EasyChair Preprint

№ 7251

Methods of Approaches to the Development Cybersecurity Strategy of an Organization. Criteria, Objectives and Functions

Ilya Shumov and Igor Mandritsa

December 23, 2021

Methods of approaches to the development cybersecurity strategy of an organization. Criteria, objectives and functions

Ylia Shumov[1], Mandritsa I.V.[1],

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

{ meggavat@gmail.com, d_artman@mail.ru}

Abstract. the questions of the strategic planning of the information cybersecurity of an organization are considered. The mathematical model setting of the strategic plan of the cybersecurity of the organization is carried out. The factorial description of the mathematical model of the strategic plan of the organization has been implemented.

Keywords: strategic planning of the information cybersecurity of the organization; criteria, objectives of the mathematical model; factors of the model.

Introduction

Considering the strategic plan of the cybersecurity of the organization (futher ICO) like a system of case-operations of an information security (futher IS) which aims to condition managing of its cyber protection, it has been noted that each of the carried out activities of an administration, is an expensive process (spending on, cost of IS).

In so doing the costs of (resources) the organization is limited, Consequently the issue of choosing the rational composition of case-actions to improve the organization's cyber-security is the main objective of the strategy.

Discussion

We share the view [1], that regular strategic management (futher strategic manegement) can be represented as a process, that determines the sequence of actions of the organization for developing and implementing a

strategy (in our context - the strategy of cybersecurity and its main indicator of the cyber-protection).

In the authors' opinion, cybersecurity is the process of developing methods, security policies and implementing measures to protect information systems, networks, and cyberspace applications of the organization from digital (computer) attacks.

In itself, the process of strategic planning involves setting goals for achieving the future state of high cybersecurity of the organization, and accordingly developing, the strategy that will enhance it, by identifying the necessary resources and methods of protection by developing case studies on the channels of organization threats.

From the foregoing it follows that the strategic management of cybersecurity has been emerged through evolutionary development from the strategic planning of the state of cybersecurity of the information environment of the organization, which constitutes its essential basis. The essence of the changes that has been taken place in the information environment of the organization from the position of cybersecurity is reduced to breaking up the process of strategic planning of its cyber-security into three interrelated, but at the same time independent activities corresponding to the basic functions of cybersecurity management:

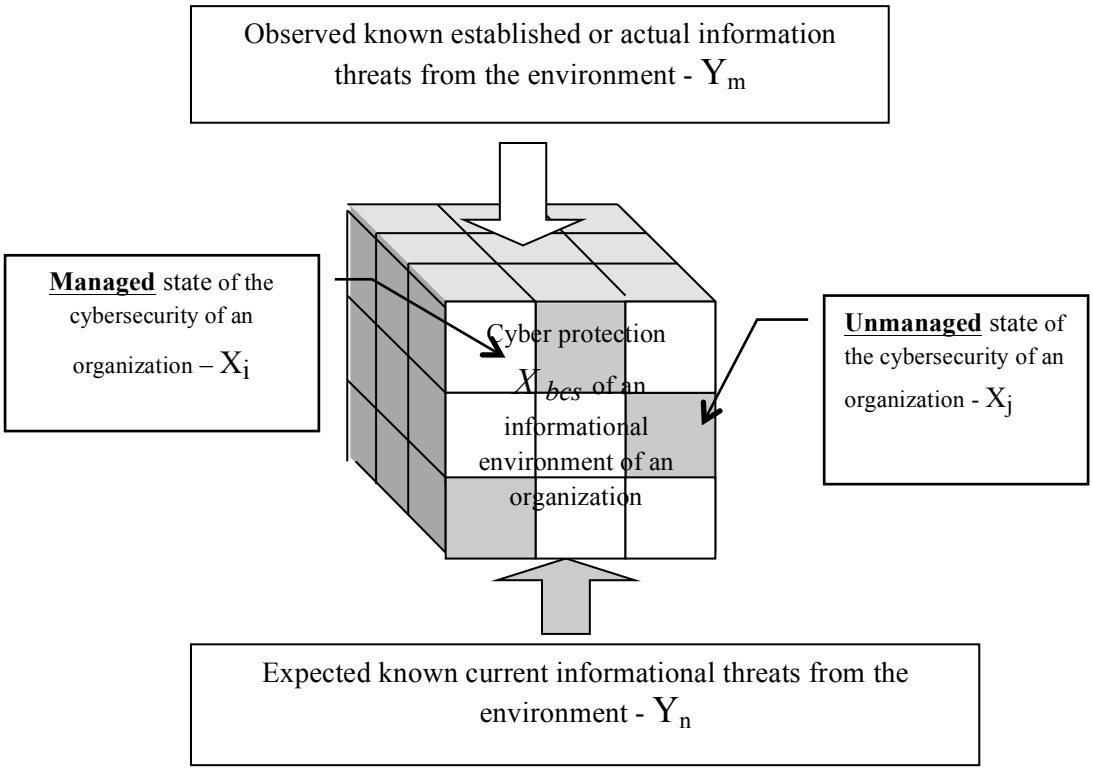
1) the development of the cybersecurity strategy based on an analysis of the external and internal environment of the information environment of the organization, consideration of possible alternatives;

