Method of Cybersecurity Level Determining for the Critical Information Infrastructure of the State

Sergiy Gnatyuk [1,2,3][0000-0003-4992-0564], Viktoriia Sydorenko [1][0000-0002-5910-0837], Artem Polozhentsev [1][0000-0003-0139-0752], Andriy Fesenko[4] [0000-0001-5154-5324], Nurbol Akatayev [5][0000-0001-5139-0792] and Gulnaz Zhilkishbayeva [3][0000-0001-9955-5994]

[1] National Aviation University, Kyiv, Ukraine
[2] State Scientific and Research Institute of Cybersecurity Technologies and Information Protection, Kyiv, Ukraine
[3] Yessenov University, Aktau, Kazakhstan
[4] Taras Shevchenko National University of Kyiv, Kyiv, Ukraine
[5] Satbayev University, Almaty, Kazakhstan

s.gnatyuk@nau.edu.ua, v.sydorenko@ukr.net, artem.polozhencev@gmail.com, aafesenko88@gmail.com

Abstract. Protection of the state's critical information infrastructure is a complex process, which requires effective tools for entities' identification, assessing their criticality, threat and vulnerability assessment, protection against threats and also determining the cybersecurity level of the individual entities, industries, regions, and countries. The conducted analysis is shown that today there is no complex, multifunctional method which helps to evaluate the cybersecurity level of the critical information infrastructure entity or a certain industry of the state. With that in mind, in this paper the method of determining the cybersecurity level of the state's critical information infrastructure was developed, taking into account the advantages and disadvantages of the known approaches. The method will be useful for CSIRT groups (or any other parties, who is responsible for cybersecurity in organization) to analyze a particular industry and evaluate its cybersecurity level. The developed method allows to calculate quantitative parameters, describing the analyzed sector, also to compare the security level of the critical entity before and after implementation of certain security measures. For example, the usage of the mentioned method in the civil aviation was shown but it can be used in various critical infrastructure sectors.

Keywords: cybersecurity index, critical information infrastructure, civil aviation, cybersecurity level determining.

1 Introduction

The current trends in the development of information and communication technologies (ICT) caused a phenomenal dependence on social services, which are provided by various sectors of infrastructure. Today, with the cutting-edge

technologies, fundamentally new global concepts have emerged, such as information and cyber space, cybersecurity, cyber threat, critical infrastructure (CI), which have nearly unlimited power and a leading role in the economic and social development of each country in the world. However, in addition to its benefits, there are a number of problems caused by the growing vulnerability of the information assets from external cybersecurity impact, which the world's community has also received.

A number of planned in advance, well-executed attacks in cyberspace increase every year, these are so-called APT attacks (Advanced Persistent Threat). According to that, there is a need to control and further regulate the relevant relationships in cyberspace, and therefore urgently creat a reliable cybersecurity system [1].

In October 2017, the Parliament of Ukraine has signed the Law "On Basic Principles of Cybersecurity of Ukraine" [2], in that paper Article 8 clearly describes the definitions, main tasks and stages of the National Cybersecurity System operation. In order to provide the necessary protection (vital interests of the individual, society and state, national interests of Ukraine in cyberspace) of critical information infrastructure (CII) sectors, according to [2], it is necessary to constantly maintain and improve the National Cybersecurity System of Ukraine, by developing and rapidly adapting the public cybersecurity policie; creating a legal and terminological framework for cybersecurity; establishing the mandatory information security requirements of CII sectors; involing the expert scientific institutions, professional and public associations in the preparation of conceptual documents in the cybersecurity field; conducting drills for emergency situations in cyberspace; developing and improving the technical and cryptographic information protection systems; ensuring compliance with the requirements of the legislation on protection of state's information resources and public information; periodicaly review the National Cybersecurity System; developing the cybersecurity indicators etc.

