International Journal of Engineering & Technology, 7 (2.23) (2018) 247-250

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET

Research paper

About the single system of protection classes of elements of critical information infrastructure by the criteria of importance and information security

Andey O. Kalashniov, Igor F. Mikhalevich*

Laboratory № 79, V. A. Trapeznikov Institute of Control Sciences of Russian Academy of Sciences, Moscow, Russia
**Corresponding author E-mail: mif-orel@mail.ru*

Abstract

In work on the basis of integration of criteria of elements of importance for critical information infrastructure and information security, and single network security trust model, a single system of protection classes of elements of critical information infrastructure is developed.

Keywords: *Use about five key words or phrases in alphabetical order, Separated by Semicolon.*

1. Introduction

Rapid development of infocommunication technologies and systems is accompanied by equally rapid development of technologies and means of violation of information security. Unauthorized disclosure, distortion or unavailability of information can have catastrophic consequences, especially if this information relates to the operation of a critical information infrastructure (CII). In these conditions, it is necessary to ensure the completeness of the complex of security measures CII from attacks, including the improvement of the scientific regulatory and legal and methodical framework the protection of CII.

2. Critical information infrastructure

2.1. General Provisions

Taking into account the impact of information on vital processes, we will include information systems, information and telecommunication networks, automated control systems operating in the spheres of state and municipal administration, state security, the country's defense capacity, justice, law and order, health care, science, transport, telecommunications, energy, industry, financial market and other sensitive areas for the public, as well as telecommunication networks used in their interests.

2.2. Elements of critical information infrastructure

Elements of CII (ECCI) it's the objects of CII (OCCI) on which information is created, processed and stored, lines and nodes of telecommunication networks used to organize OCII interaction and access to them users, also devices of users and any other terminals.

2.3. Criteria of categories of the importance of elements of critical information infrastructure

The importance of ECII is determined by the possible damage caused to vital interests (processes) in the event of a violation of ECII functioning. As criteria of the importance of ECII, social, political, economic, ecological importance, importance for ensuring defense of the country, safety of the state and law and order, and other criteria can be used.
The importance of ECII can be expressed, for example, in the following:

- social – in assessment of possible causing damage to life or health of people, the possibility of termination or violation of the functioning of life support facilities, transport infrastructure, telecommunication networks, as well as maximum time of lack of electronic access to justice systems, law and order, state and municipal services, etc. for recipients of such services;
- political – in assessment of possible causing damage to the interests of the country in questions of domestic and foreign policy;
- economic – in assessment of possible causing a direct and/or consequential damage to subjects of economic activity;
- ecological – in assessment of level of a possible environmental damage;
- etc.

2.4. Attacks on elements of critical information infrastructure

Attack – attempt to destroy, expose, alter, disable, steal or gain unauthorized access to or make unauthorized use of an asset ([1] point 3.2). The asset is meant as information of ECII and all other that has value for ECII.

3. Protection of elements of critical information infrastructure

3.1. Violations of information security

Information security – preservation of confidentiality, integrity and availability of information ([1] point 3.28). By protection (P)

ECII we will characterize property ECII to provide information security of the processed (stored, transferred) information:

$$P = (C;\quad I;\quad A), \text{ where} \tag{1}$$

C – confidentiality – property that information is not made available or disclosed to unauthorized individuals, entities, or processes ([1] point 3.10);
I – integrity – property of accuracy and completeness ([1] point 3.36);
A – availability – property of being accessible and usable on demand by an authorized entity ([1] point 3.7).
Attacks on ECII pursue a violation of information security as their ultimate or intermediate targets. The main targets of attacks on ECII are reflected in Figure 1.

