Method for Calculating the Criticality Level of Sectoral Information and Telecommunication Systems

Sergiy Gnatyuk [1], Viktoriia Sydorenko [1], Oleksii Yudin [2], Oksana Zhyharevych [3] and Artem Polozhentsev [1]

[1] *National Aviation University, 1, Liubomyr Huzar Ave. Kyiv, 03058, Ukraine*
[2] *State Scientific and Research Institute of Cybersecurity Technologies and Information Protection Kyiv, Ukraine*
[3] *Lutsk National Technical University, 75 Lvivska Str., Lutsk, 43000, Ukraine*

Abstract

Global trends to increase the number and complexity of cyber-attacks have led to the actualization of the issue of protection of information and telecommunication systems (ITS), in particular, sectoral, critical to the functioning of society, socio-economic development of the state, and ensure the information component of national security. Considering the need for national security and the need to introduce a systemic approach to solving the problem of critical infrastructure protection at the national level, creating a security system is one of the priorities in reforming Ukraine's defense and security sector. Thus, there is a need to develop methods and models for the ITS categorization as a critical information infrastructure to ensure the national security of Ukraine. The study presents the method for calculating the criticality level of the sectoral ITS, which, due to the use of a structural-logical and functional model for determining the functional profile of the sectoral ITS security, as well as a functional model for calculating the quantitative criterion for assessing the security of ITS, allow to increase the accuracy of the decision to categorize ITS as critical. Using the developed method makes it possible to classify ITS as critical, considering information properties (such as confidentiality, integrity, availability, and observability). In addition, an experimental study of the proposed method was carried out on the example of the ITS of the National Confidential Communication System (NCCS), which was used to check the adequacy of the method's response to changes in input data. The usage of the method allows to calculate the criticality ranks for functional disruption of the components, subsystems, and systems of the NCCS. Method also helps to calculate the quantitative indicator of the severity of the consequences of the functionality disruption of the NCCS, as well as the quantitative indicator of the ranks of criticality of the NCCS and a conclusion was made regarding the NCCS criticality.

Keywords

Information and telecommunication systems (ITS); critical infrastructure; critical infrastructure object; criticality; criticality rank; functional security profile.

1. Introduction

Global trends to increase the number and complexity of cyber-attacks have led to the actualization of the protection of information and telecommunication systems (ITS) sectoral, which is critical to the functioning of society, and socio-economic development of the state and ensure the information component of national security. Considering the need for national security and the need to introduce a systemic approach to solving the problem of critical infrastructure protection at the national level, creating a security system is one of the priorities in reforming Ukraine's defense and security sector [1].

Information Technology and Implementation (IT&I-2022), November 30 – December 02, 2022, Kyiv, Ukraine
EMAIL: s.gnatyuk@nau.edu.ua (S. Gnatyuk); v.sydorenko@ukr.net (V. Sydorenko); alex@ukrdeftech.com.ua (O. Yudin); o.zhyharevych@gmai.com (O.Zhyharevych); artem.polozhencev@gmail.com (A. Polozhentsev);
ORCID: 0000-0003-4992-0564 (S. Gnatyuk); 0000-0002-5910-0837 (V. Sydorenko); 0000-0002-4730-1463 (O. Yudin); 0000-0002-1979-4168 (O. Zhyharevych); 0000-0003-0139-0752 (A. Polozhentsev)

It should be noted that the Law of Ukraine "On the Fundamentals of Cybersecurity of Ukraine" [2] determines the need to form a list of critical infrastructure facilities and the need to develop a procedure for attributing facilities to that list. Resolution No. 1109 of the Cabinet of Ministers of Ukraine on certain critical infrastructure issues approves the procedure for classifying facilities as critical infrastructure; the list of sectors (subsectors) and essential services of the state's critical infrastructure; and the methodology for categorizing critical infrastructure facilities [3]. The mentioned methodology describes the mechanism of assigning critical infrastructure to a certain category of criticality, which is determined based on the analysis of the level of possible negative impact. In addition, the Law of Ukraine "On Critical Infrastructure" has recently come into force. [4], which describes in detail the legal and organizational basis for protecting critical infrastructure facilities in the creation and operation of the national critical infrastructure protection system. However, the issue of assessing the effectiveness of critical infrastructure protection of sectoral ITS remains open. At the same time, it is possible to evaluate the effectiveness of protection using risk assessment mechanisms. Thus, the point of protection is an inverse function of the risk assessment indicator.

2. Analysis of modern approaches and problem statement

Methods of risk assessment are classified according to the stages of the risk assessment process in which they have applied [5]: methods of risk identification; methods of risk analysis (consequences analysis); methods of risk analysis (qualitative, semi-quantitative, or quantitative probability assessment); methods of risk analysis (performance evaluation of existing management measures); methods of risk analysis (quantitative assessment of risk level); methods of risk assessment.

The ability to apply the methodology for each stage of the risk assessment process is characterized by the following levels: the method is recommended for usage, or it can be applied (Table 1), where "Rec" means recommended for use, "Can" means can be used, and "Not" is not possible to use.