2) organization of the strategy (case-based cybersecurity) by the criterion of maximum cyber-security with a minimum of cost options;

3) monitoring and evaluation of the results of cybersecurity, before and after implementation of case-events.

We will also consider the issue of forming an economically effective (rational) strategic plan for the ICO. We will determine that the efficiency of the strategic plan of the ICO is understood as the maximum of the ratio of

the final level of the cyber-security of the organization, in the form of the ratio of the amount of value available to the organization methods of countering threats (the cost of the reporting period for the IC activities) to its initial (basic) level. Figure 1 depicts this basic condition for managing cyber security factors of the organization.



Picture 1 –Information environment of an object and factors of the strategical managing its cybersecurity

From a mathematical point of view, it can be seen that all the factors affecting the input Yij or the output parameters of ICO object Xi, causes changes in its state of cyber-security from the position of its effectiveness.

It means that for describing the model of strategic management of cybersecurity of the organization, that along with the cost process (IC case-events), it is necessary to consider input values and output values of the probability of threats for the whole system of ICO, also any factors affecting them from the external environment.

There are many parameters for accounting of the ICO mathematical model.

Result

According to [2], the formalization of cybersecurity has as a cumulative state of cybersecurity of some organization X_{bcs}, which has three components in its composition:

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

Where:

SI (X) - information security of an object X,

SNet (X) – network security of an object X,

SInet (X) – internet security of an object X,

Accordingly, if you think rationally and reasonably, then the target function of the cybersecurity economy of the object X, in the form of cybersecurity index of the information environment of this organization X, will tend to expression (2):

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

However, cybercrime shows itself impermanently in the form of a certain probability that the threat of leakage of cyber information will appear or will not appear for the object X. From the position of the economy, it is accompanied by two characteristics: the probability of occurrence and the amount of possible future damage from loss of cyber information.

The formula of risk of threats of leakage and possible damage for cyber information R (RE) is well known [2]:

$$R=\rho U (Threat)*CU (Threat) \quad (3)$$

where: ρU (Threats) – the likelihood of a threat of damage to cyber information, the relative number;

CU (Threats) – the amount of possible damage from the leak (loss) of cyberinformation, rubles.

Introducing the categories of risk and the severity of threats from the leak should be philosophically deciphered (comprehend), what "Damage of

loss" of cyberinformation (leaks) are. Accordingly, expression 1 is converted to the following (4):

$$X_{bcs} = \sum (X_{SI} + X_{SNet} + X_{SInet}) - (\rho U_{(Threats)} * CU_{(Threats)})(X_{bcs}) \quad (4),$$

As a result of the arguments above, we get a verbal model of the strategic plan for cybersecurity of the information environment of the organization, presented in Figure 2