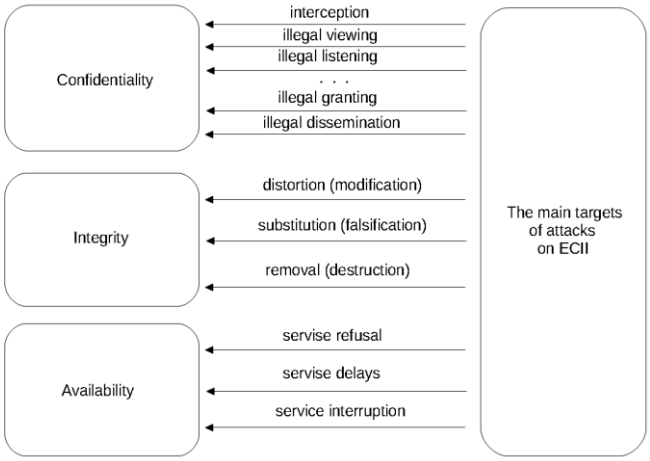

Fig. 1: The main targets of attacks on ECII

Confidentiality violations are fixed when information is compromised, which happen when at least one of the events happen:
• interception of information during the periods of its processing, storage or transfer in open form;
• illegal viewing (document, e-mail, etc.), listening, copying, granting or dissemination of information.
The specified list of events is open. If the information was compromising, then its confidentiality cannot be restored. Therefore, the integrated indicator (hereinafter integrated indicators are considered in relative values) confidentiality can accept values only 1 or 0:

$$C = \begin{cases} 1, & \text{if there is no compromising;} \\ 0, & \text{if there were compromising.} \end{cases} \tag{2}$$

About violation of integrity is evidence of violations of the authenticity of information. Authenticity is property that an entity is what it claims to be ([1] point 3.6). Violation of authenticity information happen in cases of partial distortion of its content (modification) or full substitution (falsification), as well as with complete removal (destruction). Authenticity can be restored. The integrated indicator of integrity can accept any value in the range from 1 to 0:

$$I = \begin{cases} 1, & \text{if autenticity is ensured;} \\ \le 1, & \text{if autenticity were violated.} \end{cases} \tag{3}$$

Violations of availability are fixed in cases of the constant or temporary blocking of information which are shown in refusal, delays, breaks (interruptions) of service. Blocking can be eliminated, and a service is restored. The integrated indicator of availability can accept any value in the range from 1 to 0:

$$A = \begin{cases} 1, & \text{if there no blockings;} \\ \le 1, & \text{if there were blockings.} \end{cases} \tag{4}$$

It should be noted that attacks, despite their initial target orientation, can also cause "related" violations of information security. For example, removal of information, as an attack on the integrity, at the same time leads to the fact that information is not available. Interrupting service when working with a database, which is an attack on availability, can cause data integrity problems. Attacks aimed at disrupting the integrity by modifying the configuration files can crash the server and cause a denial of service. Violation of the integrity of files with the rights and authority of users may violate the confidentiality of information. There are many such examples.

3.2. Ensuring the protection of elements of critical information infrastructure

The interrelation of the events influencing protection of ECII is presented in the Figure 2.

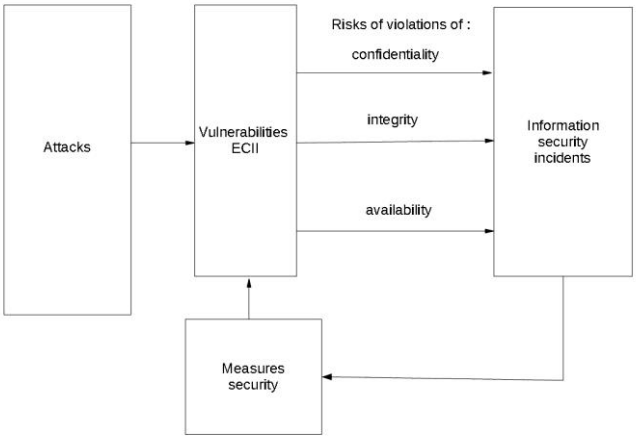

Fig. 2: The interrelation of the events influencing protection of ECII

The protection of ECII can be provided only in case the attacks did not cause incidents of information security. Information security incident – single or a series of unwanted or unexpected information security events that have a significant probability of compromising business operations and threatening information security ([1] point 3.31).
After the information security incident prior to taking security measures and verifying their sufficiency, the protection of ECII cannot be considered restored. On this basis, the integral indicator of ECII protection can take values of only 1 (before the incident or after the completion of the complex of security measures) or 0 (from the moment of the incident to the completion of the complex of security measures:

$$P = \begin{cases} 1, & \text{if} \quad C = 1, \quad I = 1, \quad A = 1; \\ < 1, & \text{if} \quad C = 1, \quad I \le 1, \quad A \le 1; \\ 0, & \text{if} \quad C = 0, \quad I \le 1, \quad A \le 1. \end{cases} \tag{5}$$

4. A single network security trust model of objects of critical information infrastructure

A single network security trust model (SNSTM) was developed using information security standards [1-3], recommendations on ensuring security of telecommunication systems [4, 5], solutions for creating a trusted environment for the operation of ECII [6].
By trust we will understand that ECII X trusts the subject Y with respect to some set of actions, if and only if in relation to these actions the subject Y behaves in a certain way.

