Method of Forming the Functional Security Profile for the Sectoral Information and Telecommunication Systems

Sergiy Gnatyuk[a], Oleksiy Yudin[b], Viktoriia Sydorenko[a], Artem Polozhentsev[a] and Rashit Brzhanov[c]

[a] *National Aviation University, 1, Liubomyr Huzar Ave, Kyiv, 03058, Ukraine*
[b] *State Scientific and Research Institute of Cybersecurity Technologies and Information Protection, 3 Maksym Zaliznyak Str., Kyiv, 03142, Ukraine*
[c] *Yessenov University, 13 Microdistrict, Aktau, 130000, Kazakhstan*

Abstract

Global trends of increasing and improving the quality of cyberattacks have led to the actualization of the Information and Telecommunications Systems (ITS) protection, in particular, sectoral, which are critical for the functioning of society, socio-economic development and ensuring the information component of national security. Given the need of national security and the need to implement a systematic approach for solving the issues of critical infrastructure protection, at the national level, the creation of protection systems for such infrastructure is one of the priorities in reforming the defense and security sectors of Ukraine. Thus, there is a need to develop methods and models for classifying the ITS as critical infrastructure to ensure the national security. This article proposes a structural-functional method for determining the functional security profile of the subsystem of the sectoral ITS, which allows to determine the basic functional security profile of the sectoral ITS by determining the sectoral requirements for confidentiality, integrity, availability and observability and more fully formulate criteria for assessing the security of information circulating in critical ITS. The article was followed by an experimental study on the example of ITS of the National System of Confidential Communication, which tested the adequacy of the method's response to changes in input data.

Keywords [1]

Information and telecommunication systems, critical infrastructure, critical infrastructure object, cybersecurity, security assessment, functional security profile.

1. List of abbreviations

Confidentiality: CT – trusting confidentiality; CA – administrative confidentiality; CO – object reuse; CC – hidden channels analysis; CE – confidentiality in the exchange;

Integrity: IT – trust integrity; IA – administrative integrity; IR – recovery; IE – integrity in exchange;

Availability: AR – use of resources; AF – resistance to failures; AQ – quick replacement; AD – disaster recovery;

Observability: ON – registration; OI – identification and authentication; OC – reliable channel; OD – segregation of responsibilities; OP – integrity of the Complex of means of protection; OT – self-testing; OE – identification during exchange; OS – sender authentication; OR – recipient authentication.

2. Introduction

Global trends of increasing and improving the quality of cyberattacks have led to the actualization of the Information and Telecommunications Systems (ITS) protection, in particular, sectoral, which are

Information Technology and Implementation – 2021 (IT&I-2021), December, 2021, Kyiv, Ukraine

EMAIL: s.gnatyuk@nau.edu.ua (S. Gnatyuk); alex@ukrdeftech.com.ua (O. Yudin); v.sydorenko@ukr.net (V. Sydorenko); artem.polozhencev@gmail.com (A. Polozhentsev); r.brzhanov@gmail.com (R. Brzhanov)
ORCID: 0000-0003-4992-0564 (S. Gnatyuk); 0000-0002-4730-1463 (O. Yudin); 0000-0002-5910-0837 (V. Sydorenko); 0000-0003-0139-0752 (A. Polozhentsev), 0000-0001-8755-8207 (R. Brzhanov)

CEUR Workshop Proceedings (CEUR-WS.org)

critical for the functioning of society, socio-economic development and ensuring the information component of national security.

Given the need of national security and the need to implement a systematic approach for solving the issues of critical infrastructure protection, at the national level, the creation of protection systems for such infrastructure is one of the priorities in reforming the defense and security sectors of Ukraine.

Therefore, the main problems that need to be solved are: 1) the absence of common criteria and methodology for the ITS infrastructure objects assigning as critical infrastructure; 2) the absence of common methodology for assessing security threats of critical infrastructure facilities.

Problem Statement. According to the Law of Ukraine "On the Basic Principles of Cybersecurity of Ukraine" [1] defines the need to form a list of critical information infrastructure facilities and the need to develop criteria and procedures for attributing objects to critical infrastructure facilities. Also, the Decree of the President of Ukraine No 96 / 2016 On the decision of the National Security and Defense Council of Ukraine on January 27, 2016 "On the Cybersecurity Strategy of Ukraine" [2] provides that the cybersecurity of critical infrastructure should determine the criteria for attributing informational (automated), telecommunications, the ITS to critical information infrastructure.

Therefore, the legal acts of Ukraine declare the need to develop common criteria and methodology for classifying the ITS infrastructure as critical infrastructure. At the same time, it should be noted that the use of qualitative assessments is associated with the complexity of their comparison and application. First of all, this is due to the complexity of expert selection and the specificity of expert data processing. These limitations are less typical for quantitative methods of criticality calculation.

The mentioned above limitations indicate that there is an important scientific problem in determining the criteria for classifying the ITS as a critical information infrastructure.

Analysis of the recent studies and publications. In accordance with the Law of Ukraine "On Protection of Information in the Information and Telecommunication Systems" [3] and the Law of Ukraine "On Protection of Personal Data" [4] the following information is subject to mandatory protection: information that is the property of the state, or information with restricted access. In order to ensure the protection of information in the ITS, the Comprehensive Information Security System (CISS) must be developed. It is also should be noted that the Decision of the Cabinet of Ministers of Ukraine "On Approval of General Requirements for Cybersecurity of Critical Infrastructure Facilities" [5] establishes a standard for the implementation of the CISS at a critical information infrastructure facility.

At the same time, the Normative Documents in the field of Technical Protection of Information of Ukraine (ND TPI), which describe the procedure for the CISS creation [6] and the criteria for the information security assessment [7] are outdated and do not meet the current requirements [8; 9]. For example, the criteria are defined in the ND TPI [7] have not been updated since 1999, the requirements for the procedure of the CISS creation have not been updated since 2005. On the other hand, the international normative documents are revised and clarified almost annually [10].