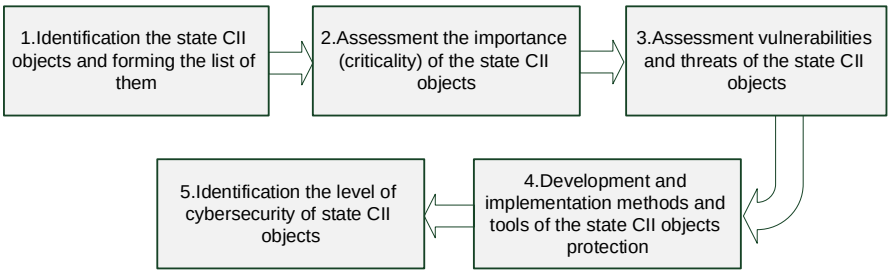

Fig. 1. The general scheme of the state CIIP stages

Rather complicated issues are the development of appropriate indicators and determination of the required protection level of cybersecurity, according to which the price of the security system will not be higher than the usefulness of the information to be protected. This problem can be solved, for example, by determining the necessary level of cybersecurity for a certain facility or relevant CII sector, according to basic approach, presented in [3] and CIIP concept (Fig. 1, Stage 5).

2 Related research analysis and problem statement

In 2016, the International Telecommunication Union (ITU) conducted a complex study of the cybersecurity level of 143 countries.
In 2017 the main results were announced in the report [4], accroding to which, the method for assessing state's security in cyberspace was proposed. It has five pillars – Legal Measures, Technical Measures, Organizational Measures, Capacity Building, and Cooperation. There are twenty-five pillars in total of all indicators. Global Cybersecurity Index (GCI) is calculated as the arithmetic mean of all pillars. A representative from an analised state should answer the 157 question to compleate the poll. Having received the answers, ITU has defined a state's index and a global ranking list was created. State's security level in cyberspace takes value from "1" (highest) to "0" (smallest). What allows to define a worldwide overwiev of the cybersecurity level, to assess the protection level in some parts of the world and to analyze the cybersecurity level of each state separetly. The main disadvantage of this approach is unjustified used indicators, their assessment is subjective. Thus, obtaining the reliable data is a complicated task.

A flexible method for determining the cybersecurity level is reflected in [5]. The authors propose to use cybersecurity metrics that can be used for evaluation, revision, and improvement of the research entity cybersecurity level.

The approach is based on the metrics, which companies and organizations are using in their business processes. To determine the new metric or specific measures, which mathematically described, a set of relevant parameters should be identified. They can be used to analyze and continually improve the business of an organization or a state. The matrics usage is widely used nowadays. The disadvantages of this approach are preliminary modeling, mathematical justification for the development and implementation of these metrics, which is a difficult problem, also the result may not be unbiased enough.

A comprehensive method is proposed in [6].The cybersecurity level can be determined by using completely independent metrics NSCI (National Cyber Security Index) and ISD (Informational Society Score). NSCI consists of some sub-indexes: ISD is divided on the following sub-indexes – IDI (The ICT Development Index) and NRI (Networked Readiness Index) [7]. The disadvantage of this method is necessity to allocate considerable resources for research due to the large number of indicators in order to collect a reliable data.

Mathematical and statistical approach is described in [8]. It is a method for assessing the cybersecurity level of CII assets, which allows to calculate a criticality index of the entity. In order to implement the method, it is necessary to identify key indicators, such as Severity level, the Availability of continuous operation systems, Cost, Downtime etc. Thereafter, a weighting factor must be used for each determinant indicator. Each of them must have a value from "0" to "100", according to the proposed scale of the value calculation. The mportance index of the CII entity can be calculated based on the value of its criticality index. The disadvantage of this method is a difficult adaption to the new systems and complexity of justifying weighting factors and indicators.

In the next paper [9] was proposed a methodology for assessing ICT security, using the example of automated banking systems, which is based on the concept of a complex security management of those systems. The mentioned concept

provides a mutually valid approach to select the most effective ways of achieving the cybersecurity goals. Which also is taking into account the risk value at each level of the management model. It makes it possible to comprehensively select the alternative options for potential cybersecurity strategic decisions. However, the proposed concept is focused exclusively on the banking sector and is not flexible, which means it can not be used for other CII sectors.

According to [3], the analysis results of the mentioned approaches of determining the cybersecurity level by the following criteria are reflected (Table 1): CS is consideration of cybersecurity means and measures; ICT is consideration of ICT implementation; QP is quantitative parameters; CIIP is CII sector protection; UM is universality [10-11].

