Method of Optimal Planning of Cyberprotection Actions for a Corporate Information System

Aleksandr Litvinenko [0000-0002-8862-8032], Boris Maslovsky [0000-0002-9421-5410],
Oleksiy Glazok [0000-0002-1888-8779] and Anton Petrov [0000-0003-3731-4276]

National Aviation University, Kyiv, Ukraine
litvinen@nau.edu.ua, mbg@nau.edu.ua, glazok@nau.edu.ua

Abstract. The modern concept of cybersecurity management involves its consideration as a process of implementing a set of measures and activities organized into projects. This approach makes it possible to use the mathematical apparatus developed in the theory of cybernetic systems and project management for developing managerial decisions in the cybersecurity field. Based on this concept, a mathematical model is built that allows to create a schedule for performing the cyberprotection measures, aimed at maximizing the profit of the organization in conditions of limited resources. It is shown that in the above statement, the task of planning the process for implementing cyberprotection measures may be transformed to the canonical form of combinatorial optimization problems with a linear structure belonging to the NP-class. For its solution, it is proposed to use an algorithm based on the improved method improved that implements the idea of directed search of variants. The directed search method uses sequential fragmentation of the full set of solutions to the problem, until either the optimal plan is found, or the fact of the incompatibility of the system of restrictions is established. The resulting new subsets of the variants are subjected to formal analysis aimed at minimization of the solution process duration. A further development of the described approach to planning cyberprotection activities can be transition to stochastic models in which all financial and time indicators that relate to the implementation of cyberprotection measures are random variables with predetermined distribution laws. The proposed method is optimization-focused, so its application can provide increased competitiveness, efficiency and financial performance of companies in the context of modern cyber threats.

Keywords: cybersecurity, project, restriction, directed search method.

1 Relevance, purpose and research method

1.1 Relevance

Security of information systems and the information that is stored and processed in them from cyber threats requires application of a number of various measures and activities. Among these measures and activities there are the acquisition and deployment of hardware, the acquisition and deployment of operating systems, system and application software, including specialized software (firewalls, anti-rootkits, etc.); installing updates to operating systems and other software, acquiring and updating software licenses, updating anti-virus software databases, backing up information, measures for the physical protection of information infrastructure, measures for examining cables and equipment, conducting internal and/or external audits, testing for penetration, organizational measures, development and implementation of security policies, staff training, etc. For each of these measures, the optimal deadlines and the requirements for the frequency of use can be determined. Also, each of the measures is associated with certain costs and expences in terms of financial, material and labor resources. On the other hand, each of these measures and activities gives some return in terms of achieving and maintaining the necessary level of information security.

The current article is devoted to the description of the mathematical model of the task of planning activities to ensure cybersecurity and proposes a method for its solution, which determines the relevance of the research topic.

1.2 Purpose

The purpose of the study is to create a mathematical method for the formation of a schedule plan of cyber threats protection measures in the organization's information system, which is optimal according to the economic criterion, taking into account investments and returns on the implementation of planned measures.

1.3 Method

The research method is based on construction of a mathematical model, which is a formal reflection of the statement of the problem of work planning. The structure of this model includes a criterion function, the values of which characterize the expected return from implementation of the planned measures, and a system of restrictions that reflects the requirement that at each time interval the difference between the organization's income and expenses for the implementation of information protection measures should not be less than a specified level. It is proven that in the considered mathematical formulation the task of planning cybersecurity maintaining activities is reduced to the canonical form of combinatorial optimization problems. It is proposed to use for its solution the method of directed search of variants, adapted to the structure of the developed mathematical model.

2 Publications

Books [1-3] provide a systematic presentation of the current state of general project management methods. Since the end of the twentieth century, in the world of commercial practice, there has been a transition from managing the execution of individual jobs to project management. This approach allows to concentrate the existing potential in order to accelerate the achievement of the set goals, as well as to strengthen control over the expenditure of resources in the conditions of limited funding. In addition to this, structurization of the performed work makes it possible to engage specialists who have relevant and versatile knowledge and skills to create a creative team corresponding to the particular subject area.