Therefore, there is a problem in the necessity of creating the CISS and the lack of standards, according to which the CISS must be created.

In the most countries of the world, the information and telecommunications industry is considered to be one of the most critical sectors (after energy and transport sectors) [8]. Given that, the experimental verification of the developed provisions was carried out on the example of the National System of Confidential Communication (NSCC).

In accordance with the Law of Ukraine "On the National System of Confidential Communications" [11] the NSCC is a set of the special telecommunications systems, which allow to exchange the information with limited access by cryptographic and technical means, in the interests of public and local authorities.

According to the Decree of the Cabinet of Ministers of Ukraine "On some issues in the interagency information exchange organization in the NSCC" [12], the main functions of the NSCC are:

- ensuring the exchange of public, proprietary and confidential information between the entities and/or users of the NSCC.
- creation of a technological basis, in which open and proprietary information of public authorities and local governments, military formations, government agencies, state enterprises, institutions and organizations circulate for the information resources integration in the ITS;

- ensuring interaction between the ITS of public authorities and local governments, military formations, government agencies, state enterprises, institutions and organizations;
- ensuring operation of the special ITS of the NSCC entities, using a special transport network of the NSCC;
- ensuring secure access to the Internet for the government agencies.

Considering these functions, it can be assumed that the NSCC (or its subsystems), belong to the critical category. Moreover, when classifying the ITS as critical, it is necessary to consider not only the declared functions, but the actual functions that the system currently executes.

In addition, in the ITS criticality determination, it is necessary to take into account that according to the Presidential Decree of 18.04.2005 No. 663 “On the provision of government communication of officials” [13] the system of government communication is provided by resources of the telecommunications operators on the entire territory of Ukraine.

According to the "Instruction on the organization of networks and systems technical operation of the state system of government communication of Ukraine" [14] one of the main elements of the government communication station is a digital control room of the NSCC transport network for the special purpose.

The purpose of article. The purpose of this article is to develop and experimentally investigate a method of the Functional Security Profile (FSP) formation of the sectoral ITS.

3. Theoretical bases

3.1. Structural and logical model of the functional security profile formation of the sectoral ITS

The ND TPI of Ukraine [7] determines the evaluation result as a rating, which represents as an ordered series (a list) of alphanumeric combinations, indicating the level of implemented services. It is necessary to implement the method of the FSP formation, which will take into account the requirements of this document and allow to use the results of the method in the construction of the CISS in combination with the level of guarantees.

The proposed structural and logical model for the FSP determination of the sectoral ITS (Fig. 1) is based on the use of the basic (initial) FSP. It is defined taking into account the requirements from [7].

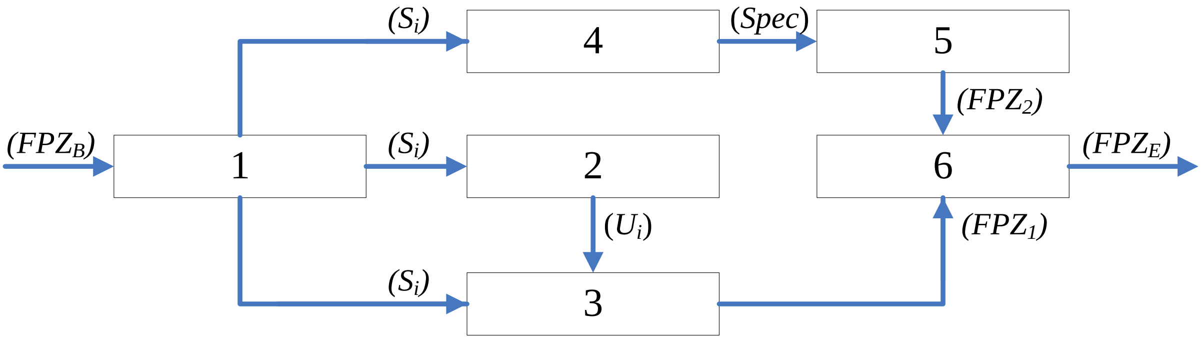

Figure 1: Structural and logical model of the FSP determination of the sectoral ITS

The set of the basic systems of the sectoral ITS is defined (Si) in Block 1.

The information flows (interfaces) of interaction between the main systems of the sectoral ITS (Ui) are defined in Block 2.

The specific (sectoral) requirements (in relation to the basic ones) which are applied to the CIAO (Confidentiality, Integrity, Availability and Observability), to (Si) are defined in Block 3, forming the FSP – FPZ_1.

The regulatory documents and the best practices (ISO / IEC, NIST, NERC CIP, ISACA, CERT, SANS, PCI DSS, COBIT, HIPAA, CSA, ITAF) are analyzed in Block 4 and show the additional (or detailed) requirements (Spec).

The comparison of the additional requirements to the semantics of the ND TPI 2.5-004-99 and the FPZ_2 requirements formation is carried out in Block 5.

The correction of the basic FSP, or development of the FSP for the new basic system of the sectoral ITS (FPZ_E) takes place in Block 6.

The developed model allows to use any other security profile that experts can offer. It also allows to formalize the implemented security services, taking into account additional security requirements, based on the world's best practices.

3.2. Structural and functional method of the functional security profile formation of the sectoral ITS

The structural and functional method of the FSP formation of the sectoral ITS consists of the following steps:

Step 1. Determination of the set of basic systems (elements) of the sectoral ITS (Si) and information flows (interfaces) of interaction of these systems (Ui);

Step 2. Formation of specific (sectoral) requirements (in relation to the basic) for the CIAO to (Si) – FPZ_1;

Step 3. Identification of the normative documents and the best practices of additional or detailed requirements (Spec);

Step 4. Formation of additional requirements in the form of the ND TPI semantics and the formation of requirements FPZ_2;

Step 5. Correction of the basic FPZ, or development of the FPZ_E for a new system of the sectoral ITS – FPZ_E.