Table 1

The ability to apply the methodology for each stage of the risk assessment process

Approaches and methods	The risk assessment process				
	Risk identification	Risk analysis			Risk assessment
		Consequences	Probability	Level	
Hazard and operability study (HAZOP)	Rec	Rec	Can	Can	Can
Analysis of the scenario	Rec	Rec	Can	Can	Can
Analysis of the impact on activity	Can	Rec	Can	Can	Can
Analysis of the original cause	Not	Rec	Rec	Rec	Rec
Fault tree analysis	Can	Not	Rec	Can	Can
Cause and effect analysis	Can	Rec	Rec	Can	Can
Decision tree analysis	Not	Rec	Rec	Can	Can
"Bow-tie" analysis	Not	Can	Rec	Rec	Can
Analysis of operator reliability	Rec	Rec	Rec	Rec	Can
FN curves	Can	Rec	Rec	Can	Rec
Risk indicators	Can	Rec	Rec	Can	Rec
Cost-benefit analysis	Can	Rec	Can	Can	Can
Multiple-criteria decision analysis	Can	Rec	Can	Rec	Can
Matrix of consequences and probability	Rec	Rec	Rec	Rec	Can
Environmental risk assessment (toxicity assessment)	Rec	Rec	Rec	Rec	Rec
SWIFT	Rec	Rec	Rec	Rec	Rec
FMECA	Rec	Rec	Rec	Rec	Rec
Reliability-centered maintenance (RCM)	Rec	Rec	Rec	Rec	Rec

According to the data presented in Table 1, only the last four techniques are fully recommended to be used. The factors affecting the choice of methods of risk assessment are the following: the complexity of the problem and the methods required for its analysis; the type and level of uncertainty of the risk assessment (based on the amount of information available, etc., which is necessary to achieve the goal); the number of resources required in the ratio of time and skill level, data needs or costs; the possibility of obtaining quantitative input data.

The most appropriate methods in terms of the possibility of obtaining quantitative indicators and the level of uncertainty, as well as complexity, are methods of functional analysis. Let's consider the following methods. ***Failure mode and effects analysis (FMECA)*** [6] is a methodology used to determine how functional failures of components or systems occur. In this case, criticality indicators are usually qualitative or semi-quantitative. At the same time, if actual failure rate data are used, the indicators can be expressed quantitatively.

The FMECA method can be used to determine the types and results of human errors; provide a process for scheduling testing and maintenance of systems; obtain qualitative or quantitative information for analysis techniques, such as fault tree analysis. Disadvantages of the method include application to identify individual types of failures, but not their combinations; studies can be time consuming; application for complex systems can be difficult and time-consuming.

Reliability-centered maintenance (RCM) [7] is a method of determining the policies that need to be implemented to manage failures in a way that effectively ensures the necessary safety, availability, and operation of all types of equipment.

The RCM method is based on risk assessment, as the method implements the basic steps of such an assessment. The type of risk assessment is a failure type, consequence, and criticality analysis (FMECA). Risk identification is aimed more at situations in which hypothetical failures can be resolved or their frequency and consequences can be reduced by performing maintenance tasks. Risk identification is performed by identifying functions and standards of performance as well as equipment and component failures that may violate specified functions. Risk analysis consists of quantifying the frequency of each failure without maintenance. Consequences are established by determining the impact of failure. A risk matrix combines the frequency of failure and the consequences and allows the establishment of risk levels. It is assessed by selecting the appropriate failure management policy for each type of failure.

The RCM method has the same drawbacks as the FMECA.

The method for calculating the criticality level of critical information infrastructure facilities, based on the FMECA method, which is different by using a three-dimensional criticality matrix, Pareto diagram, Ishikawa causal diagram, and calculation of additional criticality weighting factors makes it possible to assess the level of critical infrastructure facilities criticality. [8-11]. The disadvantage of this method is the lack of consideration of such properties of information as confidentiality, integrity, availability, and observability [12].

The method of risk-based criticality analysis proposed by M. Theocharidou is based on risk analysis. The method can apply it to the calculation of quantitative indicators of the ITS security level of an individual institution. This method does not apply to a state because it operates with the concept of criticality to the organization [13-14]. This method's disadvantages are inherent to determining the criticality level of critical information infrastructure facilities.

The analyzed methods are used to determine the criticality of risk assessment frameworks. A comparison of methods is given in Table 2 according to the following criteria: the number of citizens involved (health and social consequences), economic effect, political consequences, the mutual dependence of critical infrastructure sectors (the result of the destruction of one is the destruction of others), the impact on the environment, the scale by territory, duration.

The conducted analysis of the approaches that can be used to assess the effectiveness of the ITS protection showed that such an assessment is proposed through an evaluation of risks (the lower the risk, the greater the effectiveness of protection). At the same time, the normative document of the system of technical security of information of Ukraine [15] defines the result of evaluation as a rating, representing an ordered series of alphanumeric combinations, denoting the levels of implemented services combined with the level of guarantees. Thus, there is a contradiction between the approaches to assessing the effectiveness of protection. In addition, the recommended methods, which analyze the consequences, probability of occurrence and level of risk, do not identify failures by the characteristics of information, such as confidentiality, integrity, availability, and observability.

Table 2
Comparison of methods for calculating the ITS criticality

Method	Analysis							
	Risk identification	Effects	Probability	Risk level	Failure identification (By properties of information)	Failure type identification	Quantitative indicators	Criticality analysis
FMECA	+	+	+	+	-	+	+	-
RCM	+	+	+	+	-	+	+	-
The method for calculating the criticality level of critical information infrastructure facilities	+	+	+	+	-	+	+	+
The method of risk-based criticality analysis	+	+	+	+	-	+	+	+

Based on the identified contradictions in the assessment of the effectiveness of the ITS protection, there is a need to develop a new method for calculating the criticality level and criteria for attributing the sectoral ITS to the critical infrastructure. Therefore, this study aims to develop and experimentally investigate a method for calculating the criticality level of the sectoral ITS, based on the fundamental properties of information.