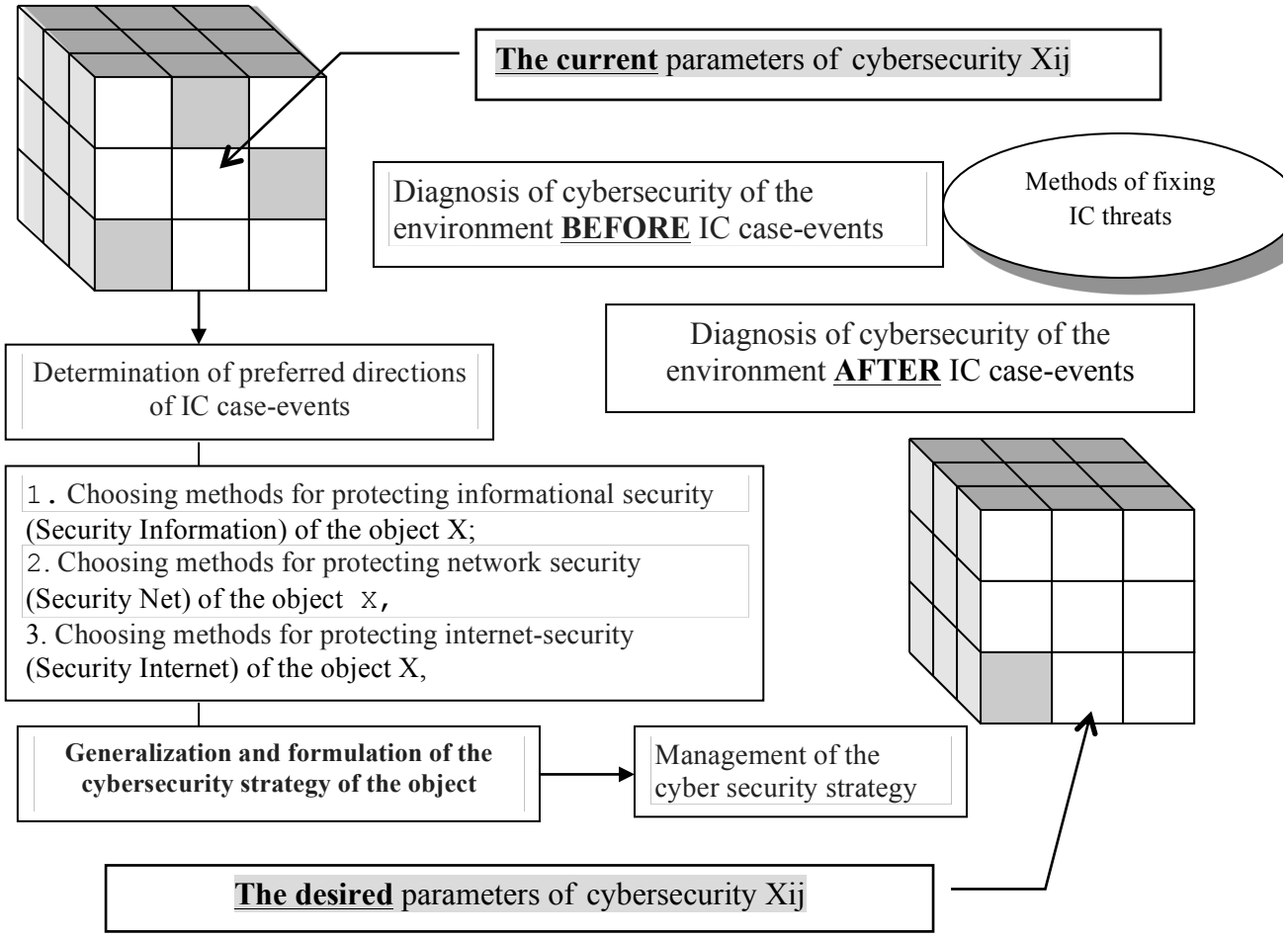


Figure 2 – stages and purpose of the ICO

To clarify the mathematical formulation of the multicriteria task of ranking the operational case-events of information security for the process of enhancing the cybersecurity of the organization X in Figure 2. The parameters of the initial ICO system will be considered as parameters of the model. We will define the list of them in the form of the X_{ICO} vector (5):

$$X = \{X_J, j = 1...N\} \quad (5)$$

In our case, x1, x2, ..., xn a list of possible strategic, costly planned case-events of the CS. In this case, n is the number of blocks of the lowest level of decomposition of the strategic plan. There are some limitations on the interrelated parameters of the system of strategic case-events. The functioning of the ICO system is determined by a set of target characteristics which depend on the parameters of this system (6):

$$F(X) = \{f_k(X), k = 1....K\}. \quad (6)$$

In the case of strategic planning of the ICO $K_{ISO}=3$.

The objective characteristics of the strategic cost-intensive business events of IS are:

1. The effectiveness of investing in the protection of information security, the level of risk for each channel of threats, the degree of strategic significance of this IC activity as part of the strategic plan of the ICO. We denote them by f_1, f_2 and f_3, respectively.
2. The effectiveness of investing in the protection of information security in this case will be considered as the profitability of a separate strategic activity of the IS for assessing the cybersecurity of the ICO.