The book [4] offers a unified methodology for organizing and managing all types of complex programs and projects in the field of high technologies.

The publication [5] investigates the relationship between efforts invested in project planning and project success. The authors consider the three aspects of planning (definition of requirements, development of technical specifications and processes and procedures for project management), and the three aspects of project success (points of view and interests of the end user, project manager and customer office).

The article [6] considers the features of project management in the activities of a security specialist, with the following objectives: to achieve competitiveness and success of the company, motivate employees, and successfully serve both internal and external clients. At the same time, the requirements of contracts and scheduling are taken into account; methods for managing the core competencies and core values of the organization are considered.

The articles [7-8] consider the decision making tasks regarding the company's investment in a subset of the security management tools chosen out of the many available ones as a resources distribution problem, taking into account conflicting goals and limitations of the task, in particular, the limited budget allocated for cyber defense. The authors have proposed several formulations of the problem of choosing a subset of security controls as the “portfolio optimization” problem known in financial management. Also, they propose approaches to solving this problem using existing methods of single-criterion and multi-criteria optimization.

The method proposed in this paper is based on a modification of the mathematical method, the development of which was begun in the book [9].

3 Statement of the problem

The concept of managing cyber protection measures as projects and their elements allows us to represent the organization's cyberprotection activities as a controlled process that is implemented in a cybernetic system.

In any cybernetic system, the function of planning the development of a controlled process is performed via solving the so-called tasks of making managerial decisions, which, as a rule, are of a multivariate and, therefore, optimization nature. Therefore, when planning cyber protection actions, it is necessary to use special mathematical methods and computer technologies.

One of such methods consists in constructing a mathematical model of a managerial problem with the subsequent application of one or another optimization method to its solution [10].

In this regard, the task of planning activities to support the security of a computer system can be considered as the task of making managerial decisions inherent to organizational-type cybernetic systems. In this case, the task acquires a multivariate and, therefore, optimization character.

To solve the optimization problem, it is necessary to use numerical indicators of the cost and effectiveness of certain actions. The cost indicators for the problem under consideration are quite simple to formulate, for this it is enough to take into account the costs of material resources and human labor (which, as applied to the business environment, can also be easily estimated in monetary terms). When developing the method, it is necessary to take into account the fact that there is a cybersecurity funding item in the organization’s budget, and the amount of that funding can be changed by the management who takes into account the current economic performance of the company [11].

As indicators of the effectiveness of the measures under consideration, the estimated return (profit) from the implementation of specific protective measures, expected by the end of the planned planning period of time, can be used. Such estimated return can be calculated on the basis of an assessment of the probability of realization of a particular threat and the probable cost of the losses that its realization will entail. Generally speaking, this indicator is a fuzzy type value, and the value of its median can be taken as a first approximation.

The proposed concept, based on the presentation of the process of protecting information and information systems as the execution of a given set of activities, allows us to formulate the planning task in the following way.

By the beginning of the planning period, the administrative body making decisions in the field of cybersecurity has at its disposal a “portfolio” of cybersecurity control measures. Each of these measures, from the point of view of the administration, is characterized by the three groups of parameters: the acceptable range of implementation time, the amount of necessary financial investments at the stages of the specific measure implementation, the values of expected financial returns at each stage of the implementation of the measure. The “return” is understood as the part of the company's profit that appears due to the cyber security of the computer system [10-12]. This value is equal to the possible financial loss from unauthorized access to information resources, together with the costs of eliminating its consequences, taken with the opposite sign.

The governing body should choose and distribute in time the measures that are accepted for implementation in such a way that to achieve the best overall financial result of this activity, taking into account the initial and current available financial resources, which dynamically change over time. It is assumed that funding of measures chosen for implementation before the beginning of the current planning period continues until they are completed in the due time.