3. The method of calculating the criticality level of the sectoral ITS

The method of calculating the criticality level of the sectoral ITS, rather than the above-mentioned methods [8-11; 13-14], is based on the usage of such properties of information as confidentiality, integrity, availability, observability, and considers the quantitative indicators of the criteria for referring to critical infrastructure [3; 12; 16]. The developed method can be represented as a flowchart (Fig. 1). It uses the results of the structural-logical model of formation of the functional profile of the sectoral ITS security level, the structural-functional method of forming the functional security profile of the sectoral ITS, as well as the model for calculating the quantitative criteria for assessing the security level of the ITS. The method consists of seven steps, each described in detail below.

1. Definition of the ITS subsystems and components

The following steps should be done to identify the ITS subsystems and their components: 1) decompose the infrastructure into general and the most critical infrastructure domains; 2) decompose the critical domains into objects; 3) generate a general list of the ITS; 4) perform decomposition of the ITS into subsystems and components. The first three steps are described in [1] and will be the input data for the criticality calculation method. Most in common, all the elements described in [1] must have cybersecurity functions (confidentiality, integrity, availability, observability, authenticity, nonrepudiation, and trustworthiness of information). These functions may be not basic (e.g., integrity or availability of information in PLC (Programmable Logic Controller) or optical amplifiers) or basic (anti-virus protection, firewall, security alarm system, means of protection against side electromagnetic emissions and pickups, means of cryptographic protection of information, means of authentication).

It also should be noted that the list of elements of the ITS of energy infrastructure management includes both means and systems. Therefore, it is advisable to divide the aspects of cyber protection of the ITS systems of energy infrastructure management, having a set of protection means, and having a complete system of information protection [17]. According to the normative documents [18], a complete information protection system is a set of organizational and engineering measures, software, and hardware, providing information protection in the ITS. Complex protection means a collection of software and hardware, ensuring the implementation of an information security policy. In addition, it

should be noted that any component of the ITS, which because of any impact can lead to a violation of security policy, should be considered as part of a set of security features [17].

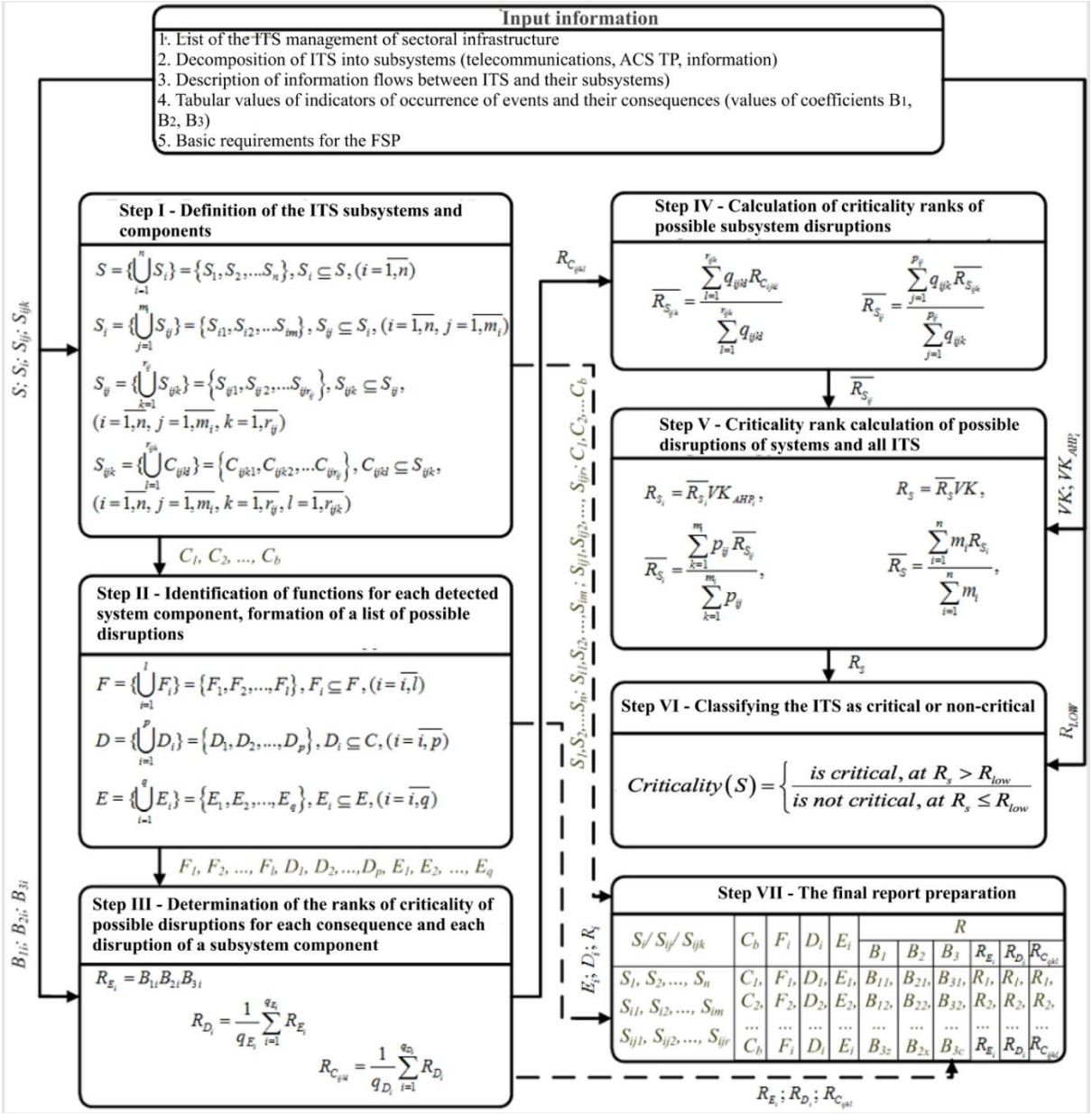

Figure 1. Flowchart of the implementation of the method for calculating the criticality level of the sectoral ITS

Based on the above, the elements that ensure cyber security of the ITS of the energy infrastructure management systems should include the following: aspects of the telecommunications subsystem, automated control systems of technological processes of energy infrastructure management and information subsystems. In addition, the security requirements will be defined separately to a set of protection tools and a comprehensive system of information protection, depending on the object of study. Let's describe the ITS elements in the form of multiple sets.

