions (powers) of the implementation of activities of the CII subject. If, in accordance with the legislation, the subject falls within any of the activities of declaring or categorizing, then these documents should also be taken into account. For example, the declaration of industrial safety;
- information on the interaction with other objects of CII. If the activity of the object in question is violated, the question will accordingly arise: “Will the functionality of other significant objects be violated?”;
- information security threats and computer incidents that may arise for a particular object.

4 Definition of critical processes

CII objects that ensure processes should be categorized. What processes should we consider first? Management, technological, production. After the commission has

determined which processes take place in the subject of CII, the commission analyzes them and identifies those processes, the damage from the violation of which can be correlated with the criteria of significance, i.e. highlight critical processes.

On the basis of critical processes, the commission concludes what kind of CII objects ensure, manage, and monitor these processes. And on the basis of the list of objects, the commission develops a list of CII objects to be categorized. This list is approved by the subject of CII and is consistent with the regulator of the established scope of activity.

Within 5 days after approval, this list should be sent to the authorized security agency of CII, as a rule, to the FSTEC of Russia, in accordance with the recommended form [2].

Having received a list of objects to be categorized, it is necessary to directly start the categorization. The term for the subject is 1 year from the date of approval of the list of objects to be categorized.

5 Categorization

So, categorization is a comparison of an object with specific values of indicators and decision making - either about a specific category or that there is no need for a given object to assign a category. All this is done on the basis of an assessment of the scale of the possible consequences of the malfunction of the CII object. The list of indicators of criteria for the significance of the CII objects is also approved by the Resolution.

The law defines five groups of indicators of significance, in which the damage from the malfunction of the CII object is seen. Each group has its own indicators. Each object should be considered for each indicator and sub-indicator. The category is assigned according to the highest value: if the object by social significance belongs to the third category, but by environmental significance, the violations causing environmental harm will be of the first category, then the CII object should be categorized by the first category of significance.

There are three categories I, II, III in the Resolution: I - most import, the damage will be maximum, and III - the damage is minimal. But there may be a situation where the object does not fall within the values of any of the categories, i.e. the damage will be much less than that stated in the Resolution. In this case, a separate category arises - these are objects for which there is no need to assign a category [10].

The commission decided on the list of objects to be considered and determined the initial data. What does it do next? Examines the actions of possible violators, as well as from all sources of threats that may be relevant to the object. Next, it analyzes the security threats and vulnerabilities that may lead to the occurrence of incidents at objects. After that, it assesses the consequences in case of computer incidents at the object. And only after that it establishes the conformity of the object to a specific category of significance. At this stage, in order to model information security threats at the CII objects, one can refer to the Basic information security threat model in key information infrastructure systems and to the Methodology for determining current information security threats in key information infrastructure systems [3].

A. The act of categorizing.

Based on the conclusion of the commission, an act of categorizing CII objects is developed. This act must contain:

- information about the CII object;
- results of the analysis of information security threats;
- security measures implemented at the object;
- information on the assignment of a certain category of significance.

This act is signed by all members of the commission, approved by the head of the CII subject, and the subject must ensure that the categorization act is kept either until the significance category of the object is changed or until the object is decommissioned.

B. At the initial stage of categorization, the logical conclusion will be to send information to the FSTEC. From the date of approval of the categorization act, the subject has 10 days to send information to the authorized body for security of CII, i.e. to the FSTEC of Russia, in accordance with the Order of the FSTEC of Russia No. 236 in the approved form [5-9]. The form is filled in, information provided to the FSTEC. After receiving information about the categorization of a particular form, the FSTEC performs a verification procedure on compliance with the order of categorization as well as the correctness of the categorization. If everything is done correctly by the subject - the data is presented in full, then within 30 days, the FSTEC will put information about this significant CII object in the register of significant objects, and within 10 days from the date of submission, the subject will be notified that the information has been put and a specific number assigned. If a violation is detected, the FSTEC notifies in writing the subject of CII about the detected nonconformities within 10 days. After receiving the answer, the subject has 10 days to eliminate the identified violations and resubmit materials to the FSTEC of Russia. In accordance with the Resolution, at least once in five years, the subject must assess its critical objects and confirm that the category complies, or it has changed for some reasons. The FSTEC of Russia maintains a register in accordance with the regulatory legal act - the Order of the FSTEC of Russia No. 227, which describes the whole procedure and the deadlines that must be met [6]. For a more complete understanding of the issue under discussion, we offer you to take a look at the CII categorization scheme proposed by us (Fig. 1).

