UDC 004.94 **doi: 10.20998/2522-9052.2017.1.09**

V. Kosenko[1], O. Malyeyeva[2], E. Persiyanova[3], A. Rogovyi[4]

[1] SE "Kharkiv Scientific-Research Institute of Mechanical Engineering Technology", Kharkiv, Ukraine
[2] National Aerospace University – Kharkiv Aviation Institute, Kharkiv, Ukraine
[3] SE "Southern National Design & Research Institute of Aerospace Industries", Kharkiv, Ukraine
[4] National Technical University "Kharkiv Polytechnic Institute", Kharkiv, Ukraine

ANALYSIS OF INFORMATION-TELECOMMUNICATION NETWORK RISK BASED ON COGNITIVE MAPS AND CAUSE-EFFECT DIAGRAM

The **subject matter** of the article is the processes of analysis and risk assessment of information and telecommunications networks. The **aim** is to reduce the potential losses caused by the risks of information and telecommunications network (ITN) functioning by taking timely risk management measures. The **objectives** are: classification of ITN risks, highlighting the main factors and causes of their occurrence; formation of a systematic presentation of risks to identify their manifestation and consequences; development of the method for assessing the influence of the risk and private risk on probable consequences; obtaining a quantitative risk assessment of ITN. The **methods** used are: system analysis of risks, method of cognitive maps, cause-and-effect analysis. The following **results** are obtained: classification of private risks of ITN according to the reasons and the factors of their occurrence is made; the negative consequences affecting the basic characteristics of the operation of ITN are defined; as a result, the structural system model of ITN risks is formed, in which the relationships between the elements of the main aspects of risk are shown; the method based on the theory of causal analysis is suggested in order to quantify the risk impact on ITN functioning. The risk model is based on the construction and analysis of probabilistic or fuzzy cognitive maps. Experts estimate the level of influence of private risks on the characteristics of the network in order to make decisions on risk management. The generalized structure of the cause-effect diagram of the risk factors, manifestation and consequences is developed; on ITN basis the method for quantifying the probability of risk consequences is suggested. The quantitative assessment of probable malfunctioning of the network that is determined by a specific effect (taking into account ITN probability), which is caused by private risks is also made. **Conclusion.** The suggested approach for quantitative assessment of ITN risk is based on the method of cause-and-effect analysis and enables taking into account both the factors causing it and probable consequences. The obtained results can be used to determine probable failures and losses in ITN functioning on the basis of the information about the degree of risk factors effects, risk events and consequences, and the cause-effect relationships between them. Thus, potential losses can be identified; measures to manage the risks of ITN functioning can be taken.

Keywords: information-telecommunication network, risk factors, consequences, cause-effect diagram, influence factors.

Introduction

Under continuously improving concepts of developing information and telecommunication networks (ITN), creating new network technologies and growing demand for services, there is a trend of their "convergence", i.e. combining into more complex structures and technologies. There is an interpenetration of information environments different in occurrence and principles of the work.

The European Commission defined the convergence in telecommunications as the ability of various network platforms to provide the same set of services or the combination of end devices, such as a telephone, a personal computer and a TV receiver in the form of a single terminal [1].

This term includes all the changes in telecommunications that relate to the development and integration of services and networks, the replacement of old technologies with new ones, and so on. Information and telecommunication components are connected on the basis of a multiservice platform.

Therefore, to provide high-quality transport services while transferring information is becoming increasingly difficult. In order to solve this problem system analysis and risk assessment of information and telecommunication networks (ITN) for further evaluation of damage and decision-making as for risk counter should be performed.

The analysis of the problem and formulation of the task

The information security of telecommunication systems is subjected to a wide range of threats: from virus infection, which can be handled locally, to regulatory collisions that require the work of legislative and law enforcement authorities. Hence, there are risks that can have a negative impact on ITN performance.

Today, ITN protection is regulated by the standards of the Technical Laboratory of Information (ITL) at the National Institute of Standards and Technology (NIST) [2].

The work of Ross R. [3] and Paulsen S. [4] is devoted to the analysis of vulnerability and risk assessment of ITN. The problems of information security and methods of protecting information activity are considered by such authors as Zadirak V. [5], Gornitnkaya D. [6], Buryachok V. [7], Furmanov A. [8], Boyarchuk A. [9]. The classification of network attacks, threats to information security [10] has been made and methods for their detection have been determined [11] so far. The issues of decision-making as for the management of information security of networks are considered in the works of Voropaev V. [10], Sklyar V. [12].

Currently, the majority of scientific developments are conducted in the field of information risk (IR) assessment without system accounting of ITN causes,

factors and interaction with other types of ITN risks. In addition, there is no classification of the causes and risk factors identified as threats.

Therefore, this article deals with the development of a systematic presentation of the ITN risks to identify the relationship between the factors that cause risks, risks manifestation and their consequences as well as with the development of the approach that enables assessing the impact of risks on ITN functioning.

Task solution

In the systemic risk model, we define the basic categories to identify the relationships between their elements (Fig. 1).

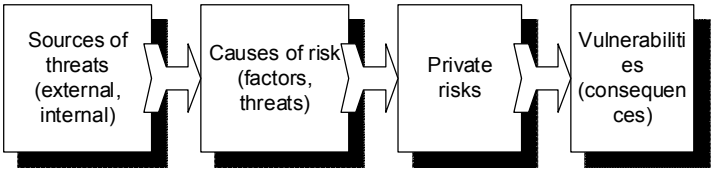


Fig. 1. Main categories of risk analysis

The procedure of analysis and risk assessment presupposes the following stages:

- analysis of risk factors (potential sources of threats),
- listing ITN key risks, which can significantly affect ITN functioning,
- analysis of the consequences of of risk events,
- analysis of cause-effect relationships between elements of the categories of the system risk model,
- assessment of the probability and cost of ITN risk.

To analyze risk factors the types of ITN risks should be classified. According to the reasons of their occurrence, the ITN risks can be divided into two main categories:

- objective risks arising as a result of disruptions in the operation of information transmission channels,
- subjective risks caused by the loss of information and ITN misuse.

The ITN risks can also be classified as internal and external factors as for their occurrence. Here, the period of ITN life cycle (LC) can be taken into account. Risks arise both at the stage of design (or modernization), and at the stage of operation (while transferring data and controlling processes).

Taking into account the factors of their occurrence, we group the internal risks as:

- risks related to the provision of services (including those with peak loads) that arise during the operation phase,
- risks of fraud, which may be the result of illegal connection, theft of traffic, etc. that arise during the operational phase,

External risks (due to the influence of external environment) include:

- part of the risks of developing and introducing new services that are related to the development of networks and the construction of communication facilities, which can be a consequence of the breakdown of terms by contract organizations, lack of funds, etc., and risks arise at the stage of modernization,
- the risks caused by the legislation imperfection that can arise at any stage of the LC.

Taking into account the categories of factors (technical, process, human, external), we list the possible ITN risks, indicating the causes of their occurrence (Table 1).

Technical factors cause risks associated with improper or unexpected function of ITN technological properties. Factors of the process cause risks associated with the problems of performing internal processes, as a result of which they do not work as expected. The human factor causes risks associated with problems caused by actions (or inaction) of people in certain situations; both insiders and external users of the network may cause problems. External factors are the causes of the risks associated with external, uncontrolled events. In most cases, such events cannot be anticipated and planned [13].

Risks have negative consequences that negatively affect the following main characteristics of ITN functioning:

1. Network performance, which is related to the concepts of reliability and survivability. The differences in these concepts are due to the causes and factors of the risks. Reliability of the communication network covers the influence of the main internal factors – accidental failures of technical means caused by aging processes, defects in manufacturing technology or errors of maintenance personnel. The survivability (stability) of a communication network characterizes ITN ability to maintain full or partial operability under the action of causes that lie outside the network (spontaneous or intentional) and lead to the destruction or significant damage to some of ITN elements.

2. Network performance (or throughput) is related to performance parameters, since the implementation of the required load must be carried out with specified quality parameters.

3. Information security during the storage and transfer of data is associated with violations of confidentiality and the integrity of information. Attempts to violate the privacy and integrity of information can be made by ill-wishers or competitors. In addition, security is affected by failures in the operation of machinery and software systems under the influence of radio electronic signals.

4. The parameter of economic efficiency refers to the ITN characteristics both at the stage of ITN creation, and at the stages of operation and modernization. It is connected with the problems of legal and business risk.

Table 1. **Categories of factors and causes of ITN risks**

Factor category	Risk reasons	Private risks
Internal risks		
Technical factors	P_{11} – lack of capacity; P_{12} – lack of performance; P_{13} – improper maintenance; P_{14} –equipment deterioration	R_1 – Risk of equipment failure
	P_{21} – incompatibility; P_{22} – improper Configuration Management; P_{23} – improper Change Management; P_{24} – incorrect security settings; P_{25} – unsafe programming practices; P_{26} – improper testing	R_2 – Risk of crashing software
	P_{31} – design Problems; P_{32} – specification problems; P_{33} – integration problems; P_{34} – complexity of the system	R_3 – Risk of error in network design
Process factors	P_{41} – Improper workflow; P_{42} - Inadequate documentation of the process; P_{43} – misunderstanding of roles and responsibilities; P_{44} – incorrect information flows; P_{45} – improper escalation of problems; P_{46} – ineffective transfer of tasks	R_4 – Risk of error in network processes (design and execution)
	P_{51} – lack of status monitoring; P_{52} – lack of metrics; P_{53} – lack of periodic analysis; P_{54} – inadequate ownership of the process	R_5 – Risk of process control error
	P_{61} – staffing problems; P_{62} – financing problems; P_{63} – learning and development shortcomings; P_{64} – procurement issues	R_6 – Risk of error in supporting processes
Human factor	P_{71} – random error; P_{72} – ignorance P_{73} –non-observance of instructions	R_7 – Risk of unintentional action
	P_{81} – fraud; P_{82} – sabotage; P_{83} – theft; P_{84} – vandalism	R_8 – Risk of willful acts
	P_{91} – lack of skills; P_{92} – lack of knowledge; P_{93} – absence of instructions; P_{94} – inaccessibility of people	R_9 – Risk of inaction
External risks		
External factors	P_{101} – weather phenomena; P_{102} – fire; P_{103} – flooding; P_{104} – earthquake; P_{105} – riots; P_{106} – quarantine	R_{10} – Disaster risk
	P_{111} – non-compliance with requirements; P_{112} – changes in legislation; P_{113} – litigation	R_{11} – Legal risk
	P_{121} – problems with suppliers; P_{122} – unfavorable market conditions; P_{123} – adverse economic conditions	R_{12} – Business risk
	P_{131} – supply problems with materials; P_{132} – dependence on emergency services; P_{133} – problems with power supply; P_{134} – transport Problems	R_{13} – Risk of substandard services

Risks have a negative impact on the basic properties of information and ITN functioning [14].

Thus, violations in the processes of collecting information, processing it, failures in the technology of data transmission lead to information leakage, unauthorized copying and distortion (forgery). There can happen the blocking of systems and information transfer delay.

Risks due to hardware-software breakdowns and radio electronic disturbances are associated with viruses and "bookmarks" – interception devices. Not only viruses disturb, but also limit the speed of transmission, and can also block the network operation.

As a result of accidents, natural disasters, direct destruction, the breakdown of technical communication systems information carriers can be abducted.

Let's develop a structural system model of ITN risks, in which we will map the interdependence between the elements of the risk main aspects (Fig. 2). With the help of this model, the full set of cause-effect relationships from the causes of risks to their consequences and the impact on the main characteristics of the ITN can be determined.

According to the suggested approach, the risk assessment is carried out in stages. At the first stage, a structural diagram is constructed; private risks that cause the factors and probable consequences of risk occurrence are identified. The interrelationships between these components are presented in the form of a cause-effect diagram [11].

Since the number of relationships between risk factors and risk events is large, for the sake of clarity of the subsequent analysis, the relationship between the risk factors with risk manifestation and consequences is presented in the form of tables (Tables 2, 3), identifying each of the consequences in the form of a variable with the corresponding index.

To quantify the impact of IR on ITN functioning, the method based on the theory of causal analysis is suggested for use [15].

The risk model in the form of a cause-effect network can be based on the construction and analysis of probabilistic or fuzzy cognitive maps [16]. The cognitive map is defined as a tuple of sets:

$$K = (\{P, R, S\}, F, \{B, C\}),$$

where $\{P, R, S\}$ is the finite set of elements, which in this case consists of three subsets (factors, risks, consequences);

F is the finite set of connections between elements;

$\{B, C\}$ is the finite set of weights of these connections.

The cognitive map is transformed into a familiar oriented graph, at the vertices of which the key elements of the modeling object are located, interconnected by arcs that reflect the cause-effect relationships between them. These relationships characterize the degree (influence) of the elements' impact on each other and are set by means of coefficients (determining the probability of risk occurrence as a result of this factor, or consequences due to the risk origin) or by linguistic terms (determining the degree of influence):

$$B=\{b_{i,j}\ i=1..n, j=1..m\},\ C=\{c_{jk}\ j=1..m, k=1..h\}.$$

The values $b_{i,j}$ and c_{jk} can be determined by objective (on the basis of statistical data) or subjective method (by expert assessments) based on past experience.

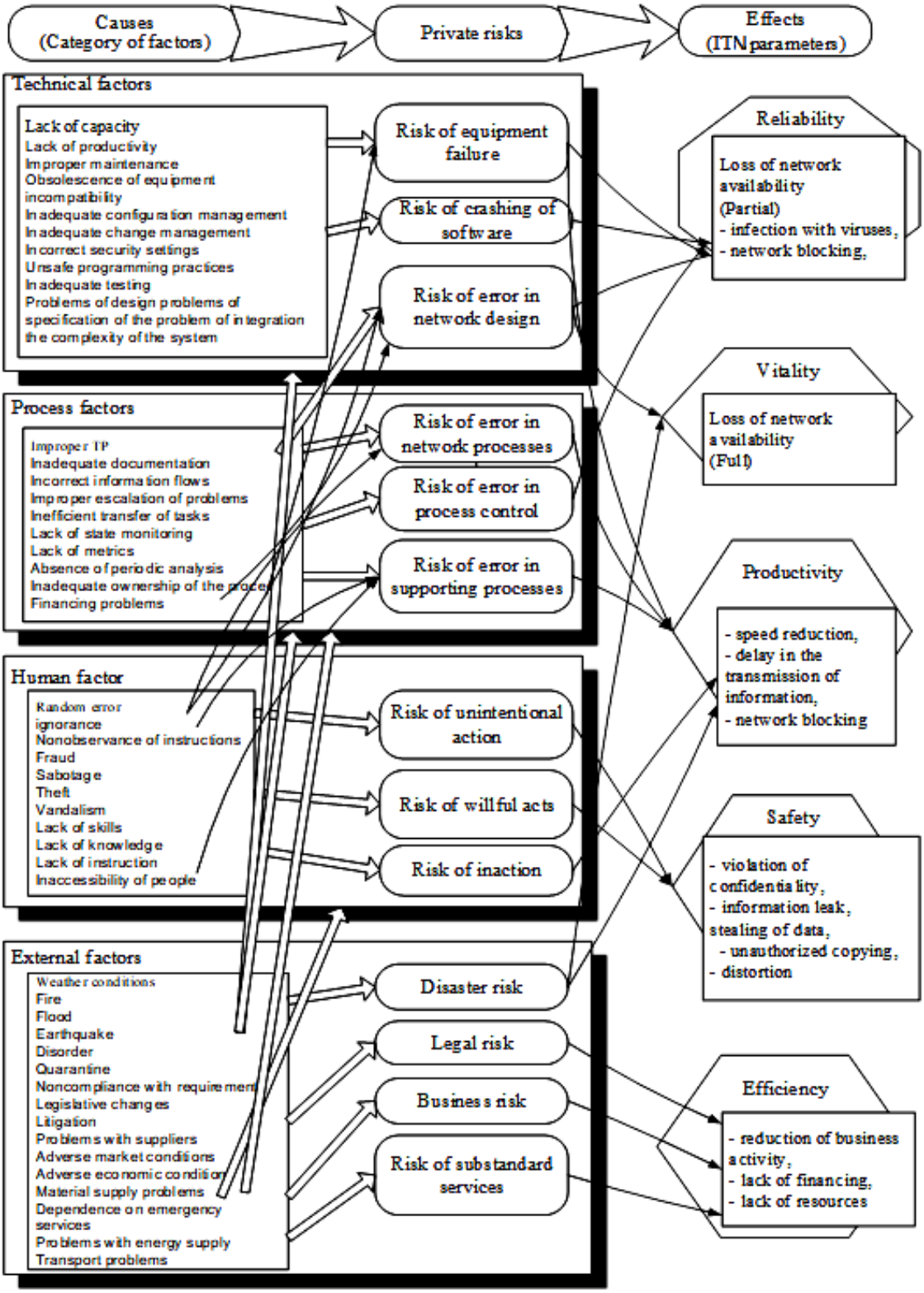


Fig. 2. Systemic risk model of ITN

Table 2. **The matrix of coefficients of factors' influence on private risks of ITN (fragment)**

Risk factors	**Private risks**												
	R_1	R_2	R_3	R_4	R_5	R_6	R_7	R_8	R_9	R_{10}	R_{11}	R_{12}	R_{13}
P_{11}	$b_{11,1}$	$b_{11,2}$	-	-	-	-	-	-	-	-	-	-	-
P_{12}	$b_{12,1}$	$b_{12,21}$	$b_{12,3}$	-	-	-	-	-	-	-	-	-	-
P_{13}	$b_{13,1}$	$b_{13,2}$	-	$b_{13,4}$	-	$b_{13,6}$	$b_{13,7}$	$b_{13,8}$	$b_{13,9}$	-	-	-	-
P_{14}	$b_{14,1}$	-	-	-	-	-	-	-	-	-	-	-	-
P_{21}	-	$b_{21,2}$	-	$b_{21,4}$	-	-	-	-	-	-	-	-	-
P_{22}	-	$b_{22,2}$	-	$b_{22,4}$	-	-	-	-	-	-	-	-	-
P_{23}	-	$b_{23,2}$	-	$b_{23,4}$	-	-	-	-	-	-	-	-	-
P_{24}	-	$b_{24,2}$	-	$b_{24,4}$	-	-	-	-	-	-	-	-	-
P_{25}	-	$b_{25,2}$	-	$b_{25,4}$	-	-	-	-	-	-	-	-	-
P_{26}	-	$b_{26,2}$	-	$b_{26,4}$	-	-	-	-	-	-	-	-	-
.....													
P_{131}	-	-	-	-	-	$b_{131,6}$	$b_{131,7}$	$b_{131,8}$	$b_{131,9}$	-	-	$b_{131,12}$	$b_{131,13}$
P_{132}	-	-	-	-	-	-	$b_{132,7}$	$b_{132,8}$	$b_{132,9}$	-	-		$b_{132,13}$
P_{133}	$b_{133,9}$	-	-	-	-	$b_{133,6}$	$b_{133,7}$	$b_{133,8}$	$b_{133,9}$	$b_{133,9}$	-	$b_{133,12}$	$b_{133,13}$
P_{134}	-	-	-	-	$b_{134,7}$	-	$b_{134,7}$	$b_{134,8}$	$b_{134,,9}$	-	-		$b_{134,13}$

Table 3. **Matrix of risk factors for possible consequences**

Private risks	**Effects**												
	Reliability		**Vitality**	**Performance**			**Security**				**Efficiency**		
	S_1	S_2	S_3	S_4	S_5	S_6	S_7	S_8	S_9	S_{10}	S_{11}	S_{12}	S_{13}
R_1	-	c_{12}	c_{13}	c_{14}	c_{15}	c_{16}	-	-	-	-	-	-	-
R_2	c_{21}	c_{22}	-	c_{24}	c_{25}	c_{26}	-	-	-	-	-	-	-
R_3	-	c_{32}	-	c_{34}	c_{35}	c_{36}	-	-	-	-	-	-	-
R_4	-	c_{42}	-	c_{44}	c_{45}	c_{46}	-	-	-	-	-	-	-
R_5	-	c_{52}	-	-	-	-	-	-	-	c_{510}	-	-	-
R_6	-	-	-	c_{44}	c_{45}	c_{46}	-	-	-	c_{410}	-	-	-
R_7	-	c_{72}	-	c_{74}	c_{75}	c_{76}	c_{77}	c_{78}	c_{79}	c_{710}	-	-	-
R_8	-	c_{82}	c_{83}	c_{84}	c_{85}	c_{86}	c_{87}	c_{88}	c_{89}	c_{810}	-	-	-
R_9	-	-	-	c_{94}	c_{95}	c_{96}	-	-	-	-	-	-	-
R_{10}	-	c_{102}	c_{103}	-	-	-	-	-	-	-	-	-	-
R_{11}	-	-	-	-	-	-	-	-	-	-	c_{1111}	-	-
R_{12}	-	-	-	-	-	-	-	-	-	-	-	c_{1212}	-
R_{13}	-	-	-	-	-	-	-	-	-	-			c_{1313}

The factor of influence of the factor of risk occurrence $b_{i,j}$ is determined on basis of the frequency of occurrence of this type of risk, based on statistical information or based on estimates of forecasting. Recently, the reliability and security indicators of the network are reduced as a result of the following events (which are related to the risks of software failure and deliberate actions):

the selection of keys / passwords (password attacks) - 13.9% of the total;

replacement of IP-address (IP spoofing) - 12,4%;

denial of service (DoS-attacks) - 16.3%;

analysis of traffic (sniffing packages) - 11.2%;

scanning (network intelligence) - 15.9%;

substitution of data transmitted over the network (data and software manipulation) -15.6%;

other methods (viruses and programs "Trojan Horse") - 14.7% [7].

It is necessary to take into account the fact that not all ITN risks can be fully realized or implemented in general in this network; the same type of threat can cause significant or minor damage. Therefore, to make a decision as for ITN risk management, it is necessary to determine the degree of private risk influence on the characteristics of the network function [10]. The level of risk influence c_{jk} can also be determined by experts according to the following scale:

- 0 - the risk does not actually affect the given network characteristic;
- 0.25 - the risk has little impact;
- 0.5 - the risk affects at average degree;
- 0.75 - the risk has a significant impact;
- 1.0 - the risk has a direct impact.

The knowledge of the structure of the causal system can be used to transform the statistical description of inputs into the description of outputs.

To do this, we form a recursive system of equations isomorphic to the structural diagram, the coefficients of which act as coefficients of influence [17]. In our case, we can draw a parallel between the

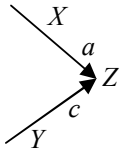
structural coefficients of influence and the probabilities of manifestation of specific events (factors, risks, consequences).

In accordance with the theory of causal analysis the following rules are used for formulating equations:

1. The value of the variable is defined by one input equal to the input value multiplied by the structural coefficient.

$X \xrightarrow{a} Y$ means $Y = aX$.

2. The value of a variable, defined by several input quantities, is equal to the sum of the input values multiplied by their structural coefficients. The order of summation does not matter.



means $Z = aX + cY$

3. The ways that escape from a variable when writing equations for this variable are not taken into account, but each incoming arrow indicates an element that must be considered.

Structural equations describe direct connections. In order to take into account the indirect links, the reduction rules are used: if one variable defines the second variable, and the other determines the third, the value of the third variable can be expressed as the value of the first variable multiplied by the product of the structure coefficients along the chain.

The same principle is applied when a chain has more than two links.

$X \xrightarrow{a} Y \xrightarrow{c} Z$ means $Z = acX$.

The generalized structure of the cause-and-effect diagram of the factors, manifestations and consequences of ITN risks is presented in Fig. 3.

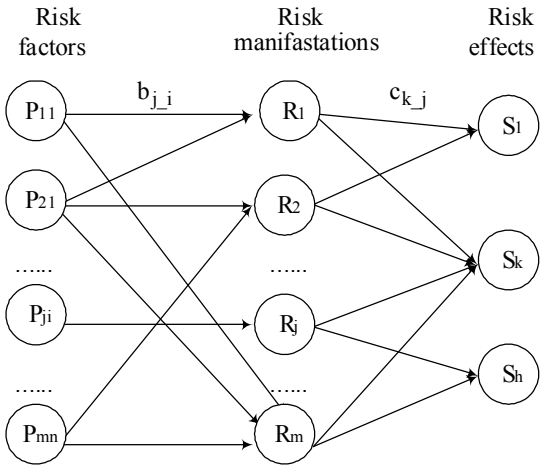


Fig. 3. Structural diagram of the cause-effect diagram

On the diagram $b_{j,i}$, $0 \le b_{j,i} \le 1$ is the coefficient of influence of the i-th factor on the occurrence of the j-th manifestation of risk; c_{kj}, $0 \le c_{kj} \le 1$ is the coefficient of influence of the j-th manifestation of risk on the k-th consequence.

Then the estimation of the probability of occurrence of the k-th consequence is made according to the formula:

$$P(S_k) = \sum_i \sum_j b_{j,i} c_{kj} .$$

For example, in accordance with the systemic representation of risk, the probability of "distortion of information" event is determined in accordance with the causal diagram (Fig. 4) and is calculated by the formula:

$$P(S_{10}) = c_{105}(b_{5,13} + b_{5,1} + b_{5,2} + b_{5,3} + b_{5,4}) +$$
$$+c_{106}(b_{6,13} + b_{6,1} + b_{6,2} + b_{6,3} + b_{6,4} + b_{13,1} + b_{13,2} +$$
$$+b_{13,3} + b_{13,4}) + c_{107}(b_{7,13} + b_{7,1} + b_{7,2} + b_{7,3}) +$$
$$+c_{108}(b_{8,13} + b_{8,1} + b_{8,2} + b_{8,3} + b_{8,4}).$$

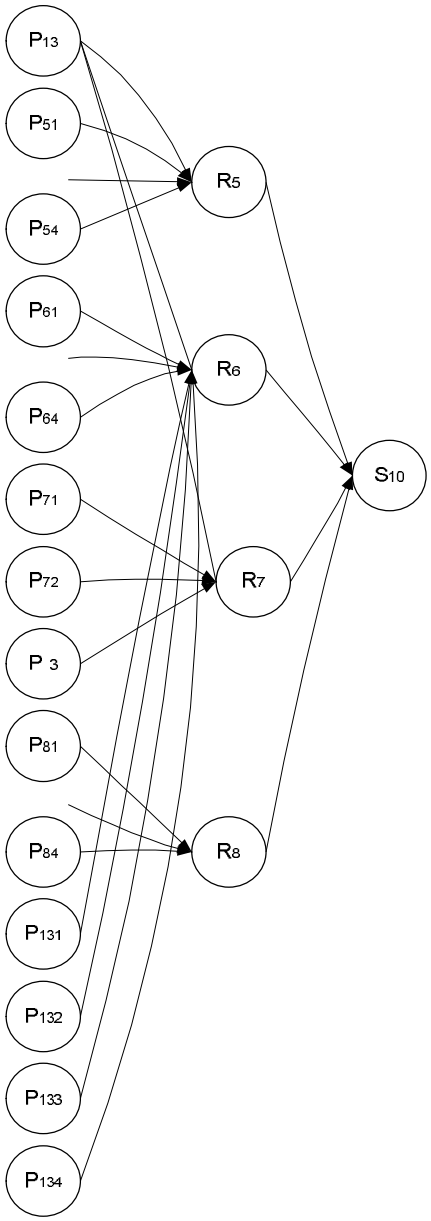


Fig. 4. Example of a cause-effect diagram for "distortion of information" event (consequences)

Thus, knowing the degree of impact (in the form of impact factors) of risk factors, risk events and consequences, as well as cause-effect relationships between them, possible failures and losses in ITN functioning can be determined.

Possible damage to the functioning of the network G_{kj}, determined by the k-th consequence, which is caused by the j-th private risk G_{kj} is calculated according to the relationship [18]:

$$G_{kj} = P(S_k)\, H(R_j \rightarrow S_k) f_k ,$$

where $P(S_k)$ is the probability of k-th consequence;

$H(R_j \rightarrow S_k)$ is the the risk R_j impact on the characteristics S_j,

f_i is the indicator reflecting the value of the k-th characteristic.

Conclusions

The suggested method for quantitative assessment of ITN risk is based on the method of cause-and-effect analysis and enables taking into account both the factors causing it, and probable consequences.

In connection, identifying potential losses can be made, as well as the measures to manage the risks of ITN functioning can be taken.

It should be noted that the main problem in the application of the suggested method is the complexity of obtaining the values of the structural coefficients of the influence of factors, private risks of ITN and their consequences.

REFERENCES

1. Konvergencija setej, tehnologij i uslug [Convergence of networks, technologies and services], available at: http://studopedia.su/6_48249_konvergentsiya-setey-tehnologiy-i-uslug.html (last accessed February 1, 2017).
2. Cichonski, P., Millar, T., Grance, T. and Scarfone, K. (2012), *Computer Security Incident Handling Guide*, National Institute of Standarts and Technology, 79 p.
3. Ross, R. (2012), *Guide for Conducting Risk Assessments,* National Institute of Standards and Technology, 95 p.
4. Paulsen, S. and Boens, J. (2012), *Summary of the Workshop on information and communication technologies supply chain risk management*, National Institute of Standards and Technology, 21 p.
5. Zadiraka, V.K. and Kudin, A.M. (2012), "Osobennosti realizacii kriptograficheskih i steganograficheskih sistem po principu oblachnyh vychislitelnyh tehnologii" [Peculiarities of realization of cryptographic and steganographic systems according to the principle of cloud computing technologies], *Shtuchnyi intelekt* [Artificial Intelligence], No. 3(55), pp. 438–444.
6. Hornytska, D.A., Zakharova, M.V. and Kladnytskiy, A.I. (2012), "Analysis and assessment system of the state of information security, socio-technical resources of attacks", *Information security*, No 2, pp. 70-74.
7. Burachok, V. (2013), "Technology of vulnerabilities using of web-resources in the organization and conducting of network reconnaissance informational telecommunication systems", *Network & Internet security*, Vol. 19, Issue 2, pp. 83-87.
8. Furmanov, A.A., Lahizha, I.N. and Harchenko, V.S. (2009), "[Modeling of guaranteed service-oriented architectures for attacks with using of vulnerabilities", *Radioelectronic and computer systems*, No. 7 (41), pp. 65-69.
9. Boyarchuk, A. (2011*), Safety of critical infrastructures: mathematical and engineering methods of analysis and support,* National Aerospace University "KhAI", Kharkiv, 641 p.
10. Voropaeva, V.Y., Shcherbov, I.L. and Haustova, E.D. (2013), “Upravlenie informacionnoi bezopasnostiu informacionno-telekommunikacionih system na osnove modeli «plan-do-checkact»” [Information Security Management information and telecommunication systems based on the model «PLAN-DO-CHECK-ACT»], *Naukovi pratsi DonNTU. Seriya: ob-chyslyuval'na tekhnika ta avtomatyzatsiya* [Proceedings of Donetsk National Technical University. Series: Computers and Automation], No. 253 (201), pp. 104-110.
11. Prikhodko, T.A. (2011), Issledovanie voprosov bezopasnosti lokal'nyh setej na kanal'nom urovne modeli OSI [Investigation of security issues of local networks on the channel level of the OSI model], available at: http://ea.dgtu.donetsk.ua:8080/handle/123456789/2068 (last accessed February 1, 2017).
12. Sklyar, V.V. (2011), "Methodology of risk analysis of functional safety of information-control systems", in *Safety of critical infrastructures: mathematical and engineering methods of analysis and provision*, Kharchenko, V.S. (Ed.), National Aerospace University "KhAI", Kharkiv, Section 12, pp. 360-408.
13. Nochevnov, E.V. (2016), ["Klassifikacija faktorov riska v upravlenii proektami v oblasti informacionnyh i kommunikacionnyh tehnologij" [Classification of risk factors in project management in the field of information and communication technologies], *Upravlenie proektami i programmami* [Project and Program Management], No. 2, pp. 44-53.
14. Chto takoe informacionnaja bezopasnost' telekommunikacionnyh sistem? [What is the information security of telecommunications systems?], available at: http://camafon.ru/informatsionnaya-bezopasnost/telekommunikatsionnyih-sistem (last accessed February 1, 2017).
15. Hayes, D. (1981), *Causal analysis in statistical studies*, Moscow, Finance and Statistics, 255 p.
16. Kiryanov, V.V. Usovershenstvovanie organizacionnyh osnov sozdanija kompleksnoj sistemy zashhity informacii v informacionno–telekommunikacionnoj sisteme [Improvement of organizational bases for creating a comprehensive information security system in the information and telecommunication system], available at: http://masters.donntu.org/2014/frt/kiryanov/diss/index.htm (last accessed February 1, 2017).
17. Maleeva, O.V. and Sytnik N.I. (2007), "Analysis of the interaction of internal and external risks on the basis of the cause-effect diagram", *Radioelectronic and computer systems*, No. 1, pp. 73-76.

18. Nadezhdin, E.N. and Sheptukhovsky, V.A. Metodika ocenivanija riskov informacionnoj bezopasnosti v vychislitel'nyh setjah obrazovatel'nyh uchrezhdenij [The method of assessing the risks of information security in the computer networks of educational institutions], available at: http://www.masters.donntu.org/2014/frt/vashakidze/library/8.htm (last accessed February 1, 2017).

Received (Надійшла) 10.02.2017
Accepted for publication (Прийнята до друку) 16.05.2017

Аналіз ризиків інформаційно-телекомунікаційної мережі на основі когнітивних карт і причинно-наслідкової діаграми

В. В. Косенко, О. В. Малєєва, О. Ю. Персіянова, А. І. Роговий

Предметом вивчення в статті є процеси аналізу та оцінки ризиків інформаційно-телекомунікаційних мереж. **Мета** - зниження потенційних втрат, зумовлених ризиками функціонування інформаційно-телекомунікаційної мережі (ІТМ), шляхом своєчасного вжиття заходів з управління ризиками. **Завдання:** класифікація ризиків ІТМ з виділенням основних факторів і причин їх виникнення; формування системного уявлення ризиків для виявлення їх проявів і наслідків; розробка методу оцінки ступеня впливу причин на прояв ризику і приватних ризиків на можливі наслідки; отримання кількісної оцінки ризиків ІТМ. Використовуваними **методами** є: системний аналіз ризиків, метод когнітивних карт, причинно-наслідковий аналіз. Отримані такі **результати**. Проведена класифікація приватних ризиків ІТМ з причин та за факторами їх виникнення. Визначено негативні наслідки, що негативно впливають на основні характеристики функціонування ІТМ. В результаті сформована структурна системна модель ризиків ІТМ, в якій відображені взаємозв'язки між елементами основних аспектів ризику. Для кількісної оцінки впливу ризику на функціонування ІТМ запропонований метод, заснований на теорії причинного аналізу. Модель ризиків заснована на побудові та аналізі імовірнісних або нечітких когнітивних карт. Для прийняття рішень з управління ризиками експертами визначається рівень впливу приватних ризиків на характеристики мережі. Розроблено узагальнену структуру причинно-наслідкової діаграми чинників, проявів і наслідків ризиків. На її основі запропоновано спосіб кількісної оцінки можливості виникнення наслідків ризиків. Також проводиться кількісна оцінка можливих збитків для функціонування мережі, що визначається конкретним наслідком (з урахуванням його ймовірності), який викликаний приватними ризиками. **Висновки.** Запропоновано підхід для кількісної оцінки ризику ІТМ заснований на методі причинно-наслідкового аналізу та дозволяє враховувати як чинники, що його викликають, так й можливі наслідки. Отримані результати можна використовувати для визначення можливих збоїв і втрат при функціонуванні ІТМ на основі інформації про ступінь впливу факторів ризику, ризикових подій і наслідків, а також причинно-наслідкових залежностей між ними. Стає можливим визначати потенційні втрати, а також вживати заходів з управління ризиками функціонування ІТМ.

Ключові слова: інформаційно-телекомунікаційна мережа, фактори, ризики, наслідки, причинно-наслідкова діаграма, коефіцієнти впливу.

Анализ рисков информационно-телекоммуникационной сети на основе когнитивных карт и причинно-следственной диаграммы

В. В. Косенко, О. В. Малеева, Е. Ю. Персиянова, А. И. Роговой

Предметом изучения в статье являются процессы анализа и оценки рисков информационно-телекоммуникационных сетей. **Цель** - снижение потенциальных потерь, обусловленных рисками функционирования информационно-телекоммуникационной сети (ИТС), путем своевременного принятия мер по управлению рисками. **Задачи**: классификация рисков ИТС с выделением основных факторов и причин их возникновения; формирование системного представления рисков для выявления их проявлений и последствий; разработка метода оценки степени влияния причин на проявление риска и частных рисков на возможные последствия; получение количественной оценки рисков ИТС. Используемыми **методами** являются**:** системный анализ рисков, метод когнитивных карт, причинно-следственный анализ. Получены следующие **результаты.** Произведена классификация частных рисков ИТС по причинам и по факторам их возникновения. Определены негативные последствия, отрицательно влияющие на основные характеристики функционирования ИТС. В результате сформирована структурная системная модель рисков ИТС, в которой отображены взаимосвязи между элементами основных аспектов риска. Для количественной оценки влияния риска на функционирование ИТС предложен метод, основанный на теории причинного анализа. Модель рисков основана на построении и анализе вероятностных или нечетких когнитивных карт. Для принятия решений по управлению рисками экспертами определяется уровень влияния частных рисков на характеристики сети. Разработана обобщенная структура причинно-следственной диаграммы факторов, проявлений и последствий рисков. На ее основе предложен способ количественной оценки возможности возникновения последствий рисков. Также производится количественная оценка возможного ущерба для функционирования сети, определяемого конкретным последствием (с учетом его вероятности), который вызван частными рисками. **Выводы.** Предложенный подход для количественной оценки риска ИТС основан на методе причинно-следственного анализа и позволяет учитывать, как вызывающие его факторы, так и возможные последствия. Полученные результаты можно использовать для определения возможных сбоев и потерь при функционировании ИТС на основе информации о степени воздействия факторов риска, рисковых событий и последствий, а также причинно-следственных зависимостей между ними. Становится возможным определять потенциальные потери, а также принимать меры по управлению рисками функционирования ИТС.

Ключевые слова: информационно-телекоммуникационная сеть, факторы, риски, последствия, причинно-следственная диаграмма, коэффициенты влияния.