The structure of the ITS of critical infrastructure facilities should be as follows (S):

$$S = \{\bigcup_{i=1}^{n} S_i\} = \{S_1, S_2, ...S_n\}, S_i \subseteq S, (i = \overline{1,n}), \quad (1)$$

where S_i is a class of systems, for example, the ITS of local production control, the ITS of supervisory control and data collection, and n is the total number of classes of systems.

A set of systems included in the ITS (S_i):

$$S_i = \{\bigcup_{j=1}^{m_i} S_{ij}\} = \{S_{i1}, S_{i2}, ...S_{im}\}, S_{ij} \subseteq S_i, (i = \overline{1,n},\ j = \overline{1,m_i}), \quad (2)$$

where S_{ij} are the systems of the i-th class, m_i is the number of systems of the i-th class, for example, an automated process control system that manages the production of components, the ITS of supervisory control and data acquisition, and n is the total number of system classes.

A set of subsystems for each of the ITS systems (S_{ij}):

$$S_{ij} = \{\bigcup_{k=1}^{r_{ij}} S_{ijk}\} = \{S_{ij1}, S_{ij2}, ...S_{ijr_{ij}}\}, S_{ijk} \subseteq S_{ij}, (i = \overline{1,n},\ j = \overline{1,m_i}, k = \overline{1,r_{ij}}), \quad (3)$$

where S_{ijk} – subsystems of S_{ij} systems, r_{ij} – the number of ij-th class subsystems, for example, measuring and control devices and automation, devices which collect data from several sources and change/transform it into other form factors of the ITS local production control system.

A set of components for each subsystem of the ITS system (S_{ijk}):

$$S_{ijk} = \{\bigcup_{l=1}^{r_{ijk}} C_{ijkl}\} = \{C_{ijk1}, C_{ijk2}, ...C_{ijr_{ij}}\}, C_{ijkl} \subseteq S_{ijk}, (i = \overline{1,n},\ j = \overline{1,m_i}, k = \overline{1,r_{ij}}, l = \overline{1,r_{ijk}}), \quad (4)$$

where C_{ijkl} is components of the S_{ijk} subsystems, r_{ijk} is the number of members of the ijk-th class, e.g., dampers, cutoff valves, electric latches, pressure, temperature, level sensors, gas analyzers, pumps, vacuum extractors.

2. Identification of functions for each detected system component, formation of a list of possible disruptions of each system component, assessment of the consequences of each of the potential violations

In addition to the main functions of the system components, it is necessary to consider the information security requirements for the categories of logical interfaces of domain objects. For this purpose, it is proposed to use the following designations of security requirements [19-21]:

- SG.AC-12 – Blocking a session.
- SG.AC-13 – Remote session termination.
- SG.AC-14 – Allowed unauthenticated and unidentified actions.
- SG.AC-15 – Remote Access.
- SG.IA-04 – User identification and authentication.
- SG.IA-05 – Device identification and authentication.
- SG.IA-06 – Message Authentication.
- SG.SC-03 – Secure function isolation.
- SG.SC-05 – DoS protection.
- SG.SC-06 – Resource prioritization.
- SG.SC-07 – Memory protection.
- SG.SC-08 – Message Integrity (communication line).
- SG.SC-09 – Confidentiality of messages (communication line).
- SG.SC-26 – Confidentiality of information in storage.
- SG.SI-07 – Integrity of software and information.

The function of each detected system component (F):

$$F = \{\bigcup_{i=1}^{l} F_i\} = \{F_1, F_2, ..., F_l\}, F_i \subseteq F, (i = \overline{i,l}), \quad (5)$$

where F_i is the functions of the C_{ijkl} component of the S_{ijk} subsystem, and l is the total number of functions of the component, for example: receiving the signal, converting the signal, and performing a specific action. List of possible disruptions of each component of the system (D):

$$D = \{\bigcup_{i=1}^{p} D_i\} = \{D_1, D_2, ..., D_p\}, D_i \subseteq C, (i = \overline{i,p}), \quad (6)$$

where D_i is a disruption of the C_{ijkl} component of the S_{ijk} subsystems, p is the total number of possible disruptions. At the same time, disruption is a violation of confidentiality, integrity, availability, or observability, which can lead to negative consequences.

Consequences of each of the possible disruptions (E):

$$E = \{\bigcup_{i=1}^{q} E_i\} = \{E_1, E_2, ..., E_q\}, E_i \subseteq E, (i = \overline{i,q}), \quad (7)$$

where E_i is the consequences of disruption of the C_{ijkl} component of the S_{ijk} subsystems, q is the total number of consequences. In this case, the consequences are DoS, disclosure of confidential data, and incorrect operation of devices.

3. Determination of the ranks of the criticality of possible disruptions for each consequence and each disruption of a subsystem component

In the third step, the criticality ranks of potential disruptions (R) are determined for each its consequence (Ei) and each disruption (Di) of the C_{ijkl} component of the S_{ijk} subsystems. In the criticality rank determination, tabular values of the indicators should be used [6].