3.1 Input data

Formalization of the problem requires breaking down each period of time during which the cyber security measures can be applied, into equal half-open intervals, which play the role of conditional units of time. The time intervals and all cyberprotection measures are numbered with natural numbers.

Let k be the number of the interval, $k = \overline{1, n}$; i is the measure number, $i = \overline{1, m}$; m – the number of measures that are under consideration with the governing body at the time of making the decision. The length of this planned time period T is chosen in such a way that its upper limit is equal to $\max\left\{t_i^{\max} + \tau_i;\, i = \overline{1, m}\right\}$, where $t_i^{\max}$ is the latest permissible start date for the implementation of the i-th measure; τ_i is the duration of its performance in calendar units.

Let n_i be the number of half-open time intervals during which the i-th project can be completed; $i = \overline{1, m}$. This parameter is calculated as the result of rounding the value of the expression $\left(\frac{\tau_i}{T} \times n\right)$ to the nearest larger integer.

The input data necessary to solve the problem of optimal planning of cyberprotection activities is formally defined in the form of quantities and sets that satisfy the requirement of the minimum amount of information that is entered into the computer system (it is assumed that all financial indicators are measured in the same units):

N_i is a set of numbers of time intervals in which the implementation of the i-th project can be started; $N_i \subseteq \{1, \ldots, n - n_i + 1\}$; $i = \overline{1, m}$;

M_i^c, M_i^s are sets of sequence numbers of time intervals in which funding is required and return is expected for the i-th project, provided that its implementation begins in the first interval; $M_i^c \subseteq \{1, \ldots, n_i\}$; $M_i^s \subseteq \{1, \ldots, n_i\}$; $i = \overline{1, m}$;

c_{ik} is the volume of financial investments, planned for the i-th project in the k-th time interval of the period of its implementation; $i = \overline{1, m}$; $k \in M_i^c$;

s_{ik} is the amount of return from the i- th project on the k th account of the time interval of the period of its implementation; $i = \overline{1, m}$; $k \in M_i^c$;

c_k is the total amount of financial investments made in the cyberprotection actions accepted for implementation prior to the beginning of considered planning period, at the k-th time interval; $k \in M^c$;

s_k is the total amount of financial return from the implementation of the measures accepted for implementation prior to the beginning of this planning period, during the k-th time interval; $k \in M^s$;

a_k is the minimum allowable difference between the incomes that accumulate over time, and the costs of performing the measures in the k-th interval; $k = \overline{1, n}$;

D is the value that characterizes the available financial resource of the research management system at the initial moment of the given period of planning time.

Taking into account the presence of initial capital $(D > 0)$, the constants a_k, $1 \le k \le n$, that are related to the initial values of the parameter k, may be negative, but the absolute value of the sum of such constants should not exceed the value of D.

The positive values of the constants a_k, $1 \le k \le n$, characterize the volume of the part of the accumulated profit, which is withdrawn from turnover in the k-th time interval and is spent for covering current expenses not directly related to the financing of cyberprotection.

To build a mathematical model of the problem of optimal planning of cyberprotection activities, based on the given input data, the sets that describe the linking of measures to the considered time periods are sequentially formed according to the procedure described in [9].

3.2 Mathematical model

A cybersecurity maintenance activity plan for a given period of time is determined by a vector of bivalent independent variable values $x = \left(x_{ik} \,\middle|\, i = \overline{1, m};\, k \in N_i \right)$. Its components define the truthiness ($x_{ik} = 1$) or falseness ($x_{ik} = 0$) of the following statement: "The i-th project is accepted for implementation starting from the k-th time interval".