Table 1. Cybersecurity level determination approaches

Criteria / *Name*	CS	ICT	QP	CIIP	UM
ICT Development index (ITU)	+	+	+	–	–
Method Black, Scarfone, Souppaya	+	+	+	–	–
NCSI (EGA)	+	+	+	–	–
Nestruhin's method	–	–	+	+	–
Yevseev's method	+	+	+	–	–

The analysis shows that the existing methods have a list of disadvantages, including unsubstantiated indicators, which are needed to develop metrics, complex modeling of the given systems, the need to use a complex mathematical tools, statistical resources involvement, which is needed for further analysis and creation of the cybersecurity metrics. Given the need to assess the cybersecurity level of a CII sector, a method for determining the cybersecurity level of the state's CII sector needs to be developed. This issue will be a main target of this work.

3 The main part of the study

A. Proposed method descryption

According to [3] the method of determining the cybersecurity level of the CII sector is implemented in the following 3 stages:

1. Determination of metrics and cybersecurity index of a CII sector;
2. Determination of the ICT development and implementation metrics of a CII sector;
3. Calculation of quantitative parameters, that describe the cybersecurity level of a CII sector.

Input data: information regarding critical infrastructure, cybersecurity methods and tools, ICT implementation.

Output data: quantitative parameters, that describe the security of a particular industry or the state's CII in general. Namely, cybersecurity metrics, ICT development and implementation metrics, also a relevant cybersecurity index.

Consider in details each of the stage of the proposed method by itself.

Stage 1. Determination of the metrics and the cybersecurity index of a CII sector

Step 1.1. Formalization of the cybersecurity metrics

Declaring a basic set of the cybersecurity metrics $\mathbf{P}$:

$$\mathbf{P} = \{\bigcup_{i=1}^{n} \mathbf{P}_i\} = \{\mathbf{P}_1, \mathbf{P}_2, \ldots, \mathbf{P}_n\}, \quad (1)$$

where $\mathbf{P}_i \subseteq \mathbf{P}$ $(i = \overline{1,n})$ is a metrics subset.

Based on the approach proposed in [12-13], the set (1) can be represented as a linked list as it shown in Fig. 2:

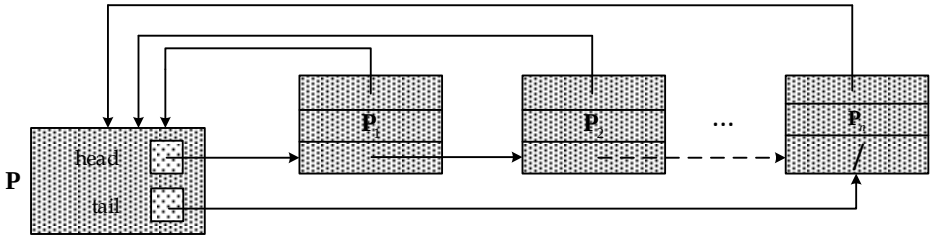

Fig. 2. Representation of a basic set of cybersecurity metrics as a linked list

The set $\mathbf{P}_i$ can be represented as a subset system:

$$\mathbf{P}_i = \{\bigcup_{j=1}^{m_i} P_{ij}\} = \{P_{i.1}, P_{i.2}, \ldots, P_{i.m_i}\}, \quad (2)$$

where P_{ij} $(i = \overline{1,n},\ j = \overline{1,m_i})$ is metrics list of the i parameter (the metric's range value is determined according to appropriate standards and recommended practices for each CII sector), m_i is a number of metrics in i parameter.

Taking into account (2), the set (1) can be represented as follows:

$$\mathbf{P} = \{\bigcup_{i=1}^{n} \mathbf{P}_i\} = \{\bigcup_{i=1}^{n} \{\bigcup_{j=1}^{m_i} P_{ij}\}\} = \{\{P_{1.1}, P_{1.2}, ..., P_{1.m_1}\},$$
$$\{P_{2.1}, P_{2.2}, ..., P_{2.m_2}\}, ..., \{P_{n.1}, P_{n.2}, ..., P_{n.m_n}\}\}, (i = \overline{1,n},\ j = \overline{1,m_i}). \quad (3)$$

Step 1.2. The value calculation of the index, that describes the CII sector cybersecurity level

The index of the CII sector cybersecurity level is calculated according to (1-3) considering (4):

$$\mathbf{I}_{CS} = \frac{\sum_{i=1}^{n}\sum_{j=1}^{m_i} P_{ij} \times 100\%}{\sum_{P_{ij}}^{max}}, \sum_{P_{ij}}^{max} \neq 0, \quad (4)$$

where $\sum_{P_{ij}}^{max}$ is the sum of the maximum possible values of P_{ij} metric.