The following formula R_{E_i} calculates the criticality ranks of the disruption of the C_{ijkl} component:

$$R_{E_i} = B_{1i} B_{2i} B_{3i}, \quad (8)$$

where B_{1i} is a tabular value of the indicator, which determines the intensity of the disruption occurrence, B_{2i} is a tabular value of the indicator, which determines the detecting possibility of disruption, B_{3i} is a tabular value of the indicator, which determines the consequences of the occurrence of disruption.

The criticality ranks of the D_i component disruption are calculated by the following formula (R_{D_i}):

$$R_{D_i} = \frac{1}{q_{E_i}} \sum_{i=1}^{q_{E_i}} R_{E_i}, \quad (9)$$

where R_{E_i} is a criticality rank, the value of which corresponds to each of the $E_i, (i = \overline{1, q_{E_i}})$, q_{E_i} is the number of consequences for each disruption.

The criticality ranks of the D_i disruption of the C_{ijkl} component are calculated by the following formula:

$$R_{C_{ijkl}} = \frac{1}{q_{D_i}} \sum_{i=1}^{q_{D_i}} R_{D_i}, \quad (10)$$

where R_{D_i} criticality rank, the value of which corresponds to each of the $D_i, (i = \overline{1, q_{D_i}})$, q_{D_i} is the number of disruptions for each component.

4. Calculation of criticality ranks of possible subsystem disruptions

In the fourth step, the criticality ranks of possible disruptions of the S_{ijk} and S_{ij} subsystems are determined. The arithmetic weighted average rank ($\overline{R_{S_{ijk}}}$), of the S_{ijk} subsystem is as follows:

$$\overline{R_{S_{ijk}}} = \frac{\sum_{l=1}^{r_{ijk}} q_{ijkl} R_{C_{ijkl}}}{\sum_{l=1}^{r_{ijk}} q_{ijkl}}, \quad (11)$$

where $R_{C_{ijkl}}$ is the criticality rank, the value of which corresponds to each of the $C_{ijkl}, (l = \overline{1, r_{ijk}})$, q_{ijkl} is the number of disruptions for each subsystem component.

The arithmetic weighted average rank of the ($\overline{R_{S_{ij}}}$) disruption of the S_{ij} system is as follows:

$$\overline{R_{S_{ij}}} = \frac{\sum_{j=1}^{p_{ij}} q_{ijk} \overline{R_{S_{ijk}}}}{\sum_{j=1}^{p_{ij}} q_{ijk}}, \quad (12)$$

where $\overline{R_{S_{ijk}}}$ is the criticality rank, the value of which corresponds to each $S_{ijk}, (j = \overline{1, p_{ij}})$, q_{ijk} is the number of disruptions for each system.

5. Criticality rank calculation of possible disruptions of systems and all ITS

In the fifth step, the criticality rank of possible disruptions of the S_i (R_{S_i}) systems and all ITS S (R_s) should be calculated as follows:

$$R_{S_i} = \overline{R_{S_i}} VK_{AHP_i}, \tag{13}$$

where VK_{AHP_i} is the ratio of the given FSP to the ratio suggested by the expert in the area for the S_i system (1), and the $\overline{R_{S_i}}$ is the arithmetic weighted average of the violation rank for the S_i system, VK_{AHP_i} is the result of calculation based on the method of hierarchy analysis, using a model for calculating the quantitative criterion for assessing the security of the ITS.

$$\overline{R_{S_i}} = \frac{\sum_{k=1}^{m_i} p_{ij} \overline{R_{S_{ij}}}}{\sum_{k=1}^{m_i} p_{ij}}, \tag{14}$$

where $\overline{R_{S_{ij}}}$ is the criticality rank the value of which corresponds to each $S_{ij}, (k = \overline{1, m_i})$, p_{ij} is the number of disruptions for each S_{ij} system.

The criticality rank of the *S* (R_S) ITS is calculated by the following formula:

$$R_S = \overline{R_S} VK, \tag{15}$$

where *VK* is a ratio that describes the severity of the consequences of the ITS disruption, $\overline{R_S}$ is an arithmetic weighted average of the disruption rank for the *S* object.

The arithmetic average weighted rank of the object *S* disruption is calculated by the following formula:

$$\overline{R_S} = \frac{\sum_{i=1}^{n} m_i R_{S_i}}{\sum_{i=1}^{n} m_i}, \tag{16}$$

where $\overline{R_{S_i}}$ is the criticality rank, the value of which corresponds to each $S_i, (i = \overline{1, n})$, m_i is the number of disruptions for each system.

The following formula describes the ratio of the severity of the consequences of the disruptions:

$$VK = \frac{1}{n} \sum_{j=1}^{m_i} \sum_{i=1}^{n} \frac{VK_{ij}}{VK_{ij}^{\max}}, \tag{17}$$

where VK_{ij}^{max} is the maximum value of the ratio of the *i*-th criteria, which is calculated as the product of the priority and the highest value of the criteria and varies from 70 to 10 (table value), *n* is the number of criteria, VK_{ij} is the product of the value of the *i*-th and *j*-th criteria.

6. Classifying the ITS as critical or non-critical

In the sixth step, the ITS (*S*) should be classified as critical or non-critical:

$$Criticality(S) = \begin{cases} is\ critical, at\ R_s > R_{low} \\ is\ not\ critical, at\ R_s \le R_{low} \end{cases},$$

where R_{low} is the limit value of the criticality rank (equal to 625.0). R_{low} is the product of the average value of *VK* (5.0), VK_{AHP} (1.0), and $\overline{R_S}$ (125.0).

