ISSN 2311-4738 (print), ISSN 2413-3000 (online)

UDC 004.94 DOI: 10.20998/2413-3000.2018.1278.4

R. V. ARTIUKH, V. V. KOSENKO, O. V. MALYEYEVA, E. V. LYSENKO

MANAGING THE RISKS OF INFORMATION AND COMMUNICATION NETWORK IN THE CONTEXT OF PLANNING THE SECURITY OF CRITICAL INFRASTRUCTURE SYSTEMS

The subject matter of the article is information and communication networks of critical infrastructure systems. The goal of the work is to create an approach for strategic managing the security of critical infrastructure systems taking into account the risks of the information and communication network. The article deals with the following tasks: determining the procedure of strategic managing the security of critical infrastructure systems, identifying the risks of the information and communication network, assessing the importance and probability of partial network risks. The following methods are used: a systematic approach, cause-and-effect analysis, statistical methods. The following results are obtained: the diagram of multi-level risk management of critical infrastructure systems is developed; the diagram of the step-by-step method of information risks management is developed for increasing the safety of the system; the complex index is suggested for determining the category of information system security; probable variants of the full-factor environment of a set of values of the complex index elements and the corresponding categories of information systems security are analyzed; the process of adaptation of the system as an integral part of the selection and specification of measures for the risk reduction of the information and communication network is determined; the example of the risk assessment of the information and communication network for a software and hardware complex in the automated control system of technological processes is considered. Taking into account the categories of factors, a list of probable risks of the information and communication network and factors that cause them is given; the cause-and-effect diagram of "cause-risk-effect" interaction is created; the total effect of each factor on the final vertices of the diagram, that is possible effects, is calculated; the factors were grouped as the most important, quite important, of mean importance, and inconsiderable ones. Conclusions: On the basis of the analysis of information and communication network risks, appropriate security measures can be planned. The application of the obtained results contributes to enhancing the operational and informational security of critical infrastructure systems at the strategic planning stage.

Keywords: information and communication network, critical infrastructure systems, information security risk, security measures, modelling.

Р. В. АРТЮХ, В. В. КОСЕНКО, О. В. МАЛЄЄВА, Е. В. ЛИСЕНКО

УПРАВЛІННЯ РИЗИКАМИ ІНФОКОМУНІКАЦІЙНОЇ МЕРЕЖІ ПРИ СТРАТЕГІЧНОМУ ПЛАНУВАННІ БЕЗПЕКИ СИСТЕМ КРИТИЧНОЇ ІНРАСТРУКТУРИ

Предметом дослідження в статті є інфокомунікаційні мережі систем критичної інфраструктури. Мета роботи – створення підходу для стратегічного управління безпекою систем критичної інфраструктури з урахуванням ризиків інфокомунікаційної мережі. В статті вирішуються наступні завдання: визначення процедури стратегічного управління безпекою систем критичної інфраструктури, ідентифікація ризиків інфокомунікаційної мережі, оцінка важливості та ймовірності часткових ризиків мережі. Використовуються такі методи: системний підхід, причинно-наслідковий аналіз, статистичні методи. Отримано наступні результати: Побудовано схему багаторівневого управління ризиками систем критичної інфраструктури. Розроблено схему покрокового методу управління інформаційними ризиками для підвищення безпеки системи. Запропоновано комплексний показник для визначення категорії безпеки інформаційної системи. Проаналізовано можливі варіанти повного факторного простору множини значень елементів комплексного показника і відповідні їм категорії безпеки інформаційних систем. Визначено процес адаптації системи як невід'ємну частину вибору і специфікації заходів щодо парирування ризиків інфокомунікаційної мережі. Розглянуто приклад оцінки ризику інфокомунікаційної мережі для програмно-технічного комплексу у складі автоматизованої системи управління технологічними процесами. З урахуванням категорій факторів наведено перелік можливих ризиків інфокомунікаційної мережі із зазначенням причин їх виникнення. Побудовано причинно-наслідкову діаграму взаємодії «причини-ризики-наслідки». Розраховано загальний вплив кожного фактора на кінцеві вершини діаграми – можливі наслідки. Було класифіковано фактори на чотири групи: найбільш важливі, досить значні, середньої значущості, незначні. Висновки. На основі проведеного аналізу ризиків інфокомунікаційної мережі можна планувати відповідні заходи безпеки. Застосування отриманих результатів сприяє підвищенню функціональної та інформаційної безпеки систем критичної інфраструктури на етапі стратегічного планування.

Ключові слова: інфокомунікаційна мережа, системи критичної інфраструктури, інформаційний ризик, заходи безпеки, моделювання.