Stage 2. Determination of the ICT development and implementation metrics of a CII sector

Step 2.1. Formalization of the ICT development and implementation metrics, that describe the ICT readiness and availability

Declaring the metrics set $\mathbf{M}$, that describe the ICT development and implementation:

$$\mathbf{M} = \{\bigcup_{k=1}^{q} \mathbf{M}_k\} = \{\mathbf{M}_1, \mathbf{M}_2, \ldots, \mathbf{M}_q\}, \tag{5}$$

where $\mathbf{M}_k \subseteq \mathbf{M}\ (k = \overline{1,q})$ is the subset of the ICT development and implementation metrics, q is a number of the metric's subsets. Similarly, taking into account [12-13], the set (5) was represented as a linked list as it shown in Fig. 3.

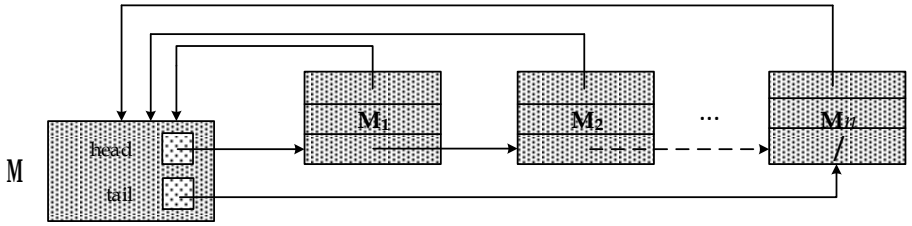

Fig. 3. Representation of the ICT development and implementation metrics as a linked list

The set $\mathbf{M}_k$ can be represented as a subset system:

$$\mathbf{M}_k = \{\bigcup_{r=1}^{p_i} M_{kr}\} = \{M_{k.1}, M_{k.2}, \ldots, M_{k.p_i}\}, \tag{6}$$

where $M_{kr}\ (k = \overline{1,q}, r = \overline{1,p_i})$ are metrics of the set k, p_i is metric's number of the k set.

Similarly, taking into account (6), the set (5) can be represented as:

$$\begin{gathered}\mathbf{M} = \{\bigcup_{k=1}^{q} \mathbf{M}_k\} = \{\bigcup_{k=1}^{q} \{\bigcup_{r=1}^{p_i} M_{kr}\}\} = \{\{M_{1.1}, M_{1.2}, ..., M_{1.p_1}\}, \\ \{M_{2.1}, M_{2.2}, ..., M_{2.p_2}\}, ..., \{M_{q.1}, M_{q.2}, ..., M_{q.p_q}\}\}, (k = \overline{1,q}, r = \overline{1,p_i}).\end{gathered} \tag{7}$$

Step 2.2. The value calculation of the ICT development and implementation metrics

The metrics, that describe ICT development and implementation in the CII sector (7), can be calculated according to (8):

$$\mathbf{I}_{DDL} = \frac{\sum_{k=1}^{q}\sum_{r=1}^{p_i} M_{kr} \times 100\%}{q \times \sum_{M_{kr}}^{max}},\ \sum_{M_{kr}}^{max} \neq 0,\ q \neq 0. \tag{8}$$

It should be noted, that since the metric $\mathbf{M_k}$ can have different dimensions, at this step, it also must be normalized using one of the known approaches.

Stage 3. Calculation of quantitative parameters, that describe the cybersecurity level of a CII sector

Based on (4) and (8), it is possible to calculate the quantitative parameters (9), that describe the cybersecurity level of a CII sector or a state:

$$\mathbf{I}_{ratio} = \mathbf{I}_{CS} - \mathbf{I}_{DDL} = \frac{\sum_{i=1}^{n}\sum_{j=1}^{m_i} P_{ij} \times 100\%}{\sum^{max}_{P_{ij}}} - \frac{\sum_{k=1}^{q}\sum_{r=1}^{p_i} M_{kr} \times 100\%}{q \times \sum^{max}_{M_{kr}}}, \sum^{max}_{P_{ij}} \neq 0, \sum^{max}_{M_{kr}} \neq 0, q \neq 0. \quad (9)$$

B. An experimental study of proposed method in aviation

According to [3. 10, 11], an example of the developed method usage for the civil aviation (CA) is showed below (Fig. 4). This sector includes to transportation and it is a part of CI for most of states (Table 2).