The proposed structural and functional method of the FSP formation of the sectoral ITS takes into account modern experience and the best international practices and allows (in comparison with the current ND TPI 2.5-004-99) to formulate criteria for assessing the security of information circulating in the critical ITS in more detail.

4. Research result

4.1. The experimental study of the structure and functional method of the functional security profile formation of the sectoral ITS

The use of the developed method was analyzed on the example of the NSCC ITS.

Step 1: Determination of the set of basic systems (elements) of the sectoral ITS (Si) and information flows (interfaces) of interaction of these systems (Ui).

According to [12], the NSCC consists of the following isolated ITS of the special communication (hereinafter referred as "NSCC systems"):

1. The NSCC special transport network is a telecommunication network which is designed to transit traffic between the NSCC systems.
2. The special NSCC ITS of their subjects which is designed to exchange public, proprietary and confidential information on behalf of the public authorities, legal entities and individuals who order and/or receive the NSCC services.
3. The NSCC special mobile communication network which is designed for exchange of proprietary and confidential information on behalf of the NSCC subjects while staying in stationary and non-stationary conditions using the mobile subscriber terminals, protection of which is ensured by cryptographic and technical methods. A special cellular communication network operates as a part of the special mobile communication network of the NSCC.
4. The special ITS for a secure video conferencing of the NSCC, which is designed for real-time official meetings for the public and local authorities' heads.
5. A secure electronic document management system of the NSCC which is designed to ensure the operational document exchange of the proprietary and confidential information between the public authorities, local governments. It also helps to analyze and monitor the implementation of the Decisions of the President of Ukraine and the Cabinet of Ministers of Ukraine. This system includes

a Certification Authority which is designed to provide the state and local authorities with electronic digital signature services.

6. A secure Internet access system provided for government authorities and designed to protect government information resources processed in the ITS, which are accessed via the Internet.

The most critical systems from the information leakage point of view are: the special transport network, the special ITS of secured videoconferencing and secured electronic document management system (hereinafter referred as "EDMS").

According to the functional purpose, the dedicated systems can be grouped as follows:

The special transport network – transport system, information protection system, management system;

The ITS videoconferencing and EDMS – service systems (provision of services to the subscriber).

Step 2: Formation of specific (sectoral) requirements (in relation to the basic) for the CIAO to (Si) – FPZ$_1$.

As of now, the core of the NSCC includes the following main components [15]:

The CUCM – Cisco Unified Communications Manager. This is the central component of the Cisco communications platform that connects to and interacts with other Cisco services such as IM & Presence, Contact Center Express, Pagginig, Media Sence, Webex, external auxiliary services and information systems such as Microsoft Active Directory (LDAP), DNS, Aurus Directory and others. The CUCM is a cluster of two virtual machines. The main server processes call and serves subscribers in a normal mode is called Publisher, the second server, despite being active, but does not serve subscribers in the normal mode, is called Subscriber.

The Cisco IM & Presence service is a virtual machine, or cluster of two virtual machines. The service allows to collect and publish information about the status of the user and expands its communication capabilities. The user’s availability shows the possibility to establish a communication with him, and also provides information about the possible ways of communication, such as audio communication, e-mail, interactive messaging. General information is displayed in the Jabber client application, which increases the speed and efficiency of interaction with colleagues, by selecting the most efficient way for communication. The central back-end component is called the Extensible Communications Platform (XCP). The XCP uses the SIP / SIMPLE and Extensible Messaging and Presence Protocol (XMPP). The primary server that processes messages and serves subscribers in normal mode is called Publisher, the second server, despite being active, but does not serve subscribers in normal mode, is called Subscriber.

The MediaSence service allows a customer to record, view, listen and download conversations through a web interface. The Cisco Webex Server service is a system for online conferences, meetings, video conferences and webinars. Clients are loaded into the web-browser as plugins, then connected to the server. It consists of the several virtual machines. An administrator virtual machine, a reverse proxy-server virtual machine (for access from the Internet), the Webex conference virtual machine, and a media processing virtual machine. Depending on the number of simultaneous sessions and the ability to access from the Internet, the number of virtual machines may change.

The R-PC is Prime Collaboration Software. It provides a single interface for subscriber management and all communication services, as well as quick configuration of equipment and integration with the data network. It has the following functions: end-to-end monitoring, sessions review (planned, executed and current sessions), quick troubleshooting in network or terminal, latency control, packet loss (operational diagnosis), monitoring the video route and voice sessions in the network, CPU statistics, memory and interfaces of Cisco equipment review, jitter, packet loss, DSCP data for Cisco equipment review. The CTI-CMS is Cisco Meeting Server 1000 Bundle. The software platform for conferencing provides the following features:

- connection of any participant using Cisco or third-party video terminals, Cisco Jabber client, Cisco Meeting App (client program or WebRTC compatible browser) or Skype for Business;
- deployment of the solutions on Cisco CMS platforms, with support for up to 96 high-definition video ports in a single rack space (1RU);
- unlimited growth with a seamless scalability and unified user environment (platform-independent function);
- costs control by the bandwidth usage optimization between the data centers.

The ASA5516-FPWR is the ASA 5516-X with FirePOWER services. A multifunctional firewall, which is designed for advanced protection against the latest threats and malware. The Cisco ASA firewall with FirePOWER services provides a seamless threat protection before, during, and after an attack, by combining the Cisco ASA firewall and the industry-leading Sourcefire threat and malware protection capabilities in a single appliance.