For an information system functioning in an environment containing cyberthreats, the results of cybersecurity maintenance measures have a cost estimate of financial return based on an estimate of the cost of possible losses that could have occurred if cyberthreats were implemented in an unprotected system, and that the company avoided as a result of applying the measures of cybersecurity maintenance. Therefore, the criterion for the effectiveness of activities to ensure cybersecurity should be the estimated return from the implementation of these activities obtained during a given planned period of time:

$$f(x) = \sum_{i=1}^{m} b_i \sum_{k \in N_i} x_{ik} \,, \tag{1}$$

where b_i is the difference between the return and costs associated with the implementation of the cyber security measures. The use of cybersecurity maintenance measures makes sense if the return on them (or the loss prevented by them) exceeds the cost of their implementation.

The system of restrictions for this problem is formed by two groups of inequalities. The first group of constraints them consists of expressions of a combinatorial nature, which reflect a restriction on the multiplicity of application of certain measures in given periods. There are two approaches to their formulation. These approaches differ in the way they describe the repeated jobs like doing information backups.

One approach is based on consideration of each instance of such a job as another project. Thus, the constraints of the first group will be formulated as

$$\sum_{k \in N_i} x_{ik} \le 1; \quad i = \overline{1, m} \,. \tag{2}$$

Another approach allows existence of projects that are repeated more than once. In such a case, the formula (2) is substituted with

$$\sum_{k \in N_i} x_{ik} \le \eta_i \, ; \quad i = \overline{1, m} \, , \tag{3}$$

where η is the vector of the corresponding constants specifying these constraints.

Each of the two approaches has its advantages and disadvantages. The second approach allows to automate the task of input data description for repeated jobs; on the other hands, the constraints (3) should be supplemented with additional constraints that prohibit the overlapping of different instances of the same type of a project in time. The first approach guarantees the absence of overlapping without additional conditions, but requires more manual work concerning the description of input data, and also may lead to sufficient growth of dimensionality of the problem.

The restrictions of the second group express the requirement that, at each time interval, the cumulative difference between returns and expenses should not be less than a given level:

$$S(x,k) - C(x,k) \ge A(k) - D \, , \quad k = \overline{1, n} \, , \tag{4}$$

where $S(x,k)$, $C(x,k)$, $A(k)$ are the functions that characterize respectively the total return, expenses, and part of the profit that must be withdrawn from circulation during the period from the first to the k-th interval inclusively.

In the given formal statement, the problem is reduced to the problem of finding a vector of values of bivalent variables $x_{ik} \in \{0, 1\}$; $i = \overline{1, m}$; $k \in N_i$, which provides the maximum of the objective function (1) to, being subject to the system of constraints (2)–(4) or (3)–(4).

The presented model (1)–(4) is a basic one and can be modified in accordance with additional features of the formulation of this problem. For example, the real situation in the development of a business may require ensuring maximum profit not until the end of a given planning period of time, but up to a certain k^*-th interval $(1 \le k^* \le n)$. In this case, the problem is reduced to finding the vector of values of bivalent variables $x_{ik} \in \{0, 1\}$; $i = \overline{1, m}$; $k \in N_i$, which maximizes the objective function

$$f(x, k^*) = S(x, k^*) - C(x, k^*) \, , \tag{5}$$

along with satisfying the same system of constraints (2)–(3).

If necessary, the initial system of restrictions (2)–(4) can be supplemented with an expression that sets the lower limit $P(n)$ of the difference between returns and expenses of the management system at the end of the current planning time period:

$$\sum_{i=1}^{m} b_i \sum_{k \in N_i} x_{ik} \ge A(n) + P(n) \, . \tag{6}$$

Another specific feature of the statement of the problem of optimal planning of cybersecurity maintenance activities is that the volumes of the costs of implementing cyberprotection measures and the amounts of returns generated from them can parametrically depend on the moment when their implementation has started. In such a case, the objective function (1), the values of which characterize the economic efficiency of cybersecurity maintenance activities for the entire given planning period of time, will have the following form:

$$f(x)=\sum_{i=1}^{m}\sum_{k\in N_i} b_i(k)\,x_{ik} \quad , \tag{7}$$

where $b_i(k)$ is the difference between the revenues and expenses associated with the i-th measure for cybersecurity maintenance, the implementation of which begins at the k-th time interval:

$$b_i(k)=\sum_{k'\in M_i^s(k)} s_{ik'}(k)-\sum_{k'\in M_i^c(k)} c_{ik'}(k)\,; \quad i=\overline{1,m}; \quad k\in N_i\,.$$

The constraints (2)–(3), as well as the general structure of constraints (4), will remain unchanged, but the functions $S(x,k)$ and $C(x,k)$, which are components of the inequalities system (4) and of the objective function (5), will take another form.