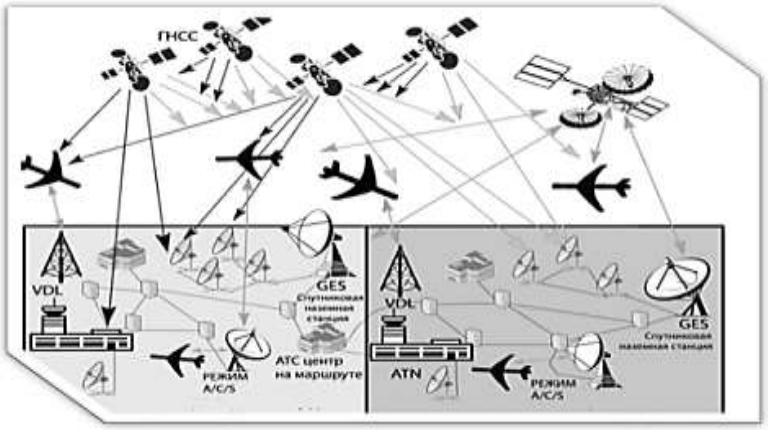

Fig. 4. Civil aviation ICT communications scheme

Stage 1. Determination of the metrics and cybersecurity index of a CII sector

Step 1.1. Formalization of the cybersecurity metrics

Taking into account [12, 14], for the cybersecurity metrics, for $n = 4$, $m_1 = 3, m_2 = 4, m_3 = 4, m_4 = 1$ the complete set of the cybersecurity metrics was defined as follows:

$$\mathbf{P} = \{\bigcup_{i=1}^{4} \mathbf{P}_i\} = \{\bigcup_{i=1}^{4} \{\bigcup_{j=1}^{m_i} P_{ij}\}\} = \{\{P_{PLC}, P_{THR}, P_{EDU}\},$$

$$\{P_{BASS}, P_{ESEV}, P_{EIDN}, P_{CIIP}\}, \{P_{CIRC}, P_{CRIS}, P_{CRIM}, P_{MIL}\}, \{P_{INT}\}\}, (i = \overline{1,n}, j = \overline{1,m_i}).$$

Step 1.2. The value calculation of index, that describes the CII sector cybersecurity level

According to (4):

$$\mathbf{I}_{CS} = \frac{(P_{PLC} + P_{THR} + P_{EDU} + P_{BASS} + P_{ESEV} + P_{EIDN} + P_{CIIP} + P_{CIRC} + P_{CRIS} + P_{CRIM} + P_{MIL} + P_{INT}) \times 100}{P^{max}_{PLC} + P^{max}_{THR} + P^{max}_{EDU} + P^{max}_{BASS} + P^{max}_{ESEV} + P^{max}_{EIDN} + P^{max}_{CIIP} + P^{max}_{CIRC} + P^{max}_{CRIS} + P^{max}_{CRIM} + P^{max}_{MIL} + P^{max}_{INT}} = 35\%.$$

Table 2. Industries of CI in accordance to ENISA

Industry / EU state	Energy	Water	Food	Health	Finance	Transport	Public admin.	ICT	Civil admin.	Space&Research
Austria	+	+	+	+	+	+	+	+	+	-
Cyprus	+	+	-	+	+	-	+	+	+	-
Czech Rep.	+	+	+	-	+	+	+	+	+	-
Estonia	+	+	+	+	+	+	+	+	+	-
Finland	+	+	+	+	+	+	+	+	-	-
France	+	+	+	+	+	+	+	+	+	+
Hungary	+	+	+	+	+	+	+	+	-	-
Lithuania	+	+	+	+	+	+	-	+	-	-
Netherlands	+	+	+	-	+	+	-	+	+	-
Poland	+	+	+	+	+	+	-	+	-	-
Slovenia	+	+	+	+	+	+	-	+	-	-
Spain	+	+	+	+	+	+	+	+	+	+
Switzerland	+	+	+	+	+	+	+	+	+	-
UK	+	+	+	+	+	+	-	+	-	-

Stage 2. Determination of the ICT development and implementation metrics of a CII sector

Step 2.1. Formalization of the ICT development and implementation metrics, that describe the ICT readiness and availability

Based on [12, 15], for $q = 2,\ p_1 = 3,\ p_2 = 10$ and considering (5-6), the set of ICT development and implementation metrics can be shown as:

$$\mathbf{M} = \{\bigcup_{k=1}^{q}\mathbf{M}_k\} = \{\{\bigcup_{k=1}^{q}\{\bigcup_{r=1}^{p_i}M_{kr}\}\} = \{\{M_{ACC}, M_{USE}, M_{SKI}\},$$

$$\{M_{POL}, M_{INN}, M_{RDN}, M_{AFF}, M_{BUS}, M_{GOV}, M_{SOC}, M_{SKIL}, M_{USE}, M_{IMP}\}\}, (k = \overline{1,q}, r = \overline{1,p_i}).$$

Step 2.2. The value calculation of the index, that describes the CII sector cybersecurity level

According to (8) the index can be calculated as:

$$\mathbf{I}_{DDL} = \frac{((M_{ACC} + M_{USE} + M_{SKI})}{(M_{ACC}^{max} + M_{USE}^{max} + M_{SKI}^{max})} +$$

$$+ \frac{(M_{POL} + M_{INN} + M_{RDN} + M_{AFF} + M_{BUS} + M_{GOV} + M_{SOC} + M_{SKI} + M_{USE} + M_{IMP}))\times 100\%}{(M_{POL}^{max} + M_{INN}^{max} + M_{RDN}^{max} + M_{AFF}^{max} + M_{BUS}^{max} + M_{GOV}^{max} + M_{SOC}^{max} + M_{SKI}^{max} + M_{USE}^{max} + M_{IMP}^{max}))} = 62,5\%$$

Stage 3. Calculation of the quantitative parameters, that describe the cybersecurity level of CA

Based on the results in Step 1.2, Step 2.2 and considering (9), quantitate parameters, that describe the cybersecurity level of CA can be calculated as follows:

$$\mathbf{I}_{ratio} = \mathbf{I}_{CS} - \mathbf{I}_{DDL} = 35\,\% - 62,5\,\% = -27,5\,\%.$$

The difference between $\mathbf{I}_{CS}$ and $\mathbf{I}_{DDL}$ indicators shows the correlation between the cybersecurity level and ICT development and implementation index. A positive result shows that cybersecurity level meets a sufficient level of ICT index for CA (or even overcame it), on the other hand, a negative result shows that cybersecurity level is not sufficient for current ICT index. The obtained result $\mathbf{I}_{ratio} = -27,5\,\%$ for CA shows that cybersecurity level should be improved.

4 Conclusion and future research study

Consequently, in this paper the modern methods, tools for assessing the cybersecurity level and their supporting instruments were analyzed. The research found that currently there are no comprehensive, flexible methods that can quantify the cybersecurity level of the CII sector. A method for determining the cybersecurity level has been developed. This method provides the sets of cybersecurity level and ICT development and implementation metrics in a linked lists view, also helps to calculate its relevant metrics. It allows to determine quantitative parameters, that describe the cybersecurity level of a particular industry or the state's CII in general. The developed method can be used to analyze a particular state's CII, determine the cybersecurity level, identify critical systems, which need to be protected from external and internal threats. For example, the proposed method can be applied for comparing the cybersecurity level before and after the implementation of certain ICT security measures.

References

1. 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.
2. The Law of Ukraine "On Basic Principles of Cyber Security of Ukraine" of 15.10.2017, №2163-VIII, Available Online, URL: http://zakon3.rada.gov.ua/laws/show/2163-19
3. V. Sydorenko, A. Polozhentsev, S. Gnatyuk, "The method of determining the security level of the critical information infrastructure", Academy of Engineering of Ukraine News, vol. 42, pp. 81- 89, 2017 (in Ukrainian).
4. Global Cybersecurity Index, Available Online, URL: https://www.itu.int/en/ITU-D/.
5. P. Black, K. Scarfone, M. Souppaya, "Cyber security metrics and measures", Wiley Handbook of Science and Technology for Homeland Security, vol. 4, 2010.
6. National Cyber Security Index, Available Online, URL: http://ncsi.ega.ee/ncsi-index/.
7. Network Readiness Index 2016. Available Online, URL: http://www3.weforum.org/docs/GITR/2014/GITR_OverallRanking_2016.

8. A. Nestrugin, Technique of automatic ranking of objects protection according to the level of potential danger on the example of oil refineries, pp. 77-84, 2014 (in Russian).
9. S. Evseev, “Methodology of Information Security Assessment of Automated Banking Systems of Ukraine”, Information Security, vol. 22, No.3, pp. 297-309, 2016 (in Ukrainian).
10. 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.
11. R. Odarchenko, V. Gnatyuk, S. Gnatyuk, A. Abakumova, Security Key Indicators Assessment for Modern Cellular Networks, Proceedings of the 2018 IEEE First International Conference on System Analysis & Intelligent Computing (SAIC), Kyiv, Ukraine, October 8-12, 2018, pp. 1-7.
12. T. Kormen, C. Leiserson, R. Rivest, C. Stein, “Algorithms: Construction and Analysis, 3rd Edition”, Moscow: LTD Williams, 1328 p., 2013.
13. Smirnov O., Kuznetsov A., Kiian A., Zamula A., Rudenko S., Hryhorenko V., “Variance Analysis of Networks Traffic for Intrusion Detection in Smart Grids”, 2019 IEEE 6th International Conference on Energy Smart Systems, Kyiv, Ukraine, 2019, P. 353-358.
14. Zhukov I.A. “Implementation of integral telecommunication environment for harmonized air traffic control with scalable flight display systems”, Aviation, 2010, №14 (4), 117-122.
15. Smirnov O., Kuznetsov A., Kavun S., Babenko B., Nakisko O., Kuznetsova K., “Malware Correlation Monitoring in Computer Networks of Promising Smart Grids’, 2019 IEEE 6th International Conference On Energy Smart Systems, Kyiv, Ukraine, 2019 P. 347-352.
16. Boyko N., Pylypiv O., Peleshchak Y., Kryvenchuk Y., Campos J.: Automated document analysis for quick personal health record creation. 2nd International Workshop on Informatics and Data-Driven Medicine. IDDM 2019. Lviv. p. 208-221. (2019)
17. Kryvenchuk Y., Mykalov P., Novytskyi Y., Zakharchuk M., Malynovskyy Y., Řepka M.: Analysis of the architecture of distributed systems for the reduction of loading high-load networks. Advances in Intelligent Systems and Computing. Vol.1080. p.759-550. (2020)
18. Kryvenchuk Y.,Vovk O., Chushak-Holoborodko A., Khavalko V., Danel R.: Research of servers and protocols as means of accumulation, processing and operational transmission of measured information. Advances in Intelligent Systems and Computing. Vol.1080. p.920-934. (2020)
19. Mishchuk O., Tkachenko R., Izonin I.: Missing Data Imputation through SGTM Neural-like Structure for Environmental Monitoring Tasks. Advances in Computer Science for Engineering and Education. ICCSEEA2019. Advances in Intelligent Systems and Computing. Springer, Cham, 2019, pp. 142-151
20. Fedushko S., Ustyianovych T.: Predicting Pupil’s Successfulness Factors Using Machine Learning Algorithms and Mathematical Modelling Methods. Advances in Intelligent Systems and Computing series, ICCSEEA 2019, AISC 938, vol. 938, pp. 625-636 (2020). https://doi.org/10.1007/978-3-030-16621-2_58
21. Korobiichuk I., Fedushko S., Juś A., Syerov Y.: Methods of Determining Information Support of Web Community User Personal Data Verification System. Automation 2017. ICA 2017. Advances in Intelligent Systems and Computing, vol. 550, pp. 144-150. Springer (2017). https://doi.org/10.1007/978-3-319-54042-9_13
22. Korobiichuk I., Syerov Y., Fedushko S.: The method of semantic structuring of virtual community content. Advances in Intelligent Systems and Computing, vol. 1044, pp. 11-18 (2020). https://doi.org/10.1007/978-3-030-29993-4_2
23. Shakhovska N., Shakhovska K., Fedushko S.: Some Aspects of the Method for Tourist Route Creation. Proceedings of the International Conference of Artificial Intelligence, Medical Engineering, Education (AIMEE2018). Advances in Artificial Systems for Medicine and Education II series, vol. 902, pp. 527-537 (2020) https://doi.org/10.1007/978-3-030-12082-5_48