Cisco ASA with FirePOWER services offers the following features:

- remote access to VPN network and advanced clustering features that provide fast and secure access, and high system reliability;
- advanced application monitoring and control supports more than 3,000 application-level controls which can activate the installed threat detection policies in the Intrusion Prevention System (IPS) in a risk event, significantly enhancing protection;
- FirePOWER is the Next-Generation Intrusion Prevention System (NGIPS), which significantly enhances threat protection and provides the full contextual information about users, infrastructure, applications and their content, timely detects multi-vector threats and automates the protection process;
- URL filtering by reputation and category provides comprehensive control over suspicious web traffic, as well as policy enforcement for hundreds of millions of URLs in more than 80 categories;
- advanced anti-malware software provides high intrusion detection, low-cost ownership and an optimal level of protection, making it possible to quickly detect, analyze and prevent the spread of a malware and other emerging threats that may be missed on other layers of protection.

Taking into account the above components of the NSCC core, as well as the decomposition of their systems (Table A.1), outline the security requirements regarding to each of the objects (systems). The specified requirements are listed in Table A.2 (the listed requirements are already implemented in the NSCC).

The formation of the sectoral requirements for the NSCC subsystems (FPZ$_1$) is carried out taking into account the standard FSP of the processed information from unauthorized access [16, 24] and taking into account Table A.2.

FSP of the transport system - 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-2, OP-1, OT-2, ON-2, OE-1, OR-1;

FSP of the service system - CA-2, CE-2, CT-2, CO-1, IA-2, IE-1, IT-1, IR-1, AF-2, AQ-2, AD-2, AR-2, OI-2, OC-1, OD-3, OP-1, OT-2, ON-2, OE-2;

FSP of the protection system - 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-1, OR-1;

FSP of the management system - CA-2, CE-2, CT-2, CO-1, IA-2, IE-2, IT-1, IR-2, AF-1, AQ-2, AD-2, AR-1, OS-1, OI-2, OC-1, OD-3, OP-2, OT-2, ON-2, OE-1, OR-1.

The final FSP of the NSCC can be calculated as a combination of the FSPs of the integral systems, namely - 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.

Step 3: Identification of the normative documents and the best practices of additional or detailed requirements (Spec).

The following regulatory documents describe the security requirements for the NSCC systems: NIST SP 800-53A. Guide for Assessing the Security Controls in the Federal Information Systems and Organizations [17]; NIST SP800-53. Security and Privacy Controls for the Federal Information Systems and Organizations [18]; State standards of Ukraine (DSTU) ISO / IEC 27002: 2015 Information technologies. Methods of protection. Code of practices for information security measures [19]; ISO/IEC 15408-1:2009 Evaluation criteria for IT security [20].

Step 4: Formation of additional requirements in the form of the ND TPI semantics and the formation of requirements FPZ$_2$.

During the formation of additional requirements in the form of semantics of ND TPI, it is advisable to use the relevant normative documents [16; 21-24].

Taking into account the security requirements for regional information systems [18], the additional requirements for the FSP of the NSCC can be formed (Table 1), where ACO_VUL means advanced composition vulnerability analysis services, AVA_VAN means enhanced methodological vulnerability analysis, ADV_ARC means additional material on security architecture (self-protection, domain distribution, traversal impossibility), ADV_INT means internal structure.

Table 1
Additional requirements for the FSP of the NSCC

No.	Security service name	NIST SP800-53	ISO/IEC 15408-1
1	Risk Assessment	RA-3	AVA_VAN.1 AVA_VAN.2 AVA_VAN.3 AVA_VAN.4 AVA_VAN.5 ACO_VUL.1 ACO_VUL.2 ACO_VUL.3
2	Vulnerability Scanning	RA-5	–
3	Security Function Isolation	SC-3	ADV_ARC.1 ADV_INT.1 ADV_INT.2 ADV_INT.3

Considering the data given in Table 1 it is possible to form the detailed (additional) requirements in the form of the ND TPI semantics and to form the FPZ$_2$ requirements (Table 2). Besides, during formation of the additional safety requirements it is necessary to take into account the standard requirements [16, 24] set out in Table 3.

Step 5: Correction of the basic FPZ, or development of the FPZ$_E$ for a new system of the sectoral ITS – FPZ$_E$.

Correction of the basic FPZ for FPZ$_E$ of the NSCC systems is carried out taking into account the data presented in Tables 2-3.

Table 2
Additional requirements

No.	Additional NIST functional criteria	ND TPI (FPZ$_2$)
1	RA-3	ON-3, ON-4, ON-5, OT-3
2	RA-5	CC-2, OT-3
3	SC-3	IA-4, AD-3, OT-3

Table 3
Standard FSP of Class 3 automated systems

No.	Standard FSP
1	3.IT.3 = {CO-1, IT-1, IA-3, IR-2, IE-2, AR-3, AF-2, AQ-2, AD-2, ON-3, OI-2, OC-1, OD-2, OP-3, OT-2, OE-2, OS-1, OR-1}
2	3.CT.3 = {CT-3, CA-3, CO-1, CC-1, CE-4, AR-3, AF-2, AQ-2, AD-2, ON-4, OI-2, OC-1, OD-3, OP-3, OT-2, OE-2}
3	3.CT.3 = {CT-3, CA-3, CO-1, CC-1, CE-4, AR-3, AF-2, AQ-2, AD-2, ON-4, OI-2, OC-1, OD-3, OP-3, OT-2, OE-2}
4	3.IT.3 = {CO-1, IT-1, IA-3, IR-2, IE-2, AR-3, AF-2, AQ-2, AD-2, ON-3, OI-2, OC-1, OD-2, OP-3, OT-2, OE-2, OS-1, OR-1}

Table 4
Correction of the basic FSP

No.	Basic FSP	Additional functional criteria	Corrected FSP
1	CT-2, CA-2, CO-1, CE-3, IT-1, IA-2, IR-2, IE-2, AR-2, AF-2, AD-2, AQ-2, OS-1, ON-2, OI-2, OC-1, OD-2, OP-1, OT-2, OE-1, OR-1	CO-1, IT-1, IA-3, IR-2, IE-2, AR-3, AF-2, AQ-2, AD-2, ON-3, ON-4, ON-5, OI-2, OC-1, OD-2, OP-3, OT-2, OT-3, OE-2, OS-1, OR-1	CT-2, CA-2, CO-1, CE-3, IT-1, IA-3, IR-2, IE-2, AR-3, AF-2, AQ-2, AD-2, OS-1, ON-3, ON-4, ON-5, OI-2, OC-1, OD-2, OP-3, OT-2, OT-3, OE-2, OR-1
2	CT-2, CA-2, CO-1, CE-2, IT-1, IA-2, IR-1, IE-1, AR-2, AF-2, AD-2, AQ-2, ON-2, OI-2, OC-1, OD-3, OP-1, OT-2, OE-2	CT-3, CA-3, CO-1, CC-1, CC-2, CE-4, AR-3, AF-2, AQ-2, AD-2, ON-4, OI-2, OC-1, OD-3, OP-3, OT-2, OT-3, OE-2	CT-3, CA-3, CO-1, CC-1, CC-2, CE-4, IA-2, IE-1, IT-1, IR-1, AR-3, AF-2, AQ-2, AD-2, ON-4, OI-2, OC-1, OD-3, OP-3, OT-2, OT-3, OE-2
3	CT-2, CA-2, CO-1, CE-3, IT-1, IA-2, IR-2, IE-2, AR-2, AF-2, AD-2, AQ-2, OS-1, ON-2, OI-2, OC-1, OD-3, OP-2, OT-2, OE-1, OR-1	CT-3, CA-3, CO-1, CC-1, CE-4, AR-3, AF-2, AQ-2, AD-2, AD-3, ON-4, OI-2, OC-1, OD-3, OP-3, OT-2, OT-3, OE-2, IA-4	CT-3, CA-3, CO-1, CC-1, CE-4, IA-4, IE-2, IT-1, IR-2, AR-3, AF-2, AQ-2, AD-2, AD-3, OS-1, ON-4, OI-2, OC-1, OD-3, OP-3, OT-2, OT-3, OE-2, OR-1
4	CT-2, CA-2, CO-1, CE-2, IT-1, IA-2, IR-2, IE-2, AR-1, AF-1, AD-2, AQ-2, OS-1, OI-2, OC-1, OD-3, OP-2, OT-2, ON-2, OE-1, OR-1	CO-1, IT-1, IA-3, IR-2, IE-2, AR-3, AF-2, AQ-2, AD-2, ON-3, OI-2, OC-1, OD-2, OP-3, OT-2, OE-2, OS-1, OR-1	CA-2, CE-2, CT-2, CO-1, IT-1, IA-3, IR-2, IE-2, AR-3, AF-2, AQ-2, AD-2, ON-3, OI-2, OC-1, OD-2, OD-3, OP-3, OT-2, OE-2, OS-1, OR-1

5. Conclusion

Therefore, the article analyzes the current normative documents, which are used to assess the effectiveness of critical infrastructure information system's protection. It was determined, that international and regional normative documents propose to assess the effectiveness of system protection through the risk assessment (the lower the risk, the higher the protection effectiveness). At the same time, Ukrainian ND TPI No. 2.5-004-99 determines the assessment result as an ordered series (listing) of alphanumeric combinations, which indicate the level of services implemented, combined with the level of guarantees. Thus, there is a contradiction between the approaches for assessing the effectiveness of system's protection, which grounds the direction of this article.

In addition, in the article the structural and functional method of the FSP formation of the sectoral ITS was developed. It consists of five stages. The proposed method takes into account current world experience in the field of information protection and allows to formulate criteria for assessing the security of information that circulates in the critical ITS in more detail, in comparison with the mentioned ND TPI. Implementation of the proposed method allows to adjust the basic FSP of the sectoral ITS, by defining the sectoral requirements for confidentiality, integrity, availability and observability.

Moreover, an experimental study of the proposed method was carried out using the developed method of forming the FSP of the sectoral ITS. A decomposition of the NSCC into component systems, subsystems and components was performed, sectoral requirements for information protection were formulated, additional requirements in the form of ND TPI semantics were determined, and the basic functional profile of security [25-26] was adjusted.

6. References

[1] Ukraine. Laws. "On the basic principles of cybersecurity in Ukraine": official text: [adopted by the Verkhovna Rada on October 5, 2017]. Kyiv, Information of the Verkhovna Rada of Ukraine, 2017, No. 45, p. 403.

[2] Decree of the President of Ukraine No. 96, 2016 "On the decision of the National Security and Defense Council of Ukraine of January 27, 2016" On the Cyber Security Strategy of Ukraine".

[3] Ukraine. Laws. "On the protection of information in information and telecommunications systems": official text: [adopted by the Verkhovna Rada on July 5, 1994]. Kyiv, Information of the Verkhovna Rada of Ukraine, 1994, No. 31, p. 287.

[4] Ukraine. Laws. "On personal data protection": official text: [adopted by the Verkhovna Rada on June 1, 2010]. Kyiv, Information of the Verkhovna Rada of Ukraine, 2010, No. 34, p. 481.

[5] Resolution of the Cabinet of Ministers of Ukraine "On approval of the General requirements for cyber protection of critical infrastructure" No. 518 of 19.06.2019.

[6] ND TPI 3.7-003-05 "The order of works on creation of complex system of protection of information in information and telecommunication system", State Service of Special Communication and Information Protection of Ukraine, 2005.

[7] ND TPI 2.5-004-99 "Criteria for assessing the security of information in computer systems from unauthorized access", State Service of Special Communication and Information Protection of Ukraine, 1999.

[8] Report on research work "Research and analysis of information security problems at critical infrastructure facilities", code "Infrastructure" (No. 0114U000038d).

[9] S. Honchar, G. Leonenko, O. Yudin. "Analysis of threats and vulnerabilities of sectoral automated control systems". Legal, regulatory and metrological support of information security in Ukraine, Vol. 2 (26), pp. 9-14, 2013.

[10] Z. Hu, Yu. Khokhlachova, V. Sydorenko, I. Opirskyy, "Method for Optimization of Information Security Systems Behavior under Conditions of Influences", International Journal of Intelligent Systems and Applications (IJISA), Vol.9, No.12, pp.46-58, 2017.

[11] Ukraine. Laws. "On the National System of Confidential Communication": official. text: [adopted by the Verkhovna Rada on January 10, 2002]. Kyiv, Information of the Verkhovna Rada of Ukraine, 2002, No. 15, p.103.

[12] Resolution of the Cabinet of Ministers of Ukraine "Some issues of interdepartmental exchange of information in the National system of confidential communication" No. 303 from 14.05.2015.

[13] Decree of the President of Ukraine of April 18, 2005 No. 663 “On providing government officials with communication”.
[14] Order of the State Service of Special Communication and Information Protection of Ukraine dated 18.05.2015 No.07 “On approval of the instruction on the organization of technical operation of networks and complexes of the state system of governmental communication of Ukraine”.
[15] Report on research work “Determination of ways to create a special system of unified communications in the interests of subscribers of government agencies, institutions and organizations”, code “Platform” (DR № 0116U000072T).
[16] ND TPI 2.5-005-99 “Classification of automated systems and standard functional profiles of protection of processed information from unauthorized access”, State Service of Special Communication and Information Protection of Ukraine, 1999.
[17] National Institute of Standards and Technology Special Publication 800-53A. Guide for Assessing the Security Controls in Federal Information Systems and Organizations: Building Effective Security Assessment Plans. June 2010.
[18] National Institute of Standards and Technology Special Publication SP800-53. Security and Privacy Controls for Federal Information Systems and Organizations. April 2013.
[19] DSTU ISO / IEC 27002: 2015 Information technologies. Methods of protection. Code of practices for information security measures.
[20] ISO/IEC 15408-1:2009 Information technology - Security techniques - Evaluation criteria for IT security - Part 1: Introduction and general model, The International Organization for Standardization and The International Electrotechnical Commission, 2009.
[21] ND TPI 2.6-002-2015 “Procedure for comparing the functional safety components defined by ISO / IEC 15408 with the requirements of ND TPI 2.5-004-99”, State Service of Special Communication and Information Protection of Ukraine, 2015.
[22] ND TPI 2.6-003-2015 “Procedure for comparing the security confidence components defined by ISO / IEC 15408 with the requirements of ND TPI 2.5-004-99”, State Service of Special Communication and Information Protection of Ukraine, 2015.
[23] ND TPI 2.7-013-2016 “Guidelines for comparing the results of the evaluation of information protection against unauthorized access for compliance with the requirements of the ISO / IEC 15408 with the requirements of ND TPI 2.5-004-99”, State Service of Special Communication and Information Protection of Ukraine, 2016.
[24] O. Yudin, “Structural-logical and functional models for determining the functional security profile of the ITS subsystems”, in: Proceedings of the XX International scientific-practical conf. Information Security in Information and Telecommunication Systems, Kyiv, May 22-24, 2018, pp. 50-51, 2018.
[25] Z. Hu, R. Odarchenko, S. Gnatyuk, M. Zaliskyi, A. Chaplits, S. Bondar, V. Borovik, “Statistical Techniques for Detecting Cyberattacks on Computer Networks Based on an Analysis of Abnormal Traffic Behavior”, International Journal of Computer Network and Information Security (IJCNIS), Vol.12, No.6, pp.1-13, 2020.
[26] Z. Hu, I. Dychka, M. Onai, Yu. Zhykin, “Blind Payment Protocol for Payment Channel Networks”, International Journal of Computer Network and Information Security (IJCNIS), Vol.11, No.6, pp.22-28, 2019.

7. Appendix

Table A.1
Decomposition of the NSCC systems

No.	Object	Description
1	2	3
	Transport network	
1	Office system (St1)	Providing connection of subscriber equipment physically
1.1	System of the subscriber equipment (St11)	Terminal equipment (telephones, cable, connectors, information protection means)
1.2	Network access system (St12)	Network access equipment (switch, router, cable structure)

1	2	3
1.3	Auxiliary protection systems (St13)	Auxiliary equipment (backup power supplies, alarm sensors, alarm lines)
2	Telecommunication operator system (St2)	Providing connection of the operator equipment at the physical level
2.1	Physical level system (St21)	Cable, connectors, signal amplifiers (repeaters), switchboards, signal converters, network adapters
2.2	Channel level system (St22)	Access switches, node switches, service switches
2.3	Transport and network layer system (St23)	Trunk switches, multiservice routers, carrier-class switches
2.4	Application systems (St24)	Physical layer management system servers, channel layer management servers, transport and network layer management servers
3	Operator system (St3)	Providing connection of the operator equipment on a logical level
3.1	Physical level system (St31)	Structured cable system, network adapters, signal converters
3.2	Channel level system (St32)	Access switches
3.3	Transport and network layer system (St33)	Switches, routers
3.4	Application systems (St34)	Transport and network layer control and management servers
Service systems (provision of services)		
4	Office system (Ss1)	–
4.1	Subscriber equipment application systems (Ss11)	Terminal equipment (communication terminal, video communication terminal, data transmission workstation)
5	Operator system (Ss2)	Providing customer service
5.1	Operator communication systems (Ss21)	E-mail servers, the CA, registry and directory servers, CUCM server, domain controller server, video call server, contact center server
5.2	Management and redundancy system (Ss22)	Backup storage servers, Prime Collaboration Assurance, Prime Collaboration Provisioning, workstation management
Information protection system		
6	Office system (St1)	Protection of terminal equipment and premises
6.1	System of the subscriber equipment (St11)	Security package of a phone, phone connection block
6.2	Network access system (St12)	Switch Security Package, Router Security Package, cryptographic protection of information
6.3	Auxiliary protection systems (St13)	Alarm sensors, fire alarm sensors, alarm panel
7	Telecommunication operator system (St2)	Protection of communication channels and operator equipment
7.1	Physical level system (St21)	Cable damage detection devices, signal amplifier (repeater) control devices, multiplexer
8	Operator system (Sd3)	Operator equipment protection
8.1	Channel level monitoring and protection system (Sd22)	Access Switch Security Package, Node Security Package, Service Switch Security Package
8.2	Transport and network layer monitoring and protection system (Sd23)	Router Security Package, Switch Security Package, Monitoring System Security Package, Management System Security Package, Workstation Control System
8.3	Auxiliary protection systems (Sd24)	Physical Communication lines Security Package, Alarm System Security Package
9	Operator system (Sd3)	Implementation of systems management to the service provider
9.1	Physical level protection system (Sd31)	Devices for cable damage detection, devices for signal amplifiers (repeaters) control, multiplexer
9.2	Channel level monitoring and protection system (Sd32)	Access Switch Security Package, Node Security Package, Service Switch Security Package, DDoS Protector

1	2	3
9.3	Transport and network layer monitoring and protection system (Sd33)	Router Security Package, Switch Security Package, Monitoring System Security Package, Management System Security Package, Workstation Control System, DDoS Protector
9.4	Application-level protection system (Sd34)	Next Generation Threat Prevention firewall, firewall, operating system protection, database protection
9.5	Cryptographic protection system (Sd35)	Cryptographic protection of information
9.6	Auxiliary protection systems (Sd36)	Backup power supplies, alarm sensors, alarm lines, alarm panel, cooling devices (systems)
	Management system	
10	Office system (Sm1)	Management and control of terminal equipment
10.1	Subscriber sensor system (Sm11)	Sensors for opening the installation box, sensors for connecting subscriber equipment, sensors for access to cryptographic protection of information
10.2	Network access control system (Sm12)	Switch and router settings, switch and router software, redundant power supply software
10.3	System of work logging (Sm13)	Switch and router software, backup power supply software, subscriber equipment software
11	Operator system (Sm2)	Managing the telecom operator's systems
11.1	Node equipment control system (Sm21)	Software for the multiplexer management, switch and router management software, server hardware management software, firewall and DDoS protection management software
11.2	Cryptographic security management system (Sm22)	Information cryptographic protection software, the CA management software
11.3	Application software management system (Sm23)	Application management servers’ software
11.4	Subscriber equipment management system (Sm24)	Remote user configuration software

Table A.2

Functional security profile of the NSCC objects

No.	Object	Description
1	2	3
	Transport network	
1	Office system (St1)	–
1.1	System of the subscriber equipment (St11)	CA-2, CE-3, IA-2, IE-2, OC-1, OE-1, ON-2, OT-2, OI-2, OS-1, OR-1
1.2	Network access system (St12)	CA-1, CA-2, CE-3,IA-1, IA-2, IE-2, AR-1, AF-1, AD-1, ON-1, ON-2, OT-2, OI-1, OI-2, OS-1, OC-1, OD-2, OP-1, OP-2, OE-1, OR-1
1.3	Auxiliary protection systems (St13)	AF-1, AD-1, OT-2, ON-1
2	Telecommunication operator system (St2)	–
2.1	Physical level system (St21)	CA-2, IA-1, AF-1, AQ-1,AD-1, ON-1, ON-2, НИ-2, OD-2, OC-1, OT-2
2.2	Channel level system (St22)	CA-1, CA-2, IA-1, IA-2, AR-1, AF-1, AD-1, ON-1, ON-2, OI-1, OI-2, OC-1, OD-2, OP-1, OE-1
2.3	Transport and network layer system (St23)	CA-1, CA-2, IA-1, IA-2, IR-2, AR-1, AF-1, AQ-1, AQ-2, AD-1, ON-1, OI-1, OI-2, OC-1, OD-2, OT-2, OE-1
2.4	Application systems (St24)	CA-2, CT-2. CO-1, CE-2, IA-1, IE-1, IT-1, IR-1, AF-2, AQ-2, AD-2, AR-2, ON-2, OI-2, OD-1, OC-1, OT-2, OE-1
3	Operator system (St3)	–
3.1	Physical level system (St31)	CA-2, IA-1, AF-1, AQ-1,AD-1, ON-1, ON-2, НИ-2, OD-2, OC-1, OT-2
3.2	Channel level system (St32)	CA-1, CA-2, IA-1, IA-2, AR-1, AF-1, AD-1, ON-1, ON-2, OI-1, OI-2, OC-1, OD-2, OE-1
3.3	Transport and network layer system (St33)	CA-1, CA-2, IA-1, IA-2, AR-1, AF-1, AD-1, ON-1, ON-2, OI-1, OI-2, OC-1, OD-2, OE-1
3.4	Application systems (St34)	CA-2, CT-2. CO-1, CE-2, IA-1, IE-1, IT-1, IR-1, AF-2, AQ-2, AD-2, AR-2, ON-2, OI-2, OD-1, OC-1, OT-2, OE-1
	Service systems (provision of services)	
4	Office system (Ss1)	–

1	2	3
4.1	Subscriber equipment application systems (Ss11)	CT-2, CE-1, CO-1, IT-1, IA-1, IE-1, IR-1, AR-1, AQ-2, AD-2, ON-1, ON-2, OI-1, OI-2, OC-1, OD-3, OT-2, OE-1
5	Operator system (Ss2)	–
5.1	Operator communication systems (Ss21)	CT-2, CA-1, CA-2, CO-1, CE-1, IT-1, IA-1, IA-2, IR-1, IE 1, AR-1, AF-1, AQ-2, AD-2, ON-2, OI-1, OI-2, OC-1, OD-1, OD-3, OT-2, OE-1
5.2	Management and redundancy system (Ss22)	CA-1, CA-2, CT-2, CO-1, CE-2, IA-1, IE-1, IT-1, IR-1, IR-2, AF-2, AQ-2, AD-2, AR-2, ON-2, OI-2, OD-1, OD-2, OC-1, OT-2, OE-1
Information protection system		
6	Office system (St1)	–
6.1	System of the subscriber equipment (St11)	IR-1, AF-1, AD-1, ON-1, ON-2, OP-1, OE-1, OT-2
6.2	Network access system (St12)	CA-1, CA-2, CE-2, IA-1, IA-2, IE-2, AR-1, AF-1, AD-1, ON-1, ON-2, OI-1, OI-2, OC-1, OD-2, OT-2, OP-1, OP-2, OE-1, OS-1, OR-1
6.3	Auxiliary protection systems (St13)	AF-1, AD-1, OT-2, ON-1, OT-2
7	Telecommunication operator system (St2)	–
7.1	Physical level system (St21)	CA-2, IA-1, AF-1, AQ-1,AD-1, ON-2, НИ-2, OD-2, OC-1, OP-1, OT-2
7.2	Operator system (Sd3)	CA-1, CA-2, IA-1, IA-2, AR-1, AF-1, AD-1, ON-1, ON-2, OI-1, OI-2, OC-1, OD-2, OP-1, OE-1
7.3	Channel level monitoring and protection system (Sd22)	CA-2, CT-2, CO-1, CE-2, IA-1, IA-2, IE-1, IT-1, IR-1, AR-1, AF-2, AQ-2, AD-2, AR-2, ON-2, OI-2, OD-1, OD-3, OC-1, OP-1, OT-2, OE-1
7.4	Transport and network layer monitoring and protection system (Sd23)	AF-1, AD-1, OT-2, ON-1
8	Auxiliary protection systems (Sd24)	–
8.1	Operator system (Sd3)	CA-2, IA-1, AF-1, AQ-1,AD-1, ON-2, НИ-2, OD-2, OC-1, OP-1, OT-2
8.2	Physical level protection system (Sd31)	CA-1, CA-2, IA-1, IA-2, AR-1, AF-1, AQ-1, AD-1, ON-1, ON-2, OI-1, OI-2, OC-1, OD-2, OP-1, OE-1, OT-2
8.3	Channel level monitoring and protection system (Sd32)	CA-2, CT-2, CO-1, CE-2, IA-1, IE-1, IT-1, IR-1, AF-2, AQ-2, AD-2, AR-2, ON-2, OI-2, OD-1, OD-3, OC-1, OP-1, OP-2, OT-2, OE-1
8.4	Transport and network layer monitoring and protection system (Sd33)	CT-2, CA-1, CA-2, CO-1, CE-1, IT-1, IA-1, IA-2, IR-1, IR-2, IE-1, AR-1, AF-1, AQ-2, AD-2, ON-2, OI-1, OI-2, OC-1, OD-3, OP-1, OP-2, OT-2, OE-1
8.5	Application-level protection system (Sd34)	CA-2, CE-3, IA-2, IE-2, OC-1, OE-1, ON-2, OT-2, OP-2, OI-2, OS-1, OR-1
8.6	Cryptographic protection system (Sd35)	AF-1, AD-1, OT-2, ON-1
Management system		
9	Subscriber sensor system (Sm11)	–
9.1	Network access control system (Sm12)	AF-1, AD-1
9.2	System of work logging (Sm13)	CA-1, CA-2, CT-2, CE-1, CO-1, IT-1, IA-1, IA-2, IE-1, IR-1, AR-1, AF-1, AQ-2, AD-2, ON-1, ON-2, OI-1, OI-2, OC-1, OD-3, OP-2, OT-2, OE-1
9.3	Operator system (Sm2)	CA-1, CA-2, IA-1, IA-2, AR-1, AF-1, AD-1, OT-2, ON-1, ON-2, OI-1, OI-2, OC-1, OD-2, OP-1, OE-1
10	Node equipment control system (Sm21)	–
10.1	Cryptographic security management system (Sm22)	CA-1, CA-2, IA-1, IA-2, AR-1, AF-1, AQ-1, AD-1, ON-1, ON-2, OI-1, OI-2, OC-1, OD-2, OP-1, OE-1, OT-2
10.2	Application software management system (Sm23)	CT-2, CA-1, CA-2, CO-1, CE-1, CE-2, IT-1, IA-1, IA-2, IR-1, IE-1, IE-2, AR-1, AF-1, AQ-2, AD-2, ON-2, OI-1, OI-2, OC-1, OD-3, OP-1, OP-2, OT-2, OE-1, OS-1, OR-1
10.3	Subscriber equipment management system (Sm24)	CT-2, CA-1, CA-2, CO-1, CE-1, IT-1, AI 1, AI 2, IR-1, IE 1, AR-1, AF 1, AQ-2, AD-2, ON-2, OI-1, OI 2, RC 1, OD-3, OP-1, OP-2, OT-2, OE-1
10.4	Subscriber sensor system (Sm11)	CT-2, CA-1, CA-2, CO-1, CE-1, IT-1, AI 1, AI 2, IR-1, IE 1, AR-1, AF 1, AQ-2, AD-2, ON-2, OI-1, OI 2, RC 1, OD-3, OP-1, OP-2, OT-2, OE-1