Р. В. АРТЮХ, В. В. КОСЕНКО, О. В. МАЛЕЕВА, Э. В. ЛЫСЕНКО

УПРАВЛЕНИЕ РИСКАМИ ИНФОКОММУНИКАЦИОННОЙ СЕТИ ПРИ СТРАТЕГИЧЕСКОМ ПЛАНИРОВАНИИ БЕЗОПАСНОСТИ СИСТЕМ КРИТИЧЕСКОЙ ИНРАСТРУКТУРЫ

Предметом исследования в статье являются инфокоммуникационные сети систем критической инфраструктуры. Цель работы - создание подхода для стратегического управления безопасностью систем критической инфраструктуры с учетом рисков инфокоммуникационной сети. В статье решаются следующие задачи: определение процедуры стратегического управления безопасностью систем критической инфраструктуры, идентификация рисков инфокоммуникационной сети, оценка важности и вероятности частичных рисков сети. Используются следующие методы: системный подход, причинно-следственный анализ, статистические методы. Получены следующие результаты: построена схема многоуровневого управления рисками систем критической инфраструктуры. Разработана схема пошагового метода управления информационными рисками для повышения безопасности системы. Предложен комплексный показатель для определения категории безопасности информационной системы. Проанализированы возможные варианты полного факторного пространства множества значений элементов комплексного показателя и соответствующие им категории безопасности информационных систем. Определен процесс адаптации системы как неотъемлемая часть выбора и спецификации мероприятий по парированию рисков инфокоммуникационной сети. Рассмотрен пример оценки риска инфокоммуникационной сети для программно-технического комплекса в составе автоматизированной системы управления технологическими процессами. С учетом категорий факторов приведен перечень возможных рисков инфокоммуникационной сети с указанием причин их возникновения. Построена причинно-следственная диаграмма взаимодействия «причины-риски-последствия». Рассчитано общее влияние каждого фактора на конечные вершины диаграммы - возможные последствия. Были классифицированы факторы на четыре группы: наиболее важные, весьма значительные, средней значимости, незначительные. Выводы. На основе проведенного анализа рисков инфокоммуникационной сети можно планировать соответствующие меры безопасности. Применение полученных результатов способствует

повышению функциональной и информационной безопасности систем критической инфраструктуры на этапе стратегического планирования.

Ключевые слова: инфокоммуникационные сети, системы критической инфраструктуры, информационный риск, методы безопасности, моделирование.

Introduction. Modern information and communication networks (ICN) which ensure data exchange in critical infrastructure systems (CIS) are being constantly improved. New network technologies emerge; there is the tendency of their "convergence". Therefore, the task to provide a quality information exchange is becoming more and more sophisticated. ICN risks at the stage of strategic managing CIS security should be systematically analyzed and assessed to solve this task.

There exist two causes of risks for critical information systems – external and internal ones. External causes are industrial accidents, terrorist and criminal activities, cyber-attacks, natural disasters, and so on [1]. Internal causes are linked to computing and information technology services. Also, CIS information security can be violated by a negative impact of human and technical factors. At the stage of strategic planning of CIS security, the methods of risk forecasting, establishing, avoiding, and overcoming should be used.

Problem analysis. At present, the issues of ICN protection are regulated by the standards of the Information Technical Laboratory (ITL) at the National Institute of Standards and Technology (NIST) [2]. Ross R. [3] and Paulsen S. [4] considered the issues of vulnerability analysis and risk assessment of ICN in their works. The problems of information security and methods of information activity protection are reviewed by such authors as Karpov E. [5], Gornitskaya D. [6], Shatovskaya T. [7], Furmanov A. [8], Boyarchuk A. [9].

Network attacks, threats to information security [10] are classified and the ways of their detection [11] are determined.

The issues of making decisions on information security management of networks are considered in the works by Voropaeva V. [10], Sklyar V. [12].

At present, most scientific developments are being conducted in the field of assessing the ICN information risk without taking into account its causes, factors, and interaction with other types of ICN risks. Apart from this, the causes and risk factors, which are determined as threats to the project objectives are not classified.

The security of information resources and information environment in CIS are traditionally considered as [13]:

- a set of tools and technological methods that ensure protecting the components of information environment;
- technologies of risk minimization for the components and resources of information environment;
- a complex of procedural, logical and physical measures that are aimed at countering the threats to the information resource and components of the information environment.

The security measures offered for information systems are designed to protect the confidentiality, integrity, and availability of information that is processed, stored and transmitted in these systems and meet a number of certain security requirements. The selection and implementation of security measures for ICN are important tasks that can have a significant impact on the operation and survivability of CIS. The selection of these measures is important for the efficient risk management process that is, for identifying, managing and counteracting the information risk [14].