7. The final report preparation

In the seventh step, the values obtained in steps I-III should be recorded in the report:

- a list of systems, subsystems, and their components.
- a list of the functions of the components, their possible disruptions, and probable consequences.
- the value of indicators determining the intensity of the occurrence of disruptions.
- the value of indicators determining the possibility of detecting a disruption.
- the value of indicators determining the consequences of the occurrence of disruptions.
- the value of criticality ranks of the consequences of the component function disruption.
- the value of the ranks of the criticality of the consequences of the component's function disruptions.
- the value of the ranks of the criticality of the component's performance disruption.
- the value of ranks of the criticality of possible disruptions of the component subsystem.

The summarized information is presented in the following form (Table 3):

Table 3

The summarized information of the system elements

S_i /S_{ij} /S_{ijk}	C_b	F_i	D_i	E_i	B_1	B_2	B_3	R R_{Ei}	R_{Di}	R_{Cijkl}
$S_1, S_2, ..., S_n$	C_1	F_1	D_1	E_1	B_{11}	B_{21}	B_{31}	R_1	R_1	R_1
.....	...	...	...	...	...	...	...	...	...	...
$S_{ij1}, S_{ij2}, ..., S_{ijr}$	C_b	F_i	D_i	E_i	B_{1z}	B_{2x}	B_{3c}	R_{Ei}	R_{Di}	R_{Cijkl}

4. Experimental verification of the method for calculating the criticality level of the sectoral ITS

Based on the proposed in [1] structural-functional method of determining the FSP of the sectoral ITS was obtained a basic (FSP_B) and adjusted by the expert (FSP_E) of the NCCS:

- FSP_B: CA-2, CE-3, CT-2, CO-1, IA-2, IE-2, IT-1, IR-2, AF-2, AQ-2, AD-2, AR-2, OS-1, OI-2, OC-1, OD-3, OP-2, OT-2, ON-2, OE-2, OR-1.
- FSP_E: CA-3, CE-4, CT-3, CO-1, CC-2, IA-4, IE-2, IT-1, IR-2, AQ-2, AD-3, AR-3, OS-1, OI-2, OC-1, OD-3, OP-3, OT-3, ON-5, OE-2, OR-1.

FSP_E is a criterion for assessing the security level of information in circulation in the NCCS.

The method for calculating the quantitative criteria for assessing the security of the NCCS, by using the hierarchy analysis method resulted in the value of $VK_{AHP} = 0,717$. The result of calculation of the VK_{AHP} is shown in Fig. 2. In addition, the decomposition of the NCCS into components of sets of systems and their subsystems was performed in (Table 1 in [1]), and the components that each subsystem consists of were also determined. A fragment of decomposition is presented in Table 4.

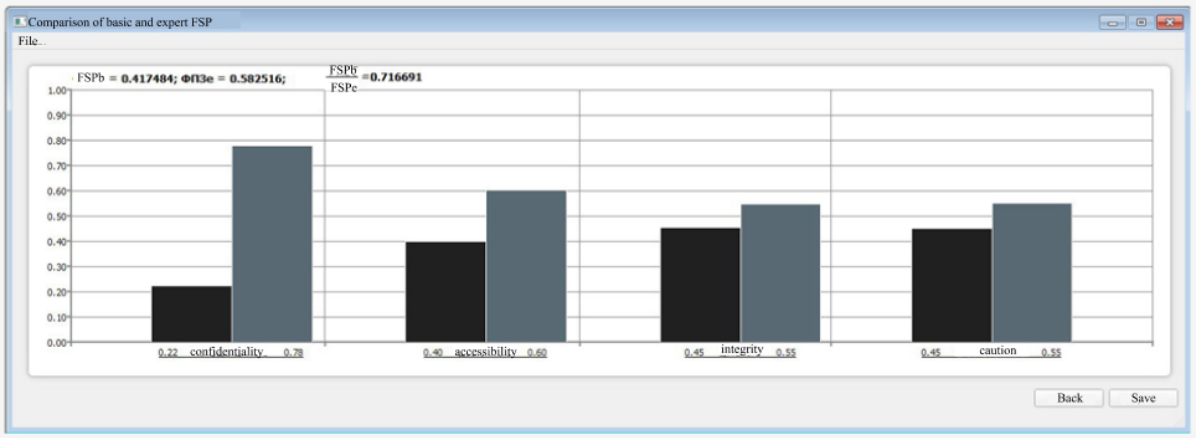

Figure 2. Result of the ratio of alternatives

Table 4

The decomposition of the NCCS

Level	Number of elements	Designation of the system/subsystem/component
1	4	S_t, S_s, S_d, S_m
2	10	S_{t1}, S_{t2}, S_{t3}, S_{s1}, S_{s2}, S_{d1}, S_{d2}, S_{d3}, S_{m1}, S_{m2}
3	34	S_{t11}, S_{t12}, S_{t13}, ..., S_{m23}, S_{m24}
4	115	C_{t111}, C_{t112}, C_{t113}, ..., C_{m231}, C_{m241}

For each component of the subsystem a list of functions F_i, possible disruptions of functioning D_i, consequences E_i and ranks of criticality of consequences R_{Ei} is defined. A fragment of the list is shown in Table 5. The calculation of criticality ranks R_{D_i} of the D_i component of the C_{ijkl} subsystems, criticality ranks of possible disruptions $R_{C_{ijkl}}$ of the C_{ijkl} component, criticality ranks of possible

disruptions $\overline{R_{S_{ijk}}}$ and $\overline{R_{S_{ij}}}$ of the S_{ijk} and S_{ij} subsystems, criticality ranks of possible disruptions R_{S_i} of the S_i systems and the overall of the NCCS (*S*) was carried out, by applying the method for calculating the criticality level of the sectoral ITS [22-23]. A fragment of the list is shown in Table 6