Let us dwell in more detail on the determination of the level of risk through the channels of threats of the ICO. We propose the following methodology for assessing the level of risk:

- Identifying the full set of risks of a strategic case study for protecting CS of the organization (Figure 3).
- Expert poll and determination of the strategic goal-setting levels affecting this i-th risk of the case-study of the strategic plan of the ICO. $i=1...I$.

- Determination of the dimension (area) of the matrix of the cumulative risk of the strategic case-event IS: since the number of levels of strategic goal setting is seven, then 7*I.
- Determination of the risk field area S_{risk} as the number of risk units of the matrix of the combined risk of the strategic CS case-study.
- The level of risk can be determined by the formula:

$$f_2 = \frac{S_{Risk}}{7 \times I} \qquad (7)$$

3. The degree of strategic importance of the CS event is proposed to be determined expertly as the degree of influence given to the event-action on the final result of the strategic plan of the CS (in fractions of a unit).

The degree of strategic importance of the IC activity is proposed to be determined expertly as the degree of influence of this IC activity on the final result of the strategic plan (in fractions of a unit). The optimization problem follows from the foregoing: to choose from the set of acceptable values such parameters of cyber-security of the whole IC organization, so that its performance indicators (target characteristics of cybersecurity through threat channels) are in the optimal range. For our case, the indicators should be maximal [2] (8):

$$f_k(X) \to \max, k = 1...K \qquad (8)$$

Assuming the non-negativity condition xi as a constraint, we obtain a system of equations and restrictions (9-11):

$$x_i > 0 \qquad (9)$$

The complexity of the task is determined by its multicriteria nature, and the main task is to choose the principle of optimality.

If the points of the optimum Xi * obtained by solving the problem for each criterion do not coincide separately, then the solution of the problem can be only some compromise solution that satisfies all the components of

the vector criterion F (X). A point X0 satisfying conditions (10-12) is Pareto optimal if there is no other point X1 for which (10):

$$f_k\left(X^1\right) \geq f_k\left(X^0\right), ë = 1...K, \qquad (10)$$

And the strict inequality should be completed at least for one of the criteria's. A set of such points is called a Pareto set. They are also called the set of "unimprovable points", because you can not find such another point for no one of them, so that one of the criteria improves, and the rest do not deteriorate. Each CS case-event, depending on the value of the indicators of the amount of investment, risk level, the degree of strategic importance of the CS activities in the composition, the strategic plan of the ICO will be assigned the appropriate rank, and the maximum rank will correspond to the IC event, the investment of which should be primarily implemented.

We represent the solution with a point on the plane with the coordinates f_1 and f_2. We number the points according to the number of the solution (Figure 4).