The constraint (6), taking into account the parametric dependence of the financial indicators (returns and investments) of the cybersecurity maintenance activities from the time of the start of their execution will get in the form:

$$\sum_{i=1}^{m}\sum_{k\in N_i} b_i(k)\,x_{ik}\geq A(n)+P(n)\,. \tag{8}$$

The considered variants of the optimal planning of cybersecurity maintenance activities, which are represented by mathematical models (1)–(4), (4)–(6), {(4), (6), (7)} and {(4), (5), (8)}, belong to the NP class of extremal combinatorial problems with a linear structure. After transforming these models to the canonical form, the method of directional search of variants [9] adapted to the structure of the given mathematical expressions may be used to solve the problem.

4 Problem solution

In the canonical form, an extreme combinatorial problem with a linear structure is formulated as the problem of maximization of the criterial function

$$f(z)=\sum_{j\in J_0} c_j z_j \tag{9}$$

subject to restrictions

$$\sum_{j\in J_j} a_{ij} z_j \leq b_i; \quad i=\overline{1,m}\,, \tag{10}$$

where z is the vector of the desired variables: $z=(z_j \mid j=\overline{1,n})$; $z_j\in\{0,1\}$; $j=\overline{1,n}$; J_0 and J_j are the sets of numbers of independent variables included in the criterion function and the i-th constraint of the problem, respectively; a_{ij}, b_i, c_j are real numbers.

For conversion of the mathematical models (1)–(4), (4)–(6), {(4), (6), (7)} and {(4), (5), (8)} to the canonical form (9)–(10) it is necessary to perform the following actions:

a) associate with each variable x_{ik}, $i = \overline{1, m}$, $k \in N_i$ the variable z_j, $j = \overline{1, n}$, where z is the vector of the searched variables;

b) replace the designation of constants in expressions (1)–(7) with the symbols utilized in the canonical form (9)–(10);

c) replace the expressions (4), (6) and (8) with inequalities opposite in sign.

The directed search method uses sequential fragmentation of the full set G of solutions to the problem, until either the optimal plan is found, or the fact of the incompatibility of the system of restrictions is established. The resulting new subsets of the variants are subjected to formal analysis in order to reduce the amount of processed information, to reduce the number of algorithm steps leading to the desired result, and, therefore, to minimize the duration of the solution process.

Let us suppose that at the beginning of a certain stage of solving the problem (9)–(10), λ of disjoint subsets G_k, $k = \overline{1, \lambda}$, containing feasible plans, have been identified in the full set of options G. The model (9)–(10), aligned with the k-th subset of options, takes the following form:

$$f_k(z) = \sum_{j \in J_{0k}^1} c_j + \sum_{j \in J_{0k}} c_j z_j \to \max\,; \tag{11}$$

$$\sum_{j \in J_{ik}} a_{ij} z_j \le b_{ik}\ ;\ i \in I_k\ ; \tag{12}$$

$$z = (z_j \mid j \in J_k)\ ;\ z_j \in \{0, 1\};\ j \in J_k\ ,$$

where $b_{ik} = b_i - \sum_{j \in J_{ik}^1} a_{ij}$; $i \in I_k$; I_k is the set of numbers of constraints from (10) that are active with respect to plans for the subset of variants G_k.

The properties of the k-th ($k = \overline{1, \lambda}$) subset of the variants of solutions to the problem (8) - (9) are formulated in the following statements.