Table 5
List of functions, possible damages, consequences and criticality ranks

Ci	*Cijkl*	*FSP*	*Fi*	*Di*		*Ei*		*Rei*	*B1i*	*B2i*	*B3i*
C_{t111}	A telephone	AQ-1, AR-1, OT-2	F_{t1111} Electric signal generation	D_{t11111}	Lack of power supply	$E_{t111111}$	Lack of connectivity	1	1,0	1,0	1,0
						$E_{t111112}$	Inability to log work	5	1,0	5,0	1,0
			F_{t1112} Network packet analysis and formation (ARP, Ethernet, IP…)	D_{t11121}	Damaged hardware	$E_{t111211}$	Lack of connectivity	1	1,0	1,0	1,0
				D_{t11123}	Incorrect settings	$E_{t111231}$	Lack of connectivity	2	2,0	1,0	1,0

Table 6
Calculation of criticality ranks

Sijk	*Ci*	*Fi*	*Di*	*Ei*	*Rei*	*Rdijk*	*Rcij*	*Rsijk*	*Rsij*	*Rsi*	*Rs*
S_{t11}	C_{t111}	F_{t1111}	D_{t11111}	$E_{t111111}$	1	3,00	1,87	6,34	13,00	29,95	51,40
				$E_{t111112}$	5						
			D_{t11112}	$E_{t111121}$	1	1,00					
			D_{t11113}	$E_{t111131}$	1	2,33					
				$E_{t111132}$	5						
				$E_{t111133}$	1						
		F_{t1112}	D_{t11121}	$E_{t111211}$	1	1,00					
			D_{t11123}	$E_{t111231}$	2	2,00					
	C_{t113}	F_{t1131}	D_{t11311}	$E_{t113111}$	2	2,00	1,75				
				$E_{t113112}$	2						
			D_{t11312}	$E_{t113121}$	2	1,50					
				$E_{t113122}$	1						
…	…	…	…	…	…	…	…	…	…	…	
S_{m24}	C_{m241}	F_{m2411}	D_{m24113}	E_{m24113}	50	2,00	40	40	40	25,78	

Considering the data given in Table 7 and in accordance with (17), the ratio of the severity of the consequences of the disruption of the NCCS is equal to $VK = 0,37$. The arithmetic weighted average of the NCCS disruption rank, calculated from (16), is $\overline{R_S} = 51,40$.

According to the results of the calculation (15) a quantitative index of criticality rank, which is equal to $R_S = 190,7$ and, as a result, it is concluded that the NCCS, at present, is not critical ITS.

5. Conclusions

In this study, the analysis of methods for calculating the criticality level of the ITS has shown that: the assessment of the effectiveness of the ITS security is carried out through an assessment of the risks that do not meet the requirements of the ND TPI; the methods of risk assessment, that analyze the consequences, probability of occurrence and the level of risk, are not performing identification of failures by the properties of information (confidentiality, integrity, availability, and observability); the

main criteria are the number of citizens involved, economic impact, political impact, mutual dependence of critical infrastructure sectors, environmental impact, the scale by territory, the duration. The above criteria must be considered when calculating the criticality level of the sectoral ITS [24-25].

Table 7

The value of indicators of the criteria for classification as critical infrastructure

Criteria \ Value	1	2	3	4	5	6	7	8	9	10
The mutual dependence of critical infrastructure sectors (the consequence of the destruction of one is the destruction of others) (7)		+								
Political impact (6)				+						
Number of citizens involved (health and social consequences) (5)	+									
Environmental impact (4)	+									
Economic impact (3)				+						
Scale by territory (2)										+
Duration (1)				+						

The study also presents an improved method for calculating the criticality level of the sectoral ITS, using the results of the structural-logical model and structural-functional method of the FSP formation of the sectoral ITS, as well as a model of calculation of the quantitative criteria for assessing the security level of the ITS, based on the use of hierarchy analysis. The developed method allows determining the classification of the ITS as critical, considering the properties of information.

In addition, the experimental study of the proposed method was carried out by using the method for calculating the criticality level of the sectoral ITS. The method was used to calculate the ranks of the criticality of the disruption of components, subsystems, and systems of the NCCS, to calculate the quantitative index of the severity of the consequences of disruption of the NCCS, and to calculate the quantitative index of the criticality rank of the NCCS and, based on this, the conclusion about the criticality was made.

6. Acknowledgment

This work is carried out within the framework of research grant №AP06851243 “Methods, models and tools for security events and incidents management for detecting and preventing cyber-attacks on critical infrastructures of digital economics” (2020-2022), funded by the Ministry of Digital Development, Innovation and Aerospace Industry of the Republic of Kazakhstan.

7. References

[1] Gnatyuk S., Yudin O., Sydorenko V., Pozhentsev A., Brzhanov R. “Method of Forming the Functional Security Profile for the Sectoral Information and Telecommunication Systems”, CEUR Workshop Proceedings, 2022, vol. 3179, pp. 272-283.

[2] Ukraine. Laws. “On the main principles of ensuring cyber security of Ukraine”: officer. text: [adopted by the Verkhovna Rada of Ukraine on July 28, 2022].

[3] Ukraine. Resolution No. 1109 (2020) of the Cabinet of Ministers of Ukraine. “Methodology for categorizing critical infrastructure facilities”: officer. text: [adopted by the Cabinet of Ministers of Ukraine on October 9, 2020].

[4] Ukraine. Laws. “About critical infrastructure”: officer. text: [adopted by the Verkhovna Rada of Ukraine on November 16, 2021].

[5] ISO/IEC 31010:2009 – Risk management – Risk assessment techniques, The International Organization for Standardization and The International Electrotechnical Commission, 2009.

[6] IEC 60812, Methods of systems reliability analysis. Methods for analyzing the nature and consequences of failure (FMEA).

[7] IEC 60300-3-11 Reliability Management, Part 3-11: Application Manual, Maintenance to Assure Reliability.

[8] Gnatyuk S., Polishchuk Yu., Sydorenko V., Sotnichenko Yu. “Determining the level of importance for critical information infrastructure objects”, Proceedings of 2019 IEEE International Scientific-Practical Conference: Problems of Infocommunications Science and Technology, PIC S and T 2019, Kyiv, Ukraine, October 8-11, 2019, pp. 829-834.
[9] Gnatyuk S., Yudin O., Sydorenko V., Smirnova T., Polozhentsev A., “The Model for Calculating the Quantitative Criteria for Assessing the Security Level of Information and Telecommunication Systems”, CEUR Workshop Proceedings, 2022, vol. 3156, pp. 390-399.
[10] Sydorenko V., Gnatyuk S., Fesenko A., Yevchenko Y., Tolbatov A., Sotnichenko Y. “Experimental FMECA-based assessing of the critical information infrastructure importance in aviation”, CEUR Workshop Proceedings, Vol. 2732, pp. 136-156, 2020.
[11] Gnatyuk S., Sydorenko V., Polihenko O., Sotnichenko Y., Nechyporuk O. “Studies on the disasters criticality assessment in aviation information infrastructure”, CEUR Workshop Proceedings, 2020, Vol. 2805, pp. 282-296.
[12] S. Gnatyuk, “Critical Aviation Information Systems Cybersecurity”, Meeting Security Challenges Through Data Analytics and Decision Support, NATO Science for Peace and Security Series, D: Information and Communication Security. IOS Press Ebooks, Vol. 47, №3, pp. 308-316, 2016.
[13] G. Stergiopoulos, V. Kouktzoglou, M. Theocharidou, D. Gritzalis, “A process-based dependency risk analysis methodology for Critical Infrastructures”, International Journal of Critical Infrastructures, Vol. 13, №2/7, 2017.
[14] Gritzalis D., Theocharidou M., Stergiopoulos G., “Critical Infrastructure Security and Resilience: Theories, Methods, Tools and Technologies”, Advanced Sciences and Technologies for Security Applications, Springer, 2019, 311 p. ISBN 978-3-030-00023-3.
[15] Normative document of technical information protection 2.5-004-99, Criteria for assessing the security of information in computer systems against unauthorized access, State Service of Special Communications and Information Protection of Ukraine, 1999.
[16] Research and Analysis of Problems of Information Protection at Critical Infrastructure Facilities, cipher “Infrastructure” (doctoral thesis 0114U000038d).
[17] Normative document of technical information protection 1.1-002-99, General provisions on the protection of information in computer systems against unauthorized access, State Service of Special Communications and Information Protection of Ukraine, 1999.
[18] Normative document of technical information protection, Terminology in the field of information protection in computer systems against unauthorized access, State Service of Special Communications and Information Protection of Ukraine, 1999.
[19] National Institute of Standards and Technology Information Report 7628. Guidelines for Smart Grid Cyber Security: Vol. 1, Smart Grid Cyber Security Strategy, Architecture, and High-Level Requirements, National Institute of Standards and Technology, 15 p. 2010.
[20] Y.-C. Liao, “Generating Targeted Attack Scenarios against Availability for Critical Infrastructures,” 2021 14th CMI International Conference - Critical ICT Infrastructures and Platforms (CMI), 2021, pp. 1-7, DOI: 10.1109/CMI53512.2021.9663753.
[21] H. Wang, “Assessing the Effects of Applying Different Simulation Models on Resilience Evaluation of Critical Infrastructure Systems,” 2021 IEEE 3rd International Conference on Frontiers Technology of Information and Computer (ICFTIC), 2021, pp. 169-173, DOI: 10.1109/ICFTIC54370.2021.9647372.
[22] R. Smith, F. Filho, “Improving Critical Infrastructure Resilience in a Rural Coastal Community: A Solar Powered Microgrid,” SoutheastCon 2022, 2022, pp. 436-437.
[23] E. Samanis, J. Gardiner and A. Rashid, “Adaptive Cyber Security for Critical Infrastructure,” 2022 ACM/IEEE 13th International Conference on Cyber-Physical Systems (ICCPS), 2022, pp. 304-305, DOI: 10.1109/ICCPS54341.2022.00043.
[24] Š. Kavan and M. Z. Freitinger Skalická, “Security of critical information infrastructure and possible disruption as a crisis,” 2022 11th Mediterranean Conference on Embedded Computing (MECO), 2022, pp. 1-5, DOI: 10.1109/MECO55406.2022.9797175.
[25] M. Divizinyuk, I. Lutsyk, V. Rak, N. Kasatkina and Y. Franko, “Mathematical Model of Identification of Radar Targets for Security of Objects of Critical Infrastructure,” 2021 11th International Conference on Advanced Computer Information Technologies (ACIT), 2021, pp. 95-100, DOI: 10.1109/ACIT52158.2021.9548374.