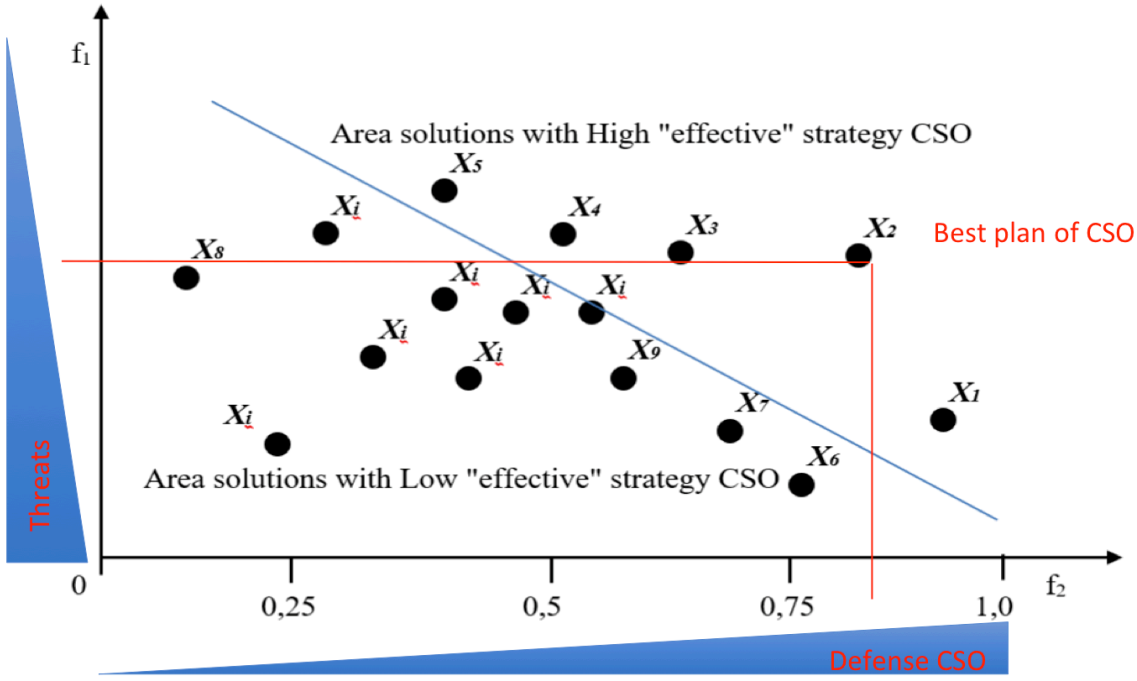


Figure 4 - Correlation of Pareto sets in coordinates «effectiveness of investment in case-activities IS - level of risk of CSO»

Figure 4 - Correlation of Pareto sets in coordinates «Effectiveness of investment in case-activities IC - level of risk of ICO»

Following the indexes of the figure 4, only the solutions x_1,x_2,x_3,x_4,x_5 lying on the right upper boundary of the domain of possible solutions for the protection of information security as part of the overall strategic plan of the ICO are optimal. For any other solution of the CS x_i, there is at least one dominant, for which both f_1 and f_2 are greater than for xi. The allocated "effective" set of solutions for protecting the CS x_1,x_2,x_3,x_4,x_5 will be the Pareto set

This set will be "effective" according to two criteria - minimum costs for a case-event and maximum security.

By transmitting the IC events of this set by the criterion f_3, we will receive a list of IC case-events for implementation in order of decreasing of their strategic importance of the all cybersecurity.

If we consider the remaining possible solutions, that is, x1 without x1, x2, x3, x4, x5, then the solutions x6, x7, x8, x9 will be optimal for them. Thus, we get a lot of solutions to the index of cyber-security of the ICO, which will be less effective than the first one.

If we continue this process, we can obtain a sequence of solutions sets - successive Pareto sets, where each set will be less efficient than the previous one, but more effectively than the subsequent one. Within a specific set, the priority of decisions in descending order of their strategic importance is determined by the ranking of the case-activities of the IS of the given set by the criterion f3

The less number of successively less "effective" sets of strategic costly business events, that IB can achieve the main goal of the strategy with - the maximum cybersecurity of the organization, the higher its effectiveness is. Obviously, this process should be iterative with correction of business processes of the strategic plan. Another theory of multi-criteria sets is one of the approaches to solving multicriteria problems that most adequately reflect the conditions of functioning of the systems under consideration.

The theory of fuzzy sets allows best to structure everything that is divided by not very clear boundaries. To this end, membership functions that characterize the degree of closeness of a given element to a given set are considered in the theory of fuzzy sets. Let's consider the solution of the problem posed by the theory of fuzzy sets [3].

Let $X = \{x_1, x_2, x_3, ..., x_n\}$ be the collection of some objects. Then the fuzzy set L is the set of ordered pairs (11):

$$L = \{(x, \mu_l(x_i)), x_i \in X\}, \quad (11)$$

Where $\mu_l(x_i)$ is the degree of belonging of x_i to L. The function μ_l is called the membership function.

In our case, we assume that $\mu_l(x_i) \in [0...1]$. Thus, the fuzzy set L, despite the indistinctness of its boundaries, can be determined by comparing to each object x_i a number lying between 0 and 1. Two fuzzy sets L and M are said to be equal if and only if $\mu_l(x_i) = \mu_m(x_i)$, for all $x_i \in X$.

The intersection of fuzzy sets L and M is a fuzzy set, denoted by $L \cap M$ and that have the membership function (12):

$$\mu_{L \cap M}(x_i) = \min(\mu_l(x_i), \mu_m(x_i)), \text{ for all } x_i \in X. \quad (12)$$

A fuzzy goal $f(X)$ will be identified with a fixed fuzzy set L in X, and a fuzzy restriction $g(X)$ with a fuzzy set M. Then the fuzzy set F formed by the intersection of L and M is called the effective solution of the ICO's cybersecurity, i.e. F= $L \cap M$.

The main drawback of this method is the subjectivity of the administrative expert, who decides on the choice of a particular function.