Information risks associated with information security are the risks that result from the loss of privacy, integrity or availability of information, and they have potentially adverse impacts on the CIS operation.

A realistic risk assessment at the strategic planning stage requires understanding the threats and vulnerabilities within the ICN and probability and potential of adverse impacts [15].

The goal of the article is to develop the approach for strategic managing CIS security taking into account ICN risks, which involves solving the following tasks:

- determining the procedures for strategic managing the security of CIS,
- identifying the risks of ICN,
- assessing the importance and probability of ICN partial risk.

Problem solution. Strategic risks management is carried out on three levels to ensure interlevel and intralevel interaction of all CIS components (Fig. 1):

- on the level of critical infrastructure system,
- on the level of CIS functional tasks,
- on the level of the processes in information and communication network.

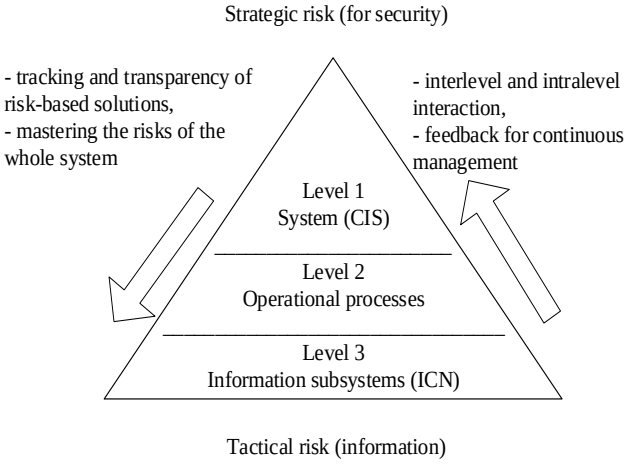

Fig. 1 – Multilevel management of CIS risks

Fig. 2 shows the diagram of CIS security lifecycle. Consequential processes of managing information security risks are presented at the first three stages [16]:

1) categorizing information system according to safety requirements,

2) selecting a basic set of security measures, based on the results of security categorization;

3) implementing and documenting security measures.

While preparing for selecting and determining appropriate measures to counteract information risks in ICN and corresponding CIS, the level of severity and sensitivity of the information to be processed, stored or transmitted over the network should be initially determined.

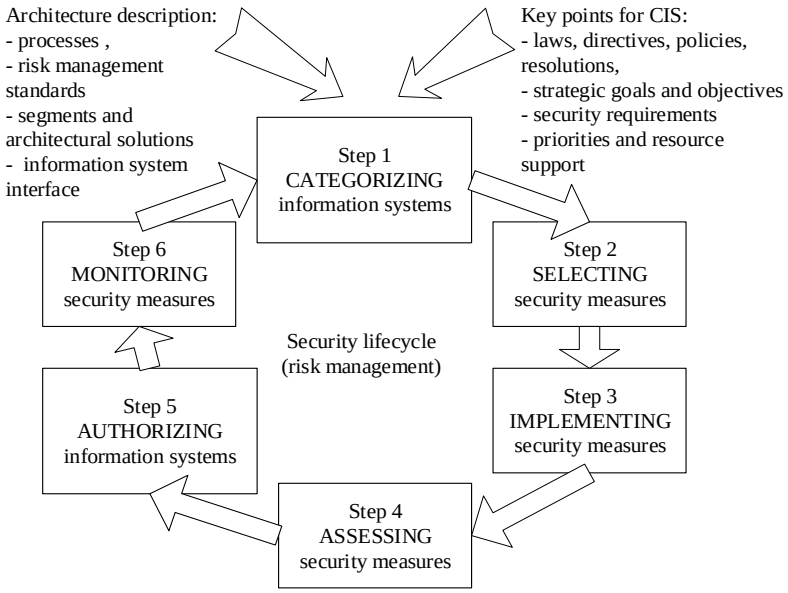

Fig. 2 – The diagram of step-by-step method of information risks management to ensure the system security

The safety categorization standard is based on the concept of identifying potentially adverse impacts on ICN.

Complex factor for determining the safety category (SC) of the information system is represented by a tuple of values:

$$SC = \{KF, IN, AC\},$$

where *KF* is the impact of the characteristic "information confidentiality" on the system security, *IN* is the impact of the characteristic "information integrity", *AC* is the impact of the characteristic "information availability".

The degrees of impact can be expressed linguistically as "low", "moderate", "high".

Variants of the full-factor environment of a set of values of the mentioned indicators and categories of information system security corresponding to them are given in table 1.

Table 1 – Categories of system security taking into account the degrees of impact of the basic information characteristics

№	KF	IN	AC	CIS categories
1	2	3	4	5
1	"low"	"low"	"low"	The system of low impact
2	"low"	"low"	"moderate"	The system of moderate impact
3	"low"	"moderate"	"low"	
4	"low"	"moderate"	"moderate"	
5	"moderate"	"low"	"low"	
6	"moderate"	"low"	"moderate"	
7	"moderate"	"moderate"	"low"	
8	"moderate"	"moderate"	"moderate"	
9	"low"	"low"	"high"	The system of high impact
10	"low"	"moderate"	"high"	
11	"low"	"high"	"low"	
12	"low"	"high"	"moderate"	
13	"low"	"high"	"high"	
14	"moderate"	"low»	"high"	
15	"moderate"	"moderate"	"high"	
16	"moderate"	"high"	"low"	
17	"moderate"	"high"	"moderate"	
18	"moderate"	"high"	"high"	

The end of the Table 1

1	2	3	4	5
19	“high”	“low”	“low”	The system of high impact
20	“high”	“low”	“moderate”	
21	“high”	“low”	“high”	
22	“high”	“moderate”	“low”	
23	“high”	“moderate”	“moderate”	
24	“high”	“moderate”	”high”	
25	“high”	“high”	“low”	
26	“high”	“high”	“moderate”	
27	“high”	“high”	“high”	

The low-impact system is determined as an information system in which all three objectives of security are low.

The system of moderate impact is an information system in which at least one of these objectives is moderate and there is no security objective greater than that of moderate.

A high-impact system is an information system in which at least one security objective is high.

The following factors should be considered while selecting the basic sets of measures that counteract risks:

1) the environment of ICN operation;

2) operation type used in CIS;

3) operational processes in ICN;

4) types of threats aimed at CIS, the processes of its operation;

5) types of information processed, stored and transmitted over the ICN.

The peculiarities of ICN operation should also be taken into account:

- there are insider threats in CIS;
- classified data are processed, stored and transmitted over the network;
- threats for CIS are continuously evolving;
- data require specialized protection based on the state legislative system, directives, standard regulations or policies;
- CIS should interact with other systems thought different security domains.

When a set of basic measures that counteract risks is selected, the process of adaptation should take place in order to change the measures in accordance with CIS specific conditions. The process of adaptation involves:

- identifying and determining general measures for counteracting risks in the initial set of basic measures;
- applying the system features to the rest of basic measures;
- selecting compensatory measures, if necessary;
- assigning specific values of parameters of measures by explicit assigning or selecting;
- supplementing basic sets with additional measures and improving them, if necessary;
- providing additional specific information for implementing measures to counteract risks, if necessary.

The process of adaptation, being an integral part of selecting and specifying measures to counteract risks, is a part of managing ICN risks.

Taking into account external conditions requires determining the factors of their impact. Therefore, attention should be paid to the following features of data handling:

1. The mobility of hardware environment. If CIS works in mobile environments, the basic set of measures to counteract risks should be appropriately adapted in order to take into account differences in mobility and the availability of specific nodes in a distributed system.

2. Data transmission and bandwidth. This is important for systems that have limited or sporadic bandwidth.

3. Limited operability of systems or system components.

4. Instability of information and systems for some applications and environments where user information is limited in time. Information services can also be unstable due to virtualization technologies for temporary installations of operating systems and applications.

5. Open access. Security measures, such as determining unsuccessful login attempts, remote access, identification and authentication, managing authenticators can be necessary for system personnel who guide and support information systems that provide websites and open access services.

Restrictions on the use of information systems and specific information technologies can be the only practical actions that can be taken in some situations.

The protection of the information resource involves the impossibility of its loss due to failures of the components of the information environment. Therefore, ensuring the safe operation of the information resource requires:

- providing a trusted computing base that ensures the continuity of information environment operation,
- developing a system of counteraction and prevention of threats to the information resource.

The technology of adaptive security systems that are oriented toward active resistance to security threats is efficient for ICN [17, 18]. The implementation of this approach requires analyzing risks, developing the security policy, using traditional procedures of protection, and implementing countermeasures to counteract threats, ongoing safety audits and monitoring the state of the system, which should enable responding to security risks efficiently.

The concrete implementation of these mechanisms for ICN information security and CIS survivability involves using both available technical and technological solutions and tools, as well as developing new methods. Implementing the mechanisms of increasing CIS survivability requires the analysis of risks, taking into account its features and operational objectives.

Let us consider the example of assessing an ICN risk for software and hardware complexes (S & H C) being a part of the Automated Control System for processing household wastes and recycling. Taking into account the categories of factors (technical, process, human, external), the list of possible ICN risks and their causes is given in Table 2.

In order to quantify risks impact on ICN operation, it is suggested to use the method based on the theory of causality [15, 19].

The cause-and-effect diagram is a sign-oriented graph; the key elements of the simulation object are arranged in vertices and connected with arcs that represent cause-and-effect interrelations among them. These relationships characterize the degree (power) of elements impact on one another:

$$B = \left\{ b_{i,j},\ i = 1...n,\ j = 1...m \right\},$$

$$C = \left\{ c_{j,k},\ j = 1...m, k = 1...h \right\}.$$

Table 2 – Reasons and partial risks of ICN in S&H C

Categories of factors	Causes of risks	Partial risks
Internal risks		
Technical factors	P_{11} – lack of capacity P_{12} – lack of productivity	R_1 – risk of hardware failure
	P_{21} – low-level management of configuration P_{22} – low-quality management of changes P_{23} – incorrect security settings P_{24} – unsafe programming practices P_{25} – inappropriate testing	R_2 – risk of software failure
	P_{31} – design problems P_{32} – integration problems P_{33} – system complexity	R_3 – risk of error in network design
Process factors	P_{41} – inadequate technological process P_{42} – incorrect data flows P_{43} – inappropriate problem escalation P_{44} – inefficient tasks transfer	R_4 – risk of error in network processes (design and performance)
	P_{51} – no status monitoring P_{52} – no periodic analysis P_{53} – inappropriate processing	R_5 – risk of error in processes control
Human factor	P_{71} – accidental mistake P_{72} – ignorance P_{73} – nonobservance of instructions	R_7 – risk of unintentional actions
External risks		
External factors	P_{101} – fire	R_{10} – risk of disaster
	P_{131} – problems with power supply	R_{13} – risk of poor-quality service

The elements of the mentioned sets (b_{ij} is the impact degree of the ith factor on the formation of the jth risk and c_{jk} is the impact degree of the jth risk on the kth consequent effect) can be determined by integer values according to the ten-point scale.

Let us draw a cause-and-effect diagram of interrelation “causes-risks-effects” [20] (fig. 4).

Values b_{ij} and c_{jk} can be determined by objective method (according to statistics) or by subjective one (according to expert analysis) of the basis of previous experience (Tables 3, 4).