6 Conclusion

At the same time, objective contradictions may arise here, which will be eliminated in interaction with the regulator.

Typical disadvantages:

- underestimation of the values of the significance criteria;
- submission of the results of the assessment of possible damage not for all indicators of the significance criteria;
- lack of substantiation of the inapplicability of the significance criteria or the obtained values on the basis of the results of the assessment of possible damage;
- application of measures taken to ensure the safety of the object to substantiate the non-applicability of indicators of significance criteria;
- submission of incomplete information;
- preparation of information not in the form specified by the order of the FSTEC of Russia No.235.

In 2018, the FSTEC of Russia received information on the results of categorization of 2000 CII objects, of which 610 categorization results were returned for revision. According to an approximate estimate of the regulator, there are 28 000 CII objects in the country, and only 5% are accepted in the country.

For this reason, a schedule has been created for the preparation of regulatory legal acts in the field of ensuring security of CII of the Russian Federation No. 8705p-P10 of October 25, 2018. From which it follows that changes to the Rules for categorizing CII objects of the Russian Federation establishes the deadline for approval of the list of objects to be categorized - June 1, 2019.

With the entry into force of Federal Law No. 187-FZ, many questions arose for discussion: “How to do this?” And most importantly - “Why it is necessary to do this?”.

Answering the second question, it is worth mentioning that before January 1, 2018, there was a notion of "key systems of information infrastructure" (KSII) that was similar to "significant objects of CII". According to KSII, there was a certain structure of documents, where the Federal Law was the missing link. The main task of the Federal Law No. 187-FZ is to regulate relations in the field of ensuring the safety of CII in order to its stable functioning during cyberattacks.

A key innovation compared with the KSII methodology was the creation of GosSOPKA - the answer to the growth of computer attacks to effectively combat cyber threats and ensure uninterrupted operation of CII objects.

The new regulatory framework will ensure the improvement, development, and modernization of the CII objects. It is changed and supplemented in a timely manner, which will not allow evading the execution of prescriptions. Fulfilling the requirements of this Federal Law is an aggressive counteraction against computer incidents.

Organizations may assume that it is possible to evade the requirements. However, innovations for non-compliance with this Federal Law were also included in the new methodology. Any computer fraud, unauthorized access to data or the creation of malicious software can lead to criminal liability not only for the person who did it but also for the person who allowed it. Article 274.1 of the Criminal Code of the Russian Federation (hereinafter – the CC RF) for unauthorized access to protected computer information contained in CII and violation of the rules for the use of the storage, processing or transfer of protected computer information contained in CII is punishable by imprisonment for up to ten years. In case of consequences, the perpetrator falls within the structure of Article 293 of the CC RF "Negligence" [**Error! Reference source not found.**].

New legislation has identified new measures and means of ensuring the security of the most important objects. However, when categorizing, the subjects increasingly face the complexity of the processes and the need to take into account the specifics of a particular sector of the national economy. This determines the importance of developing sectoral regulations on categorizing and ensuring the safety of CII, the importance of developing typical models of violators, which would take into account, for example, such industry characteristics as cross-border interaction with foreign counterparties. It is also important not to forget that ensuring information security is a process, and it cannot be completed, it needs to be centrally managed at all levels, starting with the creation of federal centers of industry competencies in the field of information security of key assets. All this sets new tasks and determines the prospects for the development of the direction of ensuring safety of CII, including on water transport.

References

1. https://tass.ru/transport/4371193 (Last accessed: 10.03.2019)
2. https://fstec.ru/component/attachments/download/2006 (Last accessed: 10.03.2019)
3. https://fstec.ru/component/attachments/download/1904 (Last accessed: 10.03.2019)
4. https://fstec.ru/component/attachments/download/1916 (Last accessed: 10.03.2019)
5. https://fstec.ru/component/attachments/download/1900 (Last accessed: 10.03.2019)
6. https://fstec.ru/component/attachments/download/1896 (Last accessed: 10.03.2019)
7. http://www.consultant.ru/document/cons_doc_LAW_113658/ (Last accessed: 10.03.2019)
8. N. Glebov, A. Zhilenkov, S. Chernyi, S. Sokolov, "Process of the Positioning Complex Modeling Objects with Elements of Intellectual Analysis", Procedia Computer Science, vol. 150, pp. 609-615 (2019) Available: 10.1016/j.procs.2