Statement 1. The subset G_k does not contain admissible plans, if, for some constraint $i \in I_k$ the condition $\sigma_{ik}^{(2)} > b_{ik}$ is satisfied.

Statement 2. The constraint $i \in I_k$ is not active with respect to the plans of the subset G_k, if for it the condition $\sigma_{ik}^{(3)} \le b_{ik}$ is satisfied.

Statement 3. If $J_{ik}^2 \ne \varnothing$ and for some $j' \in J_{jk}^2$ the condition $\sigma_{ik}^{(2)} \le b_{ik} < \sigma_{ik}^{(2)} - a_{ij'}$ holds, then of the complementary plans of the subset G_k only those ones can be admissible in which $[\forall j \in J_{ik}^2(j')](z_j = 1)$.

Statement 4. If $J_{ik}^{3} \neq \varnothing$ and for some $j'' \in J_{ik}^{3}$ the condition $\sigma_{ik}^{(2)} \leq b_{ik} < \sigma_{ik}^{(2)} + a_{ij''}$ holds, then of the complementary plans of the subset G_k only those ones can be admissible in which $[\forall j \in J_{ik}^{3}(j'')](z_j = 0)$.

Here $\sigma_{ik}^{(2)}$ is the sum of the negative coefficients of the i -th constraint of the combinatorial optimization problem; $\sigma_{ik}^{(3)}$ is the sum of the positive coefficients of the i -th constraint of the combinatorial optimization problem.

J_{ik}^{2} and J_{ik}^{3} are the sets of numbers of independent variables that are present in the i -th constraint of the system (12) with negative and positive coefficients, respectively:

$$J_{ik}^{2} = \left\{ j \in J_{ik} : a_{ij} < 0 \right\};\ J_{ik}^{3} = \left\{ j \in J_{ik} : a_{ij} > 0 \right\};$$

$J_{ik}^{2}(j')$ are the sets of numbers of independent variables that are present in the i -th constraint of the system (12) with negative coefficients not exceeding the value $a_{ij'}$:

$$J_{ik}^{2}(j') = \{ j' \} \bigcup \left\{ j \in J_{ik}^{2} : a_{ij} \leq a_{ij'} \right\};$$

$J_{ik}^{3}(j'')$ are the sets of numbers of independent variables that are present in the i -th constraint of the system (12) with positive coefficients not less than $a_{ij''}$:

$$J_{ik}^{3}(j'') = \{ j'' \} \bigcup \left\{ j \in J_{ik}^{3} : a_{ij} \geq a_{ij''} \right\}.$$

The algorithm of directed search of variants provides for the performance of the following sequence of actions at each stage of solving the problem (9)–(10):

1) Selection of a subset of variants for further partitioning.

For further partitioning, a subset is selected that corresponds to the maximum estimate of the criterion function:

$$\xi(G_{k^*}) = \max\{ \xi(G_k); k = \overline{1,\lambda} \} ,$$

where

$$\xi(G_k) = \sum_{j \in J_{0k}^{1}} c_j + \sum_{j \in J_{ok}^{3}} c_j \ .$$

2) Selection of a variable the values of which are to be fixed.

The variable, which is included in the criterion function with the maximum coefficient, should be selected for this purpose.

3) Partitioning a subset of options into two disjoint subsets.

By fixing the values of the selected variable z_{j^*}, the subset is split into two disjoint subsets: $G^0_{k^*}$ and $G^1_{k^*}$. The plans in the first of the sets have $z_{j^*}=0$; the plans in the second set have $z_{j^*}=1$.

4) Analysis of the subsets of variants $G^0_{k^*}$ and $G^1_{k^*}$.

The procedure of analysis of any k -th subset of the options for solving the combinatorial optimization problem consists in sequential checking the fulfillment of the conditions of each of the formulated statements for all the constrictions of the system (11)–(12). Depending on the results of this check, one or another sequence of actions is carried out in the analysis cycle.

After completing the analysis of the subsets, the subsets of options remaining in the field of consideration are again renumbered by numbers of the natