Theoretical Basis of Economics of Cybersecurity Organization

Igor Mandritsa, Massimo Meccello, Anna Fensel,
Dijana Capeska Bogatinoska, Irina Solovieva,
Vyacheslav Petrenko and Olga Mandritsa

June 23, 2021

Theoretical Basis of Economics of Cybersecurity organization

Mandritsa I.V.[1], Massimo Meccello [2],Anna Fensel[3], Dijana Capeska Bogatinoska[4]
Solovieva I.V.[1], Petrenko V.I.[1] and Mandritsa O.V.[5]

[1] North-Caucasus Federal University, Institute of Information Technologies and Telecommunications, 1, Pushkin Street, Stavropol, 355009, Russia

[2] SAPIENZA University, DIAG, formerly DIS - Department of Computer, Control and Management Engineering, Via Ariosto 25, I-00184 Rome, Italy

[3] University of Innsbruck, Department of Computer Science, Technikerstr. 21a, A-6020 Innsbruck, Austria

[4] St. Paul the Apostle" Ohrid, "University of Information Science and Technology" Macedonia

[5] Russian Technological University - MIREA, Branch office, Department of regional Economics, 8, Kulakov street, Stavropol, 355035, Russia

imandritsa@ncfu.ru

Summary: This article proposes a theoretical concept of economic construction of cyber-protection, as an integral part of cyber security and all its elements: information security, network and Internet security against modern threats for organizations. At first, such categories as cyberinformation, economics of cybersecurity, and classification of the concept of «Damages from loss or cyber information» and its value of content in the form of loss of business information are introduced.

Keywords: Economics of cybersecurity, the cost of protecting information units of cybersecurity, security information.

1. Introduction

The notions 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 on January 10th, 2014, has not been accepted, and there are no prerequisites to its scientific and practical recognition due to the position of the Russian Federal Security Buro. Despite of this, the «cyber-" terminology should be taken into account, since the issues of cybersecurity are established in the international community, and in particular, International Standard ISO/IEC 27032:2012 (ISO/IEC 27032:2012) Information Technology Security Techniques - Guidelines for Cybersecurity [1] describes the concept of "cybersecurity" and its relation to other categories of information security.

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 cyberspaces. In turn, the security of critical information infrastructures, though related to cyber security (as it is understood throughout the world), is addressed only partially. The standard provides the diagram that visualizes the relationship of the various terms (translated by the authors), see Figure 1. 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 [1], the definition 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 all of the possible threats and impacts with undesirable consequences."

2. Methods

One of the relevant conditions is the economic evaluation of the rationality of the protecting cyberspace entity methods from the all of the possible threats and impacts with undesirable consequences.

The subject of our study is the cyber information users, both individuals and legal entities, that are part of the information system in the state, in a region or a locality. All cyberinformation of either private (physical) person or legal organizations (firms) can be divided into two groups: with a value and without a value. The part of cyber information which brings its owner(s) some income is considered to be the information that has a value or business information.

However, the market for business information is not broadly available, because e.g. today you do not find the ads such as «buy information» or "sell information».

The cyberinformation which is to 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 generation. Since then, the defense economy cyber information as the future value of its protection threats is born, and at this moment the rationality of the cyber information owner's conduct concerning its protection is required and a reasonable and rational economic behavior is expected.

Rationality implies the reasonableness of spending money on the protection of cyberspace and cyber data of the subject of this space, and not irrationality, when the subject to make a decision in the field of information protection comes from the principles of freedom of amounts or resources spent on the protection of their information.

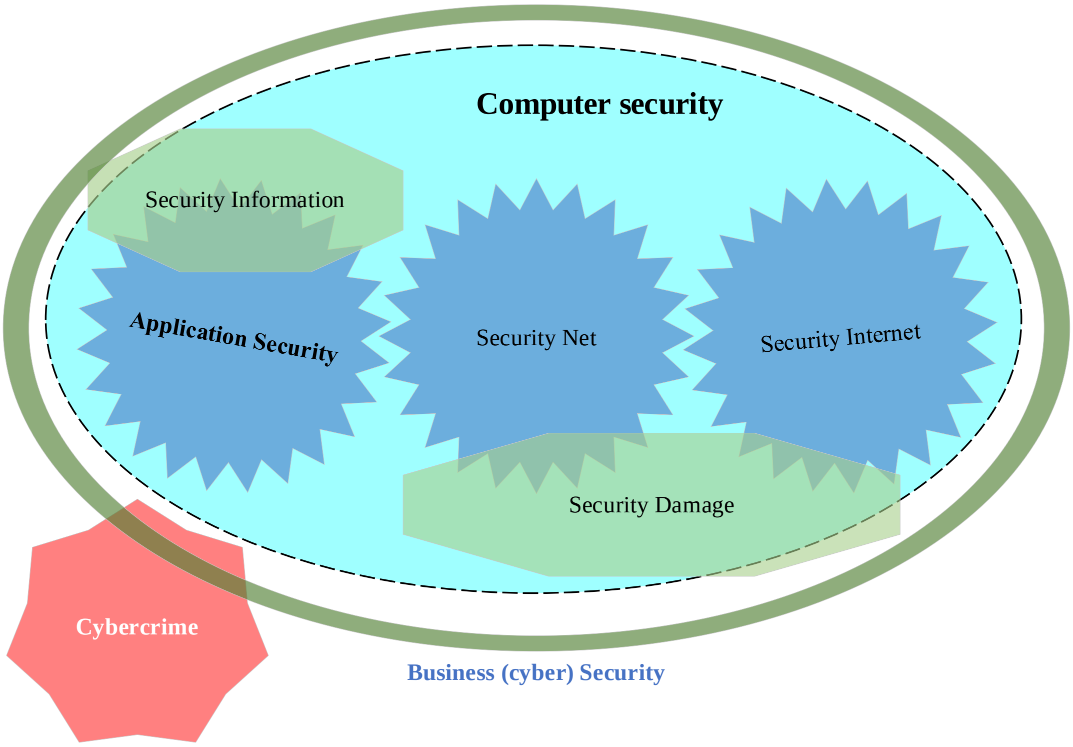

Figure 1- *Cybersecurity* according to ISO/IEC 27032:2012

Cybersecurity relates to network security, application security, Internet security, and the security of critical information infrastructures from the perspective of Western experts. Thus, cybersecurity and information security should be distinguished as two separate 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:

SI (X) - Security Information object X,

SNet (X) - Security Net object X,

SInet (X) - Security Internet object X,

SD (X) - Security Damage critical information infrastructure facility, as the sum of *SNet (X)* и *SInet (X)*.

And thus, the Figure 1 can be transformed into the new dependency of safety factors listed above as shown in Figure 2. The authors introduce the cyberinformation of an organization category as the sum of all valuable information (economic profit, usefulness) which is to bring an income for the organization in future.

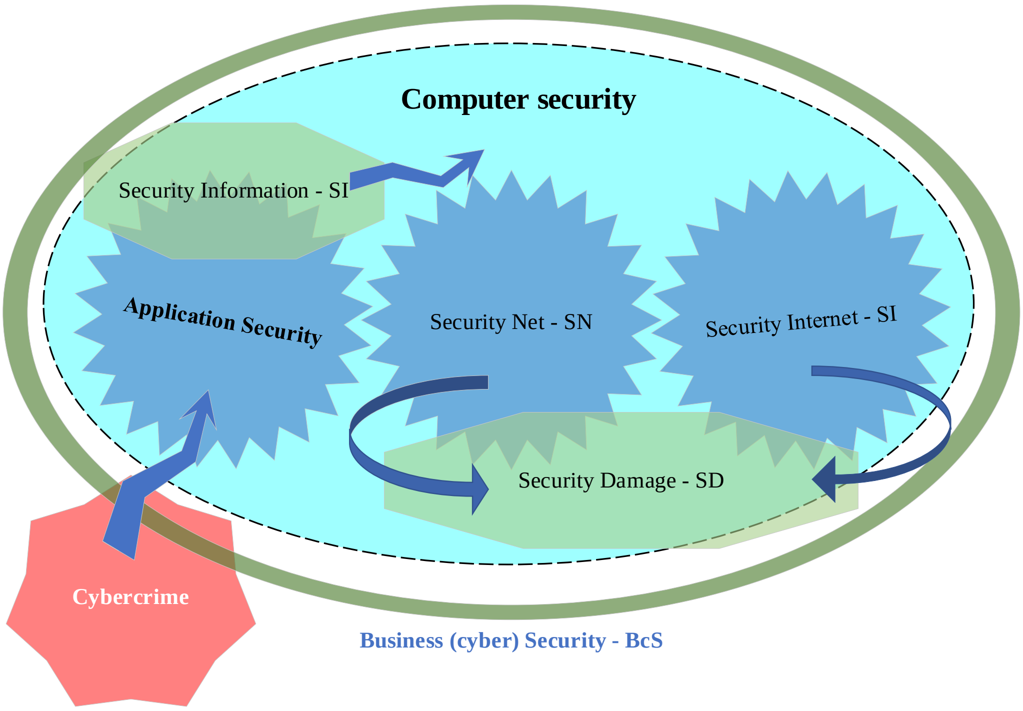

Figure 2 - Theoretical basis of Economics of cybersecurity
(newly introduced category)

The accounting 9/99 "Profits" for the Russian business environment defines the organization's income (in our case review-income from the cyber information): "Income which the organization recognizes is 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 the organization. Thus, from the moment when the cyberinformation, consisting of business information, is beginning to bear its owner's income rises the question of its rational protection against cybercrime.

3. Discussion 1

Here, we relate to the scientific field of this research: economics of cybersecurity organization. Accordingly, the theft of cyber information containing business information is a kind of enrichment, or thief's "clean" profits, as at the level of an individual physical person, and at a higher level of an economic involvement of criminals in this type of activity. Thus, any cyber information that brings benefits has value, and is business information that fills the country's economy with added value, which later becomes the "wealth" of its people. [2]

In this case the agents (physical cyber information owners and legal structure of society) and the state, creating valuable cyberinformation raises unnecessary expenditure on the organization of workplaces, the maintenance of market conditions and other economic categories. A company's cyberspace as a legal entity has the highest relevance for our study, for example of a commercial company (organization), or a budgetary organization.

It is more reasonable to protect cyberinformation than just to lose it, to make senseless publicity and thereby generate a competitor to the detriment of your business, as well as to reduce the cost of your information (business information). At the moment, the cyberspace (the network perimeter, information units and the organization of interaction with the external environment of the Internet) of the company is organized under its network perimeter (periphery), as follows (see Figure 2) [3].

RESULTS 1

As a result, the cumulative state of an object cybersecurity (company) *X*, -according to Figure 1) *Xbcs* 2 will consist of three above-mentioned components (1):

$$X_{bcs} = \sum (X_{SI} + X_{SNet} + X_{SInet}) \qquad 1$$

Accordingly, then the target function of economics of cybersecurity to protect or cyber information object *X* will be covered by expression (2), if we think economically rationally and reasonably:

$$f(\mathrm{X}) \rightarrow \max BcS \qquad 2$$

However, cybercrime discretely manifests itself in the form of a certain probability that the threat of cyber information leakage will arise or not arise for object X.

It should be noted that the category of threat (risk) **ρ** (term) - there are the risks of cyber information diversion. This category is dynamic, it is not constant at different stages of the organization's life. For organizations which are already losing its competitive advantage the risk of leakage is reduced, and vice versa for startups the relevance of diversion is high.

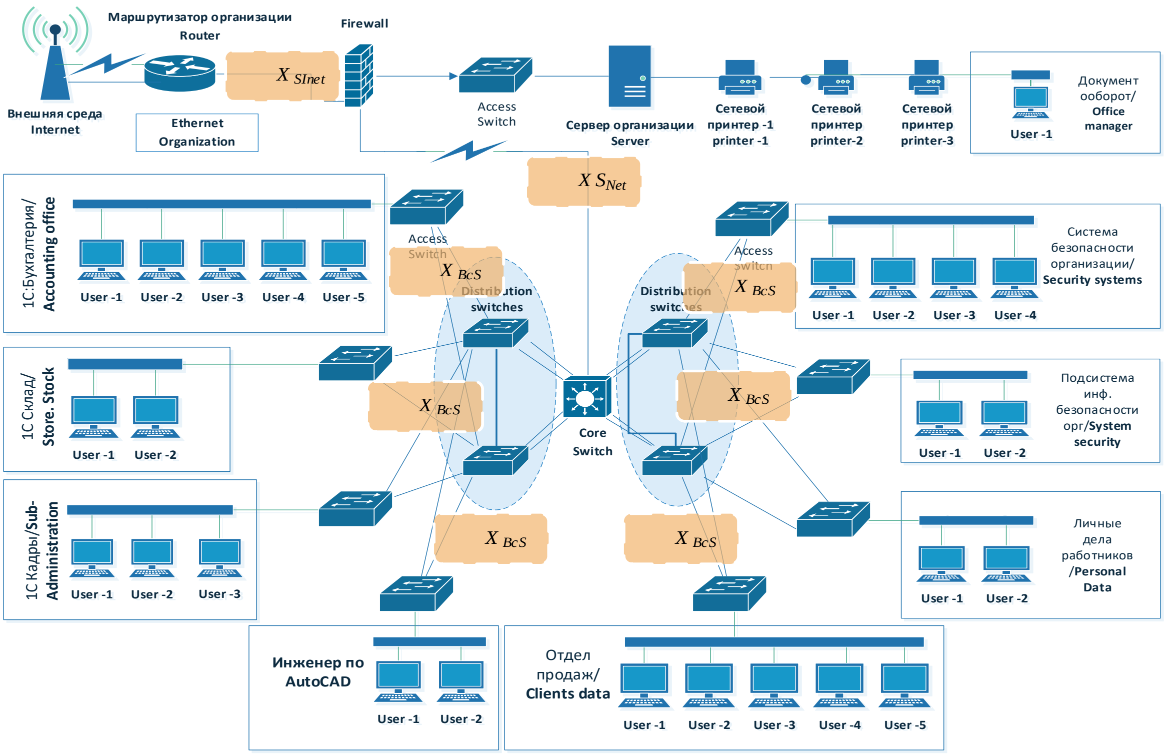

Figure 2 – The cyberspace localization for an organization (firm) used for determining the cost of cyberinformation protection [3]

The above-mentioned information makes it necessary to introduce a new category: the damage possibility from losses (cyber information), and the second category: the seriousness effect on cyberinformation by the threats' channel.

For example, we use the current cyber-attack known to all specialists cyber-DDoS-attack (Distributed Denial of Service — «denial of service»). This is an attack on the firm's website, with the main aim of breaking the website by making a large number of spurious requests. The economics point of view here has two characteristics: the likelihood of damage and amount of damages from loss or cyberinformation (cyber information). The formula of the risk for cyber information R (RE) is well known (3) [2, c.6]

$$R=\rho U\ (\text{Threat})*CU\ (\text{Threat}) \qquad (3)$$

Where: ρU (Threat) – the likelihood of threat cyberinformation, relative number;

CU (Threat)-the amount of possible damage from the cyberinformation (loss) in rubles.

Having entered the category of risk and severity of threats from leaking the cyber information, it is necessary to describe philosophically what is a "Damage" loss (leakage) or cyber information. Correspondently, expression (1) is converted into the following (4):

$$X_{bcs} = \sum (X_{SI} + X_{SNet} + X_{SInet}) - (\rho U\ (_{\text{Угрозы}})*CU\ (_{\text{Угрозы}})(\mathrm{X}_{bcs}) \qquad 4,$$

The authors assume that the damage of cyberinformation loss (and its value content as business information) entails the consequences for its owners, as depicted in Table 1.

4. Discussion 2

The variety of damage-forming manifestations for the topic under investigation, determining the occurrence of an undesirable event-loss (loss) of information, confirms the need for a clear delineation of the possible types of damage from the loss of cyber information, depending on the aspect of the review.

In this study, the authors propose a classification of damages for cybersecurity of the organization based on a number of grounds for division, which determine the most common signs of the original concept - "damage from loss of cyber information", which is necessary both to identify the kind of damage that can be provided by measures to protect the cyber information of the object, and implementation of accurate complex calculations of the economic damage under consideration as a result of hacker attacks on the grounds:

1. Formation space;
2. Origin;
3. Type of initiating impact;
4. Type of manifestation;
5. Field manifesting;
6. Industry the emergence;
7. Scope of proliferation;
8. The level of consideration;
9. Amount;
10. Forecasting;
11. Reversibility of effects;
12. The frequency of application;
13. Thrust causing;
14. Manifestation;
15. Perception;
16. Localization;
17. Time of application;

18. Identification;
19. Homogeneity of objects;
20. The possibility of extending;
21. Sequence manifestations.

5. Results 2

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

$$f(\mathrm{X}) \rightarrow \max\ (BcS - (\rho U\ * \mathrm{C}U)(\mathrm{X}\ (\mathrm{Threat})) \qquad 5$$

i.e. reducing threats for object X, we reach the maximum reasonable limit of the object's 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 (6).

$$K_{bcs}(\mathrm{X}) = \frac{\sum Z\ cyber\ defence\ (\mathrm{X}bcs)}{S\ cyberinformation\ (\mathrm{X}bcs)} \qquad (6)$$

where is:

$\sum$ Z 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 (cyber information) cybersecurity localization of the object X_{bcs}.

Thus, the expressions 4, 5 and 6 will take a "matrix" view (7 and 8), on the basis of the correspondence between tables localization of cybersecurity and the likelihood of threats to this localization per the amount of its damage, that can be calculated by the simplex method (Table 2).

These tasks are linear programming tasks and can be solved by the famous simplex method. In our case we have a typical "transport task", let us call it the task of cybersecurity for the object X.

Table 1- Classification of the concept of " cyber information"
(and its value content in the form of loss business information) (introduced for the first time)

The Foundation Division	*Damages from loss or cyber information*				
Formation area	Natural (natural)		Artificial (man-made)		
	The human factor	Depreciation of equipment	External area		Internal area
The nature of the occurrence	Emergency		Operational		
Display	Actual (come, happened or realized)		Partially taken place		Potential (expected)
	Past (retrospective)	The current, present			
Type of initiating	As a result of other human actions	As a result of Virus attack	Due To SPAM	Due to DDoS attack	As a result of other hacker attacks
The field of formation	As a result of economic activities		Social, non-manufacturing time		
The level of consideration	Moral damages		Economic harm to the subject of economic activity		
Direction of infiction	Focused (intentional or planned)		Random (careless or natural)		
Forecasting	The predicted		Unexpected		
Reversibility of effects	Reimbursed		Non-reimbursed		
Coverage, dissemination	Local	Across the Organization, company	In the scale of region		Global (country) or continental.
Rate of damage	Minor	Moderate (average)	Large (a large, substantial, significant)		Catastrophic
Identification	Identified (recognized)		Unidentified (unrecognized)		

Table 2 - Initial data for cybersecurity transport tasks cybersecurity – a calculation of damages' possible values

$R(Xbcs)$ $S\ bcs\ (X)$	$R_{SI}=\rho U * CU(_{SI})$	$R_{SNet} = \rho U * CU(_{SNet})$	$R_{BInet} = \rho U * CU(_{SInet})$
S_{SI}	CU_{11}	CU_{12}	CU_{13}
S_{SNet}	CU_{21}	CU_{22}	CU_{23}
S_{SInet}	CU_{31}	CU_{32}	CU_{33}

This transport task integrates a wide range of tasks with a single mathematical model. However, a basic transport task has a large number of variables and solving it by the simplex method is cumbersome.

On the other hand, the matrix of system's limitations applied to the "transport task" is very peculiar, so the special solution methods have been developed. These methods, as the simplex method, allow to find an initial support solution, and then improve it, get a sequence of reference solutions, which culminates the optimal solution. The conditions of the "transport task" (we use the initial formulations) are:

"The Homogeneous value" (in this case the cost of cyber information protection S (Xbcs) in its area of concentration CU in the object X) focus on *m* suppliers c*yber localization CU*) in the "volumes" (with the cost of this or cyber information):

a1 *(S_{SI}*), a2 (S_{SNet}), a2 (S_{SInet}).

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_{SI}), b2(R_{SNet}), b3(R_{SInet}).

Thus, we set the possible damage amount for information on cyber security localizations, namely:

$CUij$, $i=1,2,...m; j=1,2,...n$

CUij— probable amounts of damage in the localization of cybersecurity "of the cost of transporting cargo units from each i-supplier to each j-th consumer".

Table 3 shows the conditions of the transport challenges of cybersecurity.

Table 3- Initial data for transport tasks-calculation sums on cybersecurity protection against threats

$Z(Xbcs)$ $S\ bcs\ (X)$	Z_{SI}	Z_{SNet}	Z_{SInet}
S_{SI}	$Kbcs_{11}$	$Kbcs_{12}$	$Kbcs_{13}$
S_{SNet}	$Kbcs_{21}$	$Kbcs_{22}$	$Kbcs_{23}$
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 cyberspace localization in object X or coefficient cybersecurity (formula 8)) from every i- supplier to ever j- consumer.

6. Results 3

As a result, we obtain the matrix of the likely amounts of damage from threats to cybersecurity localization and second matrix of costs for the data protection in the cybersecurity localization of cybersecurity threats' values. These variables can be written in the form of matrices "transport", see formulas 7 & 8:

Threat localizations of cyberspace object X:

$$\text{CU}=\begin{matrix} CU_{11} & CU_{12} & CU_{13} \\ CU_{21} & CU_{22} & CU_{32} \\ CU_{31} & CU_{23} & CU_{33} \end{matrix} \qquad 7$$

The cost of the protection localizations in the object X:

$$Kbcs = \begin{matrix} Kbcs_{11} & Kbcs_{12} & Kbcs_{13} \\ Kbcs_{21} & Kbcs_{22} & Kbcs_{32} \\ Kbcs_{31} & Kbcs_{23} & Kbcs_{33} \end{matrix} \qquad 8$$

It is necessary to compile the "roadmap" to calculate the value cybersecurity protection factor for the object X, where "the reserves of all suppliers (threat amounts of damages)" removed entirely (covered (protected) localization protection activities cyberspace), requests for all consumers are met completely, and total expenses "for the transportation of all volumes (coefficient of cybersecurity for the localization) are minimal". As the product of *CUij* Kbcsij* defines the cost of volume transportation "(the cost of the cyberspace protection localization in correlation with the value of this threat localization) from the i-supplier of j- consumer, total expenses" all the transportation volumes "(the amount of the cyberspace protection localization) are equal. I.e., we get the following expressions 9 & 10:

$$\sum_{i=1}^{m} \sum_{j=1}^{n} CU\ ij * Kbcsij \qquad 9$$

Following the objective of our work, we want to provide a minimum total cost of protection for the localization in the object X. Consequently, the target function is presented for the localization:

$$f(\mathrm{X}) = \sum_{i=1}^{m} \sum_{j=1}^{n} CU\ ij * Kbcsij \ \rightarrow min \qquad 10$$

The best solution of our problem is to find a minimum value of spent cost on cyber information protection activities for each threat and the probable amount of damage for cyberinformation (cybersecurity) in the object X. The task's constraints system consists of two groups of equations.

The first group of *m* equations describes the fact that "reserves" (the cost of protection or cyber information correspondence with its execution value) of all *m* (supplies localization of cyberspace) is removed completely and is presented in form (11):

$$\sum_{i=1}^{n} \ Kbcsij = Rj, \ \text{j=1,2, m} \qquad 11$$

The second group of *n* equations expresses the requirement to satisfy the requires (threats by cyberspace localizations) of all *n* users (covered by the protection activities) completely and is presented in (12):

$$\sum_{j=1}^{m} \ CU\ ij = Si, \ \ \text{i=1,2, n} \qquad 12$$

On the basis of the nonnegativity of transposition volumes the mathematical model is as follows: (13):

$$\begin{cases} f(\mathrm{X}) = \sum_{i=1}^{m} \sum_{j=1}^{n} CU\ ij * Kbcsij \ \rightarrow min \\ \sum_{i=1}^{n} Kbcsij = Rj, \ \text{j=1,2, m} \\ \sum_{j=1}^{m} CU\ ij = Si, \ \ \text{i=1,2, n} \\ Kbcsij \geq 0, \ \text{j=1,2, m, i=1,2, n} \end{cases} \qquad 13$$

In this model of the transport task it is assumed that the total suppliers’ resources cyberinformation or cost protection per a localization of cyberspace is equal to total "customers’ demands» (the cost of possible economic damages) or likely possible damage amounts for the same localization of cyberspace, i.e. view (14):

$$\sum_{i=1}^{n} Kbcsij = \sum_{j=1}^{m} CU\ ij \qquad 14$$

This type of transport task can be called as 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.

7. Conclusion

The cyberspace localization for an organization (firm) is shown to be applied for determining the cost of cyberinformation protection. The authors assume that the damage of cyberinformation loss (and its value content as business information) entails the following consequences for its owners.

The authors get the expression of cybersecurity in the form of formula (5) to reducing threats for object X and 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 cyberdefense, which will be based on the ratio of economic indicators. The authors suggest the model of the transport task to solve the calculations related to the defense from all kinds of treats for cybersecurity of organization. It assumes that the total suppliers’ resources cyberinformation or cost protection per the localizations of cyberspace are equal to total `customers’ demands (the cost of possible economic damages) or likely possible damage amounts for the same localizations of cyberspace.

The best solution for the cybersecurity of organization is to find a minimum value of spent cost on cyber information protection for each of the threats in relation to the potential amount of damage for cyberinformation in the object.

8. References

1. ISO/IEK 27032 2012. «Information technology. Security methods. Guidance to ensure cybersecurity». 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 № 32н.
3. Tutorial Software risk management, B. W. Boehm, IEEE Computer Society, 1988.
4. Information security Economics: cost approach, Boychenko O.V., Mandritsa I.V., Mandritsa O.V., Solovieva I.V., Antonov V.V., Petrenko V.I., Rybnikov A.S., Rybnikov M.S., Korolev O.I., etc. Monograph/edited by O.V. Boychenko. Simferopol, 2018.
5. Theory of prejudice as a basis for assessing the adverse externalities in the economy, Tulupov A.S., Herald of the University (State University of management). 2010. № 2. C. 92-97.