Next, we suggest using the well-known technique of constructing the membership function, based on the ranking of the original arrays. We arrange the IS activities in order of increasing one of the given parameters -

in order of increasing profitability of investing in the protection of information security.

Then, for each IB event, we determine the value of *n/N*, where n is the serial number of the strategic case-event of the IC in an ordered sequence, and *N* is the total number of strategic costly case activities

Next, graphs are plotted in the coordinates "Cyber-security - *n/N*", "Risk level - *n/N*" and "Degree of strategic significance - *n/N*" and approximate the resulting point dependences. As a result, we get three functional dependencies:

$\mu_1 = \mu(f_1)$(cybersecurity),

$\mu_2 = \mu(f_2)$ (level of risk),

$\mu_3 = \mu(f_3)$ (degree of strategic importance).

which we will consider as a membership function. The use of these functions essentially means the normalization of the initial criteria. Next, it is proposed to use the verification of the criteria for obtaining the principle of optimality. As a verification, we consider the function (13):

$$\mu = \sqrt[3]{\mu_1 \mu_2 \mu_3} \qquad (13)$$

Each cost-based case-event of the IS corresponds to a specific parameter value μ . The maximum value of the parameter μ corresponds to the strategic expenditure event IC, which must be invested in the first place. Minimum - a costly IC event, which can be implemented in the last turn. That is, reducing threats for object X, we will reach the maximum-reasonable limit of cybersecurity security of the object.

As a result, the overall value of the current protection of the subject's cyber security can be expressed by the following indicator - the coefficient of cyber security protection, which will be based on the ratio of economic indicators (14).

$$K_{bcs}(\text{X}) = \frac{\sum Z \text{ защиту киберинформации (X}bcs)}{S \text{ киберинформации (X}bcs)} \quad (14)$$

Где: ∑ Z protection of cyber information (X) – amount of funds for the protection of cybersecurity throughout the facility and its component components for X_{bcs};

S - the cost of funds for the creation of cyber information on the zones of cybersecurity of the object X_{bcs}.

Conclusion

This assessment, along with other procedures, can be reflected in the methodological approach to transformations.

The essence of the process of increasing the cybersecurity of the ICO allows to choose two directions for evaluating of its results. The first direction requires the efficiency index of increasing the cyber security of the ICO as the ratio of all the components of the effect from the conducted case-events to all costs associated with the implementation of the cyber security transformation process.

The second direction considers the informational adaptation of an organization, which manifests itself in improving, reaching a new level of the response speed of an organization to the effects of external threats as the main result of increasing the cybersecurity of the ICO. For example, the components of the effect for the whole organization can be achieved through [4]:

- implementation of CS case-events at the level of Software used on all channels of the organization;
- streamlining the CS case-events for informational flows and the composition of informational arrays, including input, intrasystem and output information of the whole organization;
- implementation of CS case-events for each employee of the organization;

- Implementation of the CS case-events at the Hardware level as a result of the strategic plan of the IKO: conservation, access control, write-off of unused and worn out workstations.

The main components of the cost of interventions of CS case-events for the organization are:

- the costs of improving the IC protection in terms of the organizational units of an organization in terms of implementing the strategic planning system;
- to attract expert advisors for information and economic security;
- the training and retraining of the personnel in the IC part;
- the maintenance of the management of the organization;

The merits of this indicator include the fact that it allows you to determine the actual amount of the effect of the cyber-protection of an organization on the ruble invested in the implementation of the strategic plan of the ICO. At the same time, it does not reflect changes in the effectiveness of the cyber-security of an organization as a whole as a result of the process of increasing the cyber-security of the ICO.

Referens

1. Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace Brussels, 7.2.2013, JOIN (2013) 1 final.
2. European Union Agency for Network and Information Security (ENISA), 2017, Reproduction is authorised provided the source is acknowledged. ISBN 978-92-9204-239-4, DOI 10.2824/549292.
3. U.S. Department of homeland security cybersecurity strategy, May 15, 2018, Action Plan 2010-2015 for Canada's Cyber Security Strategy, Her Majesty the Queen in Right of Canada, 2013, ISBN: 978-1-100-21895-3.
4. W. R. King, D. I. Cleland, Strategic Planning and Policy Hardcover, November, 1978.
5. B. W. Boehm, Tutorial Software risk management, IEEE Computer Society, 1988.