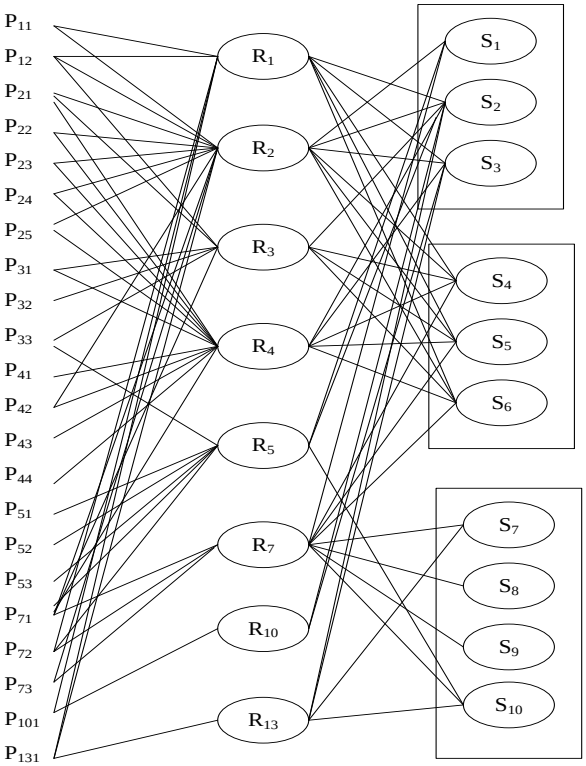

Fig. 4 – Cause-and-effect diagram of risks of ICN in S&H C

Table 3 – Score of factors impact on ICN partial risks

causes	Partial risks							
	hardware failure	software failure	error in network design	error in network processes	error in processes control	unintentional actions	disaster	poor-quality service
P_{11}	9	5	0	0	0	0	0	0
P_{12}	10	4	2	0	0	0	0	0
P_{21}	0	5	3	2	0	0	0	0
P_{22}	0	4	0	1	0	0	0	0
P_{23}	0	10	0	8	0	0	0	0
P_{24}	0	2	0	1	0	0	0	0
P_{25}	0	3	0	1	0	0	0	0
P_{31}	0	0	5	2	0	0	0	0
P_{32}	0	0	4	0	0	0	0	0
P_{33}	0	0	3	0	2	0	0	0
P_{41}	0	0	0	4	0	0	0	0
P_{42}	0	6	0	8	0	0	0	0
P_{43}	0	0	0	4	0	0	0	0
P_{44}	0	0	0	8	0	0	0	0
P_{51}	0	0	0	0	6	0	0	0
P_{52}	0	0	0	0	6	0	0	0
P_{53}	0	0	0	0	5	0	0	0
P_{71}	1	2	1	2	3	6	0	0
P_{72}	0	0	0	0	1	2	0	0
P_{73}	0	2	0	0	2	3	0	0
P_{101}	5	0	0	0	0	0	7	0
P_{131}	4	3	0	2	0	0	0	6

Table 4 – Score of risks impact on probable effects

Partial risks	Network indices (risks effects)									
	Reliability		Survivability	Productivity			Security			
	S_1	S_2	S_3	S_4	S_5	S_6	S_7	S_8	S_9	S_{10}
Hardware failure	0	10	9	7	7	7	0	0	0	0
Software failure	10	7	1	4	6	5	0	0	0	0
Error in design	0	5	0	8	8	4	0	0	0	0
Error in processes	0	4	1	8	8	3	0	0	0	0
Error in control	2	5	0	0	0	0	0	0	0	2
Unintentional actions	6	2	0	3	3	1	4	2	2	8
Disaster	0	5	3	0	0	0	0	0	0	0
Poor-quality service	0	3	1	0	0	0	1	0	0	2

The total impact of each factor (cause) on the final vertices of the diagram – probable effects (table 5) was calculated using the following formula:

$$P(S_k) = \sum_i \sum_j b_{ij} c_{jk} \ .$$

Table 5 – Calculation of significant factors and probable effects

Factors	Basic network parameters										Total value	Standard value (a')
	Reliability		Survivability	Productivity			Security					
	S_1	S_2	S_3	S_4	S_5	S_6	S_7	S_8	S_9	S_{10}		
P_{11}	50	125	86	83	93	88	0	0	0	0	525	0,109
P_{12}	40	138	94	102	110	98	0	0	0	0	582	0,121
P_{21}	50	58	7	60	70	43	0	0	0	0	288	0,060
P_{22}	40	32	5	24	32	23	0	0	0	0	156	0,032
P_{23}	100	102	18	104	124	74	0	0	0	0	522	0,108
P_{24}	20	18	3	16	20	13	0	0	0	0	90	0,019
P_{25}	30	25	4	20	26	18	0	0	0	0	123	0,025
P_{31}	0	33	2	56	56	26	0	0	0	0	173	0,036
P_{32}	0	20	0	32	32	16	0	0	0	0	100	0,021
P_{33}	4	25	0	24	24	12	0	0	0	4	93	0,019
P_{41}	0	16	4	32	32	12	0	0	0	0	96	0,020
P_{42}	60	74	14	88	100	54	0	0	0	0	390	0,081
P_{43}	0	16	4	32	32	12	0	0	0	0	96	0,020
P_{44}	0	32	8	64	64	24	0	0	0	0	192	0,040
P_{51}	12	30	0	0	0	0	0	0	0	12	54	0,011
P_{52}	12	30	0	0	0	0	0	0	0	12	54	0,011
P_{53}	10	25	0	0	0	0	0	0	0	10	45	0,009
P_{71}	62	64	13	57	61	33	24	12	12	54	392	0,081
P_{72}	14	9	0	6	6	2	8	4	4	18	71	0,015
P_{73}	42	30	2	17	21	13	12	6	6	28	177	0,037
P_{101}	0	85	66	35	35	35	0	0	0	0	256	0,053
P_{131}	30	87	47	56	62	49	6	0	0	12	349	0,072
Total impact	576	1074	377	908	1000	645	50	22	22	150	4824	1
Standard coefficient (p')	0,119	0,222	0,078	0,188	0,207	0,134	0,104	0,005	0,005	0,031	1	
	0,341		0,078	0,529			0,145				1	

The table shows total values of each cause (factor), and their specified values.

Bottom lines of the table contain the total impact for each probable effect and their standard values, which can

be considered as the probability of each effect. Moreover, the degree of risk for basic parameters of network operation is calculated.

According to the results presented in the table the factors were grouped as the most important (a' > 0,072), quite important (0,045 < a' < 0,072), of mean importance (0,045 < a' < 0,072), inconsiderable (0,019 < a' < 0,045); that is, the most important factors (causes) of risks are the following:

- of capacity
- lack of productivity
- incorrect security settings,
- incorrect data flows,
- accidental mistake.

In addition, it is possible to conclude that the most vulnerable ICN element is "productivity" (p'=0,53); the second vulnerable parameter is "reliability" (p'=0,34).

According to the results of the analysis of risks (matching important factors to their effects), appropriate security measures were suggested.

Conclusions. The task of ensuring CIS information security taking into account the risks of the information and communication network is considered. The main causes of threats for CIS operation are determined. The strategic risk management process is suggested to be carried out on three levels with the purpose of effective interlevel and intralevel interaction of all components of the system. The diagram of the step-by-step method of safety management of CIS is developed.

The suggested method for quantifying ICN risks is based on the method of cause-and-effect analysis and enables taking into account both factors causing it and probable effects. Identifying potential losses becomes possible, as well as taking measures to manage the risks of ICN operation.

The cause-and-effect diagram was developed as an example of ICN, the matrices of impact coefficients were determined, which resulted in calculating the levels of factor significance and the probability of their effects. The most vulnerable network characteristics were detected. As a result, some measures to counteract partial risks were formulated.

References

1. *Australian Government Critical Infrastructure Resilience Strategy*, available at : http://www.tisn.gov.au/
2. Cichonski P., Millar T., Grance T., Scarfone K. *Computer Security Incident Handling Guide.* National Institute of Standards and Technology, 2012. 79 p.
3. Ross R. *Guide for Conducting Risk Assessments*. National Institute of Standards and Technology, 2012. 95 p.
4. Paulsen S., Boens J. *Summary of the Workshop on information and communication technologies supply chain risk management*. National Institute of Standards and Technology. 2012. 21 p.
5. Karpov É. A., Kosareva Y. N., Kobzeva A. H. Otsenka ynformatsyonnykh ryskov po metodyke SRAMM [Information Risk Assessment by the CAMM methodology]. *Visnyk NTU «KHPI». Seriya: Aktual'ni problemy upravlinnya ta finansovo-hospodars'koyi diyal'nosti pidpryyemstva* [Bulletin of the NTU "KhPI". Series: actual problems of property management and financial and economic activity of the enterprise]. 2013, no. 52 (1025), pp. 69-72.
6. Hornyts'ka D. A., Zakharova M. V., Kladochnyy A. I. *Systema analizu ta otsinky rivnya zakhyshchenosti derzhavnykh informatsiynykh resursiv vid sotsiotekhnichnykh atak* [System of analysis and estimation of the level of protection of state information resources from sociotechnical attacks]. National Aviation University. 5 p.
7. Shatovs'ka T. B., Kamenyeva I. V. Doslidzhennya efektyvnosti zastosuvannya BDD-freymvorkiv u testuvanni bezpeky web-oriyentovanoho prohramnoho zabezpechennya [The study of the effectiveness of the use of BDD-frameworks in the testing of security of web-based software]. *Visnyk NTU «KHPI». Seriya: «Mekhaniko-tekhnolohichni systemy ta kompleksy»* [Bulletin of the NTU "KhPI". Series: "Mechanic-technological systems and complexes"]. 2015, no. 21 (1130), pp. 69-75.
8. Furmanov A. A., Lakhizha I. N., Kharchenko V. S. Modeling of service-oriented service-oriented architectures in attacks using vulnerabilities [Modelirovaniye garantosposobnykh servis-oriyentirovannykh arkhitektur pri atakakh s ispol'zovaniyem uyazvimostey]. *Radiotechnical and computer systems*. 2009, no. 7 (41), pp. 65-69.
9. Boyarchuk A. V., Kharchenko, V. S. ed. *Bezopasnost' kriticheskikh infrastruktur: matemati-cheskiye i inzhenernyye metody analiza i obespecheniya* [Safety of critical infrastructures: mathematical and engineering methods of analysis and provision]. National Aerospace University "Kharkiv Aviation Institute"(KhAI), 2011. 641 p.
10. Voropayeva V. Ya., Shcherbov I. L., Khaustova E. D. Upravlinnya informatsiynoyu bezpekoyu infor-matsiyno–telekomunikatsiynykh system na osnovi modeli "PLAN–DO–CHECK–ACT" [Information Security Management of Informational-Telecommunication Systems on the basis of the model "PLAN-DO-CHECK-ACT"]. *Scientific works of DonNTU. Series: Computing and Automation*. 2013, no. 2 (25). 7 p.
11. Prikhod'ko T. A. Issledovaniye voprosov bezopasnosti lokal'nykh setey na kanal'nom urov-ne modeli OSI [Investigation of the security of local networks on the channel level of the OSI model]. *Scientific publications of DonNTU Computer Engineering Department*. 2011. 4 p.
12. Sklyar V. V., Kharchenko V. S. ed. *Metodologiya risk-analiza funktsional'noy bezopasnosti informatsionno-upravlyayushchikh sistem. Bezopasnost' kriticheskikh infrastruktur: matematicheskiye i inzhenernyye metody analiza i obespecheniya* [Methodology of risk analysis of functional safety of information-control systems. Security of critical infrastructures: mathematical and engineering methods of analysis and security]. National Aerospace University "Kharkiv Aviation Institute"(KhAI), 2011, section 12, pp. 360-408.
13. Domarev V. V. *Bezopasnost' informatsionnykh tekhnologiy. Metodologiya sozdaniya sistem zashchity* [Information Technology Security. Methodology for creating protection systems]. Kyiv: OOO "TID "DS", 2001. 688 p.
14. Kosenko V. Principles and structure of the methodology of risk-adaptive management of parameters of information and telecommunication networks of critical application systems. *Innovative technologies and scientific solutions for industries*. Kharkiv. 2017, no. 1 (1), pp. 45-51.
15. Malyeyeva O. V., Sytnik N. I. Analiz vzaimodeystviya vnutrennikh i vneshnikh riskov na osno-ve prichinno-sledstvennoy diagrammy [Analysis of the interaction of internal and external risks on the basis of the cause-effect diagram]. *Radiotechnical and computer systems*. 2007, no. 1. pp. 73-76.
16. Kosenko V. V., Persiyanova E. Yu., Timofyeyev V. O. ed., Chumachenko I. V. ed. Adaptyvne uprav-linnya ryzykamy informatsiynoyi merezhi dlya informatsiynoyi bezpeky system krytychnoyi infrastruktury [Adaptive risk management of the information network for information security of critical infrastructure systems]. *Mathematical models and new technologies of management of economic and technical systems: monograph*. Kharkiv, KNURE, 2017, pp. 284-301.
17. Budushcheye informatsionnoy bezopasnosti: integrirovannaya sistema okhrany perimetra [The future of information security: an integrated perimeter security system]. *Zashchita informatsii. Konfident* [Data protection. Confident]. 2001, no. 2, pp. 56-59.
18. Il'in V. Ye., Komarovich V. F., Osadchiy A. I. Analiz problemy adaptivnoy zashchity IVS v usloviyakh informatsionnogo protivoborstva [Analysis of the problem of adaptive protection of IVS

in the context of information confrontation]. *Zashchita informatsii. Konfident* [Data protection. Confident]. 2002, no. 4-5, pp. 99-107.
19. Kheys D. *Causal analysis in statistical studies*. Moscow: Finance and Statistics. 1981. 255 p.
20. Kosenko V., Malyeyeva O., Persiyanova E., Rogovyi A. Analysis of information-telecommunication network risk based on cognitive maps and cause-effect diagram. Advanced Information Systems. 2017, vol. 1, no. 1, pp. 49-56. doi: 10.20998/2522-9052.2017.1.09

Received 05.12.2017

Відомості про авторів / Сведения об авторах / About the Authors

Артюх Роман Володимирович **(*Артюх Роман Владимирович, Artiukh Roman*)** – кандидат технічних наук, Державне підприємство "Південний державний проектно-конструкторський та науково-дослідний інститут авіаційної промисловості", директор, м. Харків, Україна; e-mail: roman.artyuh77@gmail.com; ORCID: 0000-0002-5129-2221.

Косенко Віктор Васильович **(*Косенко Виктор Васильевич, Kosenko Viktor*)** – кандидат технічних наук, доцент, Державне підприємство "Харківський науково-дослідний інститут технології машинобудування", директор, м. Харків, Україна; e-mail: kosv.v@ukr.ua; ORCID: 0000-0002-4905-8508.

Малєєва Ольга Володимирівна **(*Малеева Ольга Владимировна, Malyeyeva Olga*)** – доктор технічних наук, професор, Національний аерокосмічний університет імені М. Є. Жуковського "ХАІ", професор кафедри інформаційні обчислювальні системи, м. Харків, Україна; e-mail: omaleyeva@ukr.net, ORCID: 0000-0002-9336-4182.

Лисенко Едуард Вікторович **(*Лысенко Эдуард Викторович, Lysenko Eduard*)** – доктор економічних наук, професор, Харківський національний університет міського господарства ім. О.М. Бекетова, професор кафедри прикладної математики та інформаційних технологій, м. Харків, Україна; e-mail: lysenko_2018@ukr.net; ORCID: 0000-0002-9742-4867.