In the context of SNSTM subjects of access to OCII X are any ECII which are outside this OCII including OCII interacting with it, terminals of users, lines and nodes telecommunication networks with which use access to OCII X is possible.
The key element of SNSTM is the OCII security domain. By analogy with [4, 5], a security domain is meant a set of the OCII elements, a security policy of ECII, a security authority of ECII and a set of security-relevant activities in which the elements are managed in accordance with the security policy determined by administration of OCII.
The functional reference architecture of OCII is based on functional objects, including logical ones. But, since the security aspects of OCII largely depend on the way in which the function objects are linked together, the OCII security architecture is based on physical network elements (PNE) OCIIs that contain one or more functional objects. The way of binding of these objects and their join in elements of network architecture is defined by administration of OCII.
A single network security trust model is shown in Figure 3.

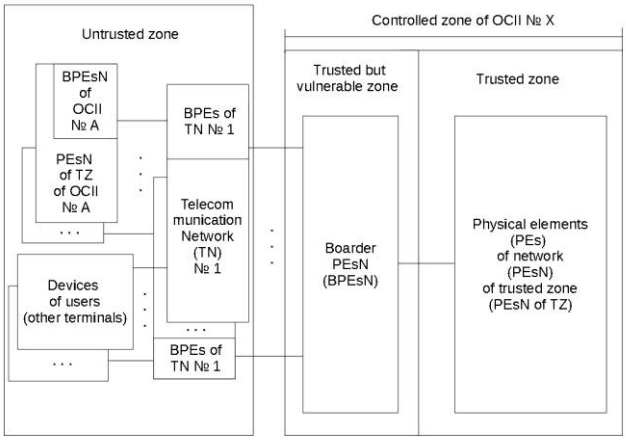

Fig. 3: A single network security trust model of OCII

Each OCII has three security zones:
- trusted zone;
- trusted but vulnerable zone;
- untrusted zone.

The trusted zone is the security domain in which the PNEs OCII is located, which never directly connects to PNEs that are outside the OCII controlled zone. The general characteristics of the PNEs OCII in this domain are that they are completely controlled by the OCII administration, which guarantees physical security, and they are associated only with the PNEs in the trusted zone and with the boarder PNEs in the trusted but vulnerable zone.
The trusted but vulnerable zone is the zone where boarder PNEs OCII resides, which are associated with PNEs in the trusted zone and with PNEs in the untrusted zone. The latter makes them vulnerable from the outside. The main security function is to protect PNEs OCII from attacks initiated in an untrusted zone, in which conditions it is necessary to preserve the stable operation of PNEs OCII is ensured.
The untrusted is the zone that includes all network elements of telecommunication networks and devices of users and other terminals outside the OCII (its domain) are connected, which connected to the boarder PNEs OCII.

5. Basic provisions for a single system of classification of protection of elements of critical information infrastructure

5.1. Protection class

The ECII protection class will be defined as a particular set of requirements to ECII on ensuring the information security of the information processed (stored, transmitted) by it, taking into account the importance of ECII.

5.2. Levels of confidentiality of information critical information infrastructure

On confidentiality degree information of CII is divided into five levels:
• open information, free of data of limited access and distribution (sign of level –" 5");
• the information containing data of level is not higher "Confidentially" (sign of level –"4");
• the information containing the data which are the state secret with a signature stamp not above is "Secret" (sign of level –"3");
• the information containing the data which are the state secret with a signature stamp not above is "Top Secret" (sign of level – "2");
• the information containing the data which are the state secret with a signature stamp to "higher top secret" inclusively (sign of level – "1").
The levels of confidentiality are reflected in Table 1.

Table 1: Levels of confidentiality of information of CII

Highest degree of confidentiality	Designation	Sign of level
Higher Top Secret	HTS	1
Top Secret	TS	2
Secret	S	3
Confidential	CI	4
Unclassified	UC	5

5.3. Information access modes

In CII the modes of full or limited access to OCII can be applied:
• in case of the mode of full access to all users having right of access to this OCII equal access rights to all information of OCII are granted (sign of the mode – "*E*");
• in case of application on the OCII mode of limited access information is differentiated. In this case the users having right of access to this OCII are granted different access rights to information of OCII according to special permissions (sign of the mode – "*D*").

5.4. Categories of the importance of elements of critical information infrastructure

According to national standards and techniques of determination of importance to each ECII should be assigned a category (level, etc.) of its importance. This category in the system of classification of security is used as sign of "iCat". Here i=1,2,…, n, where n – total number of categories of importance of ECII.
When processing (storing, transferring) in ECII in an open form of information with the stamp of secrecy, it establishes the first level of importance of ECCI regardless of other criteria of importance. This is due to the highest importance of information containing state secrets. The sign of the importance category "1Cat" in the designation of the class of such ECII is pointless, since it is always automatically implied.

5.5. Contours of elements of critical infrastructure

In many cases on each ECII simultaneously processes both open and restricted information (at least official or personal data) with different access modes. Its processing, depending on the ECII architecture, can be performed within the framework of a single or several isolated contours (zones, segments, levels, subsystems, etc.).
The contours can be autonomous or interact with other contours of their ECII. Through the contours, having an exit in a cyberspace, ECII interacts with other ECCI and other subjects of access to the processed (provided) information of this ECII.

The interaction of contours both within the ECII and with the contours of other ECII must obey certain rules permitting or prohibiting each contour a bi-directional or unidirectional interaction with the internal contours of ECII and / or external contours of subjects of access to this ECII, and also providing the possibility of establishing for contours complete ban on their internal and / or external interaction.

5.6. Assignment of protection classes for multiconturs elements of critical information infrastructure

The above-mentioned feature of ECII defines the principle of OCII separation into many isolated contours that are individual objects of protection. For each contour, a protection class should be established and security measures developed. The degenerate case of the ECII architecture is ECII, which contains only one contour.

6. A single system of classification of protection of elements of critical information infrastructure

On the basis of the described main conditions the following key attributes of classification of protection of ECII are accepted:
• levels of confidentiality of the information being processed (stored, transmitted) ECII,
• categories of importance (Cat) ECII;
• access modes of users to the ECI
The protection class (Pr*Cl*) of a particular ECII № X will be determined by the index of criteria vector:

$$\Pr Cl(X) = \left[jC(X);\quad I;\quad A;\quad iCat(X) \right], \text{ where} \qquad (6)$$

j – value of sign of level of confidentiality of information;
i – value of sign of category of importance ECII № X.
An example of an ECII protection class system is shown in Table 2.

Table 2: Example a single system of classification of protection of ECII

Requirements on ECII	Protection classes of ECII								
	5E1Cat *5E2Cat* ... *5EqCat*	*4E1Cat* *4E2Cat* ... *4EzCat*	*4D1Cat* *4D2Cat* ... *4DwCat*	*3E*	*3D*	*2E*	*2D*	*1E*	*1D*
confidentiality	-	*CI*	*CI*	*S*	*S*	*TS*	*TS*	*HTS*	*HTS*
integrity	+	+	+	+	+	+	+	+	+
availability	+	+	+	+	+	+	+	+	+
importance	+	+	+	+	+	+	+	+	+

Note: The index *n* has designated the total number of categories of importance of ECII, the signs "+" – if requirement is imposed, "-" – if requirement isn't imposed.

7. Conclusion

The unified security trust model of the of elements of the CII provides a unification of the approaches to the organization of the safe functioning of the ECII, interacting with open cyberspace. The unified system of ECII protection classes, in contrast to the known classification systems, additionally takes into account the criteria for the importance of ECIIs. This of class system is applicable for the classification of single- and multicontour ECIIs. The joint application of the developed model of trust and the system of classification of ECIIs protection provide a high level of systemic character in the development of ECII security measures against attacks, as well as in the organization of ECII interaction between themselves and users.

References

[1] International standard ISO/IEC 27000:2018, “Information security management systems - Overview and vocabulary”, Geneva: ISO, 2018, 19 p.
[2] International standard ISO/IEC 27001:2013, “Information security management systems — Requirements”, Geneva: ISO, 2014, 48 p.
[3] International standard ISO/IEC 13335-1:2004, “Management of information and communications technology security - Part 1: Concepts and models for information and communications technology security management”, Geneva: ISO, 2004, 28 p.
[4] ITU-T Recommendation Y.2701, “Security requirements for NGN release 1”, Geneva: ITU-T, 2008, 44 p.
[5] ITU-T Recommendation X.805, “Security architecture for systems providing end-to-end communications”, Geneva: ITU-T, 2008, 28 p.
[6] Igor F. Mikhalevich, “Problems of creation of the entrusted environment of functioning of automated control systems in the protected execution”, Works XII of the All-Russian meeting on control problems (ARMCP-2014, Moscow), Moscow: ICS of RAC, 2014, pp. 9201-9207.