Mathematical modelling of economic planning issues of cyber security and organization of information security

Mathematical modelling of economic planning issues of cyber security and organization of information security

I V Mandritsa[1], A Fensel[2], M Mecella[3], D Capeska Bogatinoska[4], V I Petrenko[1], O V Mandritsa[5] and I V Solovieva[1]

[1]North-Caucasus Federal University, 1, Pushkin Street, Stavropol, 355009, Russia
[2]University of Innsbruck, 21a, Techniker str., 6020 Innsbruck, Austria
[3]SAPIENZA University, DIAG, B211, Rome
[4] University of Information Science and Technology "St. Paul the Apostle", Ohrid, Macedonia
[5] Russian Technological University – MIREA, Branch office, 8, Kulakov street, Stavropol, 355035, Russia

E-mail: d_artman@mail.ru

Abstract. The article presents the theoretical concept of economic protection of cybercasting as part of cybersecurity and all its elements: information security, network and Internet security against modern threats for organization. Such categories as: cyberinformation, economics of cybersecurity, and classification of the concept of «Damages from loss or cybercasting» and its value of content in the form of loss of business information are firstly introduced. For example, famous in optimal programming in math of its proposed transport task solution to search for optimum protection in view of possible threats or cybercasting the emergence of economic damages.

1. Introduction

The notion of cyberspace and cybersecurity are not available in the legislation of Russia at the moment. The "cybersecurity" strategy concept discussed by the Russian Council of Federation at January, the 10th 2014 year has not been actually accepted and there are no prerequisites to its scientific and practical recognition due to position of the Russian Federal Security Service. Despite this fact, the «cyber-" terminology should be taken into account, since the issues of cybersecurity were firmly established in the international community and International Standard ISO/IEC 27032:2012 (ISO/IEC 27032:2012) Information Technology Security Techniques - Guidelines for Cybersecurity says "[1], which describes the concept of "cybersecurity" and its relation to other categories of information security was issued.

In reality, the adopted standard provides only a set of recommendations to improve "cybersecurity", revealing the unique aspects of this activity and its dependence on other security areas, in particular:

- information security,
- network security,
- online safety,
- protecting critical information infrastructure.

The standard defines only basic security techniques for stakeholders in cyberspace. In turn, the security of critical information infrastructures, though related to cyber security (as it is understood throughout the world), but only partially. The standard provides the diagram that visualizes the

relationship of the various terms (translated by the authors). In the Russian legislation this term was only conceptually expressed in the concept of cyber security in the Russian Federation.

According to the standard ISO/IEC 27032 2012 the definition [1] of this term is the following, "Cybersecurity is the protection conditions against physical, spiritual, financial, political, emotional, professional, psychological, educational or other impacts against the consequences of an accident, damage, error, accident, injury, or any other event in cyberspace that could be considered undesirable."

According to the adopted concept of cybersecurity strategy in the Russian Federation, [3] the same notion sounds differently: "Cybersecurity is a set of conditions under which all components of cyberspace are protected from the maximum possible threats and impacts with undesirable consequences. "

According to the authors one of these conditions is the economic evaluation of the rationality of the protecting cyberspace entity methods from the maximum possible threats and impacts with undesirable consequences. The subject is considered to be the cybercasting users both individuals and legal entities that are part of the information system in the State, in a region or a locality. All the cyberinformation of either private (physical) person or legal organizations (firms) can be divided into two groups: have a value and does not have a value. The part of cybercasting which brings its owner (s) some income is considered to be the information that has value or business information. However, there is not any direct business information on the information market, because today you do not find the ads like -«buy information» or "sell information». The cyber information which will bring some business income in future is either hidden from the public or is born in the form of business ideas in the minds of entrepreneurs and becomes secret since its outbreak. Since then, the defense economy cybercasting as the future value of its protection threats is born and at that moment the rationality of the cybercasting owner's conduct concerning its protection is required and called the reasonable rational economic behavior.

The cybersecurity rationality is supposed the reasonable owner costs on the cyberspace defense cyberinformation security but not the irrationality when the subject in order to adoption its decisions in the field of the information protection is based on the freedom amounts or spending resources principles.

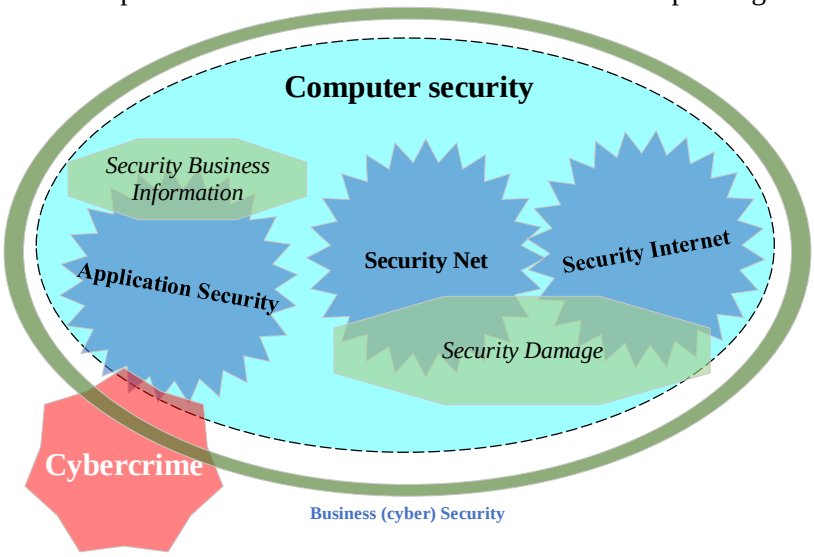

Figure 1. *Cybersecurity* according to ISO/IEC 27032:2012

Figure 1. The term “cybersecurity” is related to network security, application security, Internet safety and security critical information infrastructures from the Western experts’ point of view. Thus, a distinction should be drawn between cybersecurity and information security as two individual factors in the economy. However, for verbal mathematical description entered the category of “Economics of cybersecurity (Business (Cyber) Security (hereinafter BCS)” introduces conditional designation of its factors:

S BIS (X) - Security Business Information object X,
S Net (X) - Security Net object X,
S Inet (X) - Security Internet object X,
S D (X) - Security Damage critical information infrastructure facility, as the sum of *SNet (X) и SInet (X)*.

Thus, the figure 1 converts to the new dependency of safety factors listed above as follows (Figure 2). The authors firstly introduce the cyberinformation of organization category as the sum of all valuable information (economic profit, usefulness) which will bring income for the Organization in future. The accounting 9/99 "Profits" for the Russian business environment defines the Organization income (in our case review-income from the cybercasting): "Income the Organization recognizes the increasing economic benefits from the proceeds of assets (cash, other assets) and (or) liabilities, leading to an increase in capital of this organization, with the exception of the deposits of founders» [2].

Thus, cyberinformation is an asset that will bring future benefit to an organization. Thus, from the moment when the cyberinformation, consisting of business information is beginning to bear its owner income rises the question of its rational protection against cybercrime.

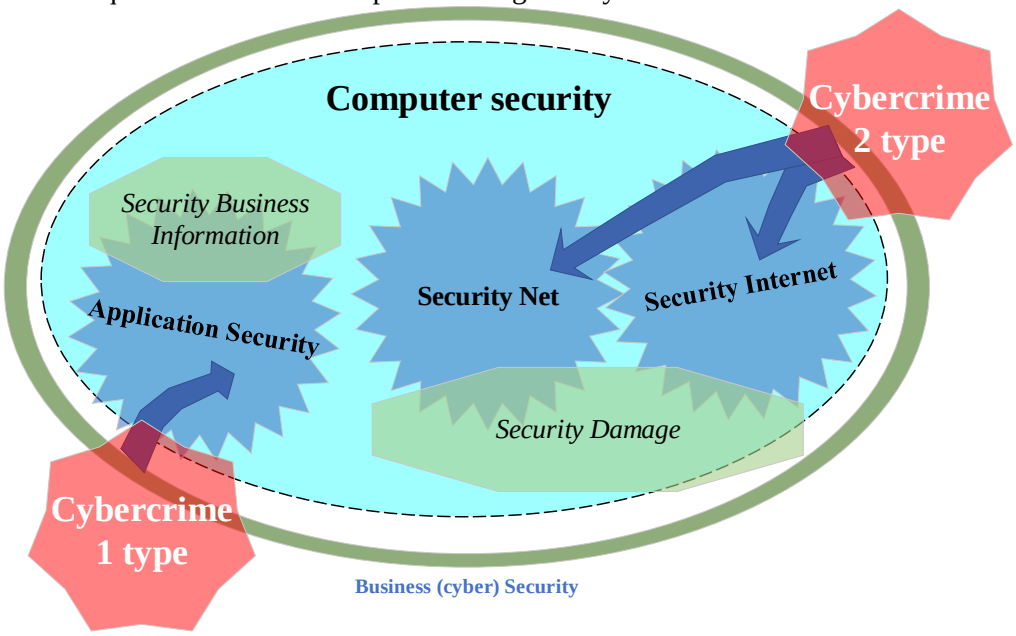

Figure 2. Theoretical basis of Economics of cybersecurity (newly introduced category)

Raises the scientific field of this research category-economics of cybersecurity organization.

Accordingly, the theft of cybercasting containing business information- is a type of enrichment, or thief's "clean" profits, as at the level of an individual physical person, and at a higher level of economic involvement of criminals in this type of activity. Thus, any cyberinformation, which carries in itself the benefit, has a cost, and is business information, fills the country economy added value, which later becomes the "richness" of his people [2]. In this case the agents and the State, creating valuable cyberinformation raises unnecessary expenditure on the organization of workplaces, the maintenance of market conditions and other economic categories. These agents are physical cybercasting owners and legal structure of society. But the highest relevance for our study has a company cyberspace as a legal entity, for example of a commercial company (organization), or a budgetary organization.

Thus, the main task for the realization of the goal set in this article will be a mathematical description of the model of cybersecurity economy for a commercial organization. Wiser (smarter) protect cyberinformation than just lose, betray a senseless publicity and thus raise itself a competitor to the detriment of their business, as well as reduce the cost of their information (business information).

2. Results and discussion

Cybercrime poses a threat to cyberspace and the information that fills this space benefit, utility or economy, as it's called value. At the moment cyberspace (perimeter, the information unit and the organization of interaction with external space of the Internet) of a company is organized under its network perimeter (periphery), as follows (Figure 3) [3].

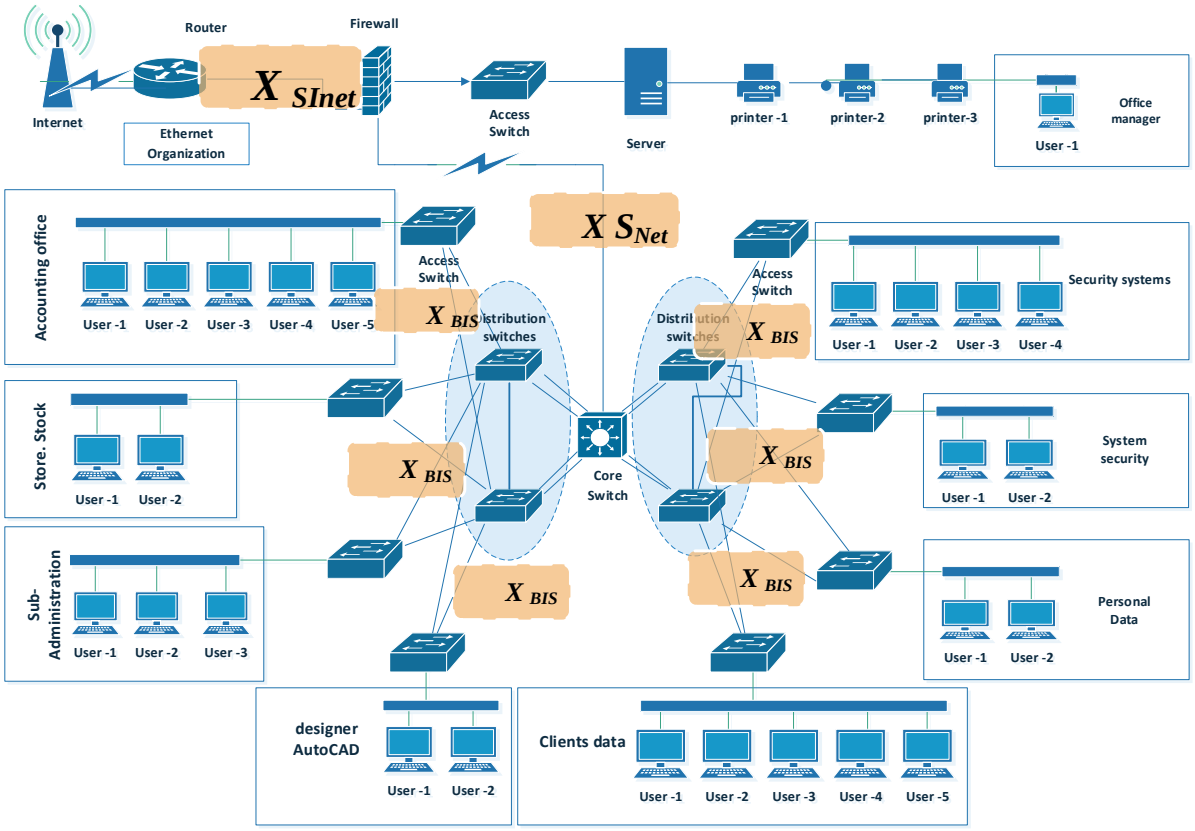

Figure 3. Cyberspace localization for an organization (company) used to determine the cost of cyberinformation protect [3]

As a result, the cumulative state of an object cybersecurity (company) *X*, -according to Figure 1) *Xbcs* will consist of three above-mentioned components (1):

$$X_{bcs} = \sum \left(X_{BIS} + X_{SNet} + X_{SInet} \right) \quad (1)$$

Accordingly, then the target function (f) of Economics of cybersecurity to protect or cybercasting object *X bcs* will be striving for expression (2), in economically rational and reasonable context:

$$f(X) \rightarrow \max BCS \quad (2)$$

However, the cybercrime (impermanent) manifests itself discretely in the form of a probability, that the cybercasting threat of diversion would arise for an object X.

Figure 3 an example of localization of cyberspace of Organization (company) for the purpose of determining the cost of protecting its cyberinformation. It should be noted that the category of threat (risk) ρ-there are the risks of cybercasting diversion.

This category is dynamic; it is not constant at different stages of company life (Organization). For companies which are already losing its competitive advantage the risk of leakage is reduced, and vice versa for startups the relevance of diversion is high.

The above-mentioned information leads the authors to the makes it necessary to present study, enter a new category-the damage possibility from losses (cybercasting) and the second correspondence

category-the seriousness effect on cyberinformation by the threats channel. At the same time, the second category is the severity of the impact via threats has its facts content.

As an example, the authors use the cyber-DDoS-attack known for all the professionals (Distributed Denial of Service — «denial of service») — This is an attack on company website, the main aim which breaking company site by making a large number of spurious requests.

The economics point of view is, accompanied by two characteristics: the likelihood of damage and amount of damages from loss or cyberinformation (cybercasting).

The formula the risk for cybercasting R (RE) is well known (3) [2, p. 6]

$$RE = Prob\ UO * Loss\ (UO) \tag{3}$$

and its Russian equivalent (3.1):

$$R = \rho U\ (Threat) * AU\ (Threat) \tag{3.1}$$

where: ρU (Threat) – the likelihood of threat cyberinformation, RH. relative number; AU (Amount of Threat Loss) - the amount of possible damage from the cyberinformation (loss) in rubles (€ or $).

Having entered the category of risk and severity of threats from leaking the cybercasting its necessary describe philosophically what is a "Damage" loss (leakage) or cybercasting. correspondently expression 1 is converting into the following (4):

$$Xbcs = \sum\ (X_{BIS} + X_{SNet} + X_{SInet}) - (\rho U\,(_{Threats}) * AU\,(_{Threats})) \tag{4},$$

The authors, thinks that the damage of cyberinformation loss (and its value content as business information) entails the following consequences for its owners.

The variety of threat-forming manifestations that's following topic under discussion determine the beginning of the undesirable event-leak (loss of) information, confirms the necessary to draw a clear distinction of possible damages from loss or cybercasting Depending its aspect of consideration.

In this study, the classification of the cybercasting damage on the set of criteria that defines the most common signs of the original concepts-damage or loss or cyberinformation (cybercasting), are particular type of identification.

It is the kind of the damage X_i that can be achieved by cyberinformation (cybercasting) protection activities and is applied for the implementation of precise integrated calculations the economic damage from hacker attacks on the following: Formation space; Origin; Type of initiating impact; Type of manifestation; Field manifesting; Industry the emergence; Scope of proliferation; The level of consideration; Amount; Forecasting; Reversibility of effects; The frequency of application; Thrust causing; Manifestation; Perception; Localization; Time of application; Identification; Homogeneity of objects; The possibility of extending; Sequence manifestations [9, 10].

Thus, the authors get the expression of cybersecurity in the form of (5):

$$f\,(X) \rightarrow \max(\text{BCS-}(\rho\text{U*AU})*(\text{X}_i(\text{Threats})) \tag{5}$$

i.e. reducing threats for object X_i, the authors reach the maximum reasonable limit of the object cybersecurity. As a result, the total value of the current security cybersecurity for the subject of protection can be expressed: by the factor of cybersecurity, which will be based on the ratio of economic indicators K_{bcs} (6).

$$K_{bcs}(X) = \frac{\sum \text{S}cyberdefense\ (Xbcs)}{\text{S}cyberinformation\ (Xbcs)} \tag{6}$$

where is: ∑ S cyberdefense (X) – the amount of money on cybersecurity protection around the object and its components on X_{bcs}; S - the cost of funds for the creation of cyberinformation (cybercasting) of the object X_{bcs}.

Thus, the expression 4, 5 and 6 will take "matrix" view (7 and 8), on the basis of the correspondence between tables zone of cybersecurity and the likelihood of threats to this zone per the amount of its damage, that can be calculate by simplex method (table 1). These tasks apply to linear programming

tasks and can be solved by the famous simplex method. In this case the authors have a typical "transport tasks", they call it the task of cybersecurity for the object X.

Table 1- Initial data for cybersecurity transport tasks cybersecurity-calculation of damages possible values

$R(Xbcs)$	$R_{SI}=\rho U * AU_{(BIS)}$	$R_{SNet}=\rho U * AU_{(SNet)}$	$R_{BInet}=\rho U * AU_{(SInet)}$
$s\ (X)$			
$\boldsymbol{S_{BIS}}$	AU_{11}	AU_{12}	AU_{13}
$\boldsymbol{S_{SNet}}$	AU_{21}	AU_{22}	AU_{23}
$\boldsymbol{S_{SInet}}$	AU_{31}	AU_{32}	AU_{33}

This transport task integrates a wide range of tasks with a single mathematical model. However, basic transport task has a large number of variables and solving them by the simple method is cumbersome. On the other hand, the matrix of system limitations applied to the "transport task" is very peculiar, so the special solution methods have been developed.

These methods, as the simple method, allow finding initial support solution, and then improving it, getting a sequence of reference solutions, which culminates the optimal solution. The conditions of the "transport task" (the authors use the initial formulations) are:

"The Homogeneous value" (in this case the cost of cybercasting protection S (Xbcs) in its area of concentration AU in the object X_i) focus on *m* suppliers c*yberzone AU*) in the "volumes" (with the cost of this or cybercasting) [6, 7] the expression (7, 8, 9):

$$a1(S_{BIS}),\ a2(S_{SNet}),\ a2(S_{SInet}) \tag{7}$$

This "volume" (cyberinformation) "needs to be delivered" (exposed to threats) to *n* consumers (and probable quantities of damage threats) in the "volumes" (possible amounts of damage for them):

$$b1(R_{BIS}),\ b2(R_{SNet}),\ b3(R_{SInet}) \tag{8}$$

Thus, the authors set the possible damage amount for information on cyber security zones, namely:

$$AUij,\ \ i=1,2,...m;\ \ j=1,2,...n \tag{9}$$

AUij— the probable amount of damages per the zones of cybersecurity "costs of column transportation on units from each i- supplier to each j- consumer". Then, the authors comply the table 2 for the conditions of the transport challenges of cybersecurity [8].

Table 2- Initial data for transport tasks-calculation sums (S) on cybersecurity protection against threats

$S(X_{BCS})$ $S_{BCS}(X)$	S_{BIS}	S_{SNET}	S_{SINET}
$\boldsymbol{S_{BIS}}$	$Kbcs_{11}$	$Kbcs_{12}$	$Kbcs_{13}$
$\boldsymbol{S_{SNET}}$	$Kbcs_{21}$	$Kbcs_{22}$	$Kbcs_{23}$
$\boldsymbol{S_{SINET}}$	$Kbcs_{31}$	$Kbcs_{32}$	$Kbcs_{33}$

Variables (unknown) transport tasks are Xij, i=1, 2,...,m j=1,2,...,n —"traffic" (the amount money for the protection of cyber space zone in object X_i or coefficient cybersecurity (formula 9)) from every i- supplier to ever j- consumer.

3. Conclusion

As a result, the authors obtain the matrix of the likely amounts of damage from threats to cyber-security zones and second matrix of costs for the data protection in the cybersecurity zones of cybersecurity threats values. These variables can be written in the form of matrices "transport" 10 & 11:

Threat zones of cyberspace object X_i:

$$AU = \begin{pmatrix} au_{11} & au_{12} & au_{13} \\ au_{21} & au_{22} & au_{23} \\ au_{31} & au_{32} & au_{33} \end{pmatrix} \quad (10)$$

The cost of the protection zones in the object X_i:

$$Kbcs = \begin{pmatrix} Kbcs_{11} & Kbcs_{12} & Kbcs_{13} \\ Kbcs_{21} & Kbcs_{22} & Kbcs_{23} \\ Kbcs_{31} & Kbcs_{32} & Kbcs_{33} \end{pmatrix} \quad (11)$$

It is necessary to compile the "road map" to calculate the value cybersecurity protection factor for the object X_i, where "the reserves of all suppliers (threat amounts of damages)" removed entirely (covered (protected) zone protection activities cyberspace), requests for all consumers are met completely, and total expenses "for the transportation of all volumes (coefficient of cybersecurity for the zone) are minimal.

As the sum of: *AUij* Kbcsij* defines the cost of volume transportation "(the cost of the cyberspace protection zones in correlation with the value of this threat zone) from the i- supplier of j- consumer, total expenses" all the transportation volumes "(the amount of the cyberspace protection zones) are equal.

I.e., the authors get the following expression 12 & 13:

$$\sum_{i=1}^{m} \sum_{j=1}^{n} AUij * Kbcsij \quad (12)$$

According to the task a minimum total cost of protection for the zone in the object X_i is provided.

Consequently, the target function is presented for the zones form 13:

$$f(Xbcs) = \sum_{i=1}^{m} \sum_{j=1}^{n} AUij * Kbcsij \to \min \quad (13)$$

The best solution of the research problem is to find a minimum value of spent cost on cybercasting protection activities for each threat and the probable amount of damage for cyberinformation (cybersecurity) in the object X_i. Tasks constraints system consists of two groups of equations.

The first group of *m* equations describes the fact that "reserves" Rj (the cost of protection or cybercasting correspondence with its creation value) of all *m* (supplies zones of cyberspace) are removed completely and is presented in form (14):

$$\sum_{j=1}^{n} Kbcs = Rj, \ \text{j=1,2...n} \quad (14)$$

The second group of *n* equations expressed the requirement to satisfy the requires (amount of threats by cyberspace zones) of all *n* users (covered by the protection activities) completely and is presented in (15):

$$\sum_{i=1}^{m} AUij = Si, \ \text{i=1,2...m} \quad (15)$$

On the basis of the nonnegativity of transposition volumes the mathematical model is as follows: (16):

$$\begin{cases} f(Xbcs) = \sum_{i=1}^{m} \sum_{j=1}^{n} AUij * Kbcsij \to \min \\ \sum_{j=1}^{n} Kbcs = Rj, \ \text{j=1,2...n} \\ \sum_{i=1}^{m} AUij = Si, \ \text{i=1,2...m} \\ Kbcs \geq 0, \ \text{j=1,2...n; i=1,2...m} \end{cases} \quad (16)$$

In this model of the transport task "It is assumed that the total supplier resources cyberinformation or cost protection per the zones of cyberspace are equal to total" customer demands» (the cost of possible economic damages) or likely possible damage amounts for the same zones of cyberspace, i.e. view (17):

$$\sum_{j=1}^{n} Kbcs = \sum_{i=1}^{m} AUij \quad (17)$$

This type of transport task is called the task with the right balance, and the model is closed.
If it fails, then the task is called a task with the wrong balance and model task is open.

References

[1] ISO/IEK 27032 2012 *Information technology. Security methods. Guidance to ensure cybersecurity* Available at: https://www.iso.org/standard/ 44375.html
[2] MODU 9/99 "Profits", *approved by the Decree of the Ministry of Finance* of 06.05.1999 № 32n.
[3] Boehm B W 1988 *Tutorial Software risk management* (IEEE Computer Society)
[4] Boychenko O V, ed 2018 *Information security Economics: cost approach* (Simferopol)
[5] Tulupov A S 2010 Theory of prejudice as a basis for assessing the adverse externalities in the economy *Herald of the University (State University of management)* **2** 92-97
[6] Sauerwein C, Pekaric I, Felderer M and Breu R 2019 An analysis and classification of public information security data sources used in research and practice *Computers & Security* **82** 140-155
[7] Havur G, Steyskal S, Panasiuk O, Fensel A, Mireles V, Pellegrini T, Thurner T, Polleres A and Kirrane S 2018 DALICC: A Framework for Publishing and Consuming Data Assets Legally *Int. Conf. on Semantic Systems (SEMANTICS), Poster&Demo*
[8] Mandritsa I V, Peleshenko V I, Mandritsa O V, Fensel A, Tebueva F B, Petrenko V I, Solovieva I V and Mecella M 2018 Defining a cybersecurity strategy of an organization: criteria, objectives and functions *Integrating Research Agendas and Devising Joint Challenges. Int. Multidisciplinary Symp. ICT Research in Russian Federation and Europe* pp 199-205
[9] Bogatinoska C and Cvetkoski A 2018 The influence and future of cryptocurrencies *Regional determinants and patterns of economic development. The materials of the int. scientifically-practical conf. The editor in Chief of Ob Bigdaj. Russia, Stavropol, 18-20 April 2018* pp 14-16
[10] Mecella M 2018 Research and business opportunities for process mining *Regional determinants and patterns of economic development. The materials of the int. scientifically-practical conf. The editor in Chief of Ob Bigdaj. Russia, Stavropol, 18-20 April 2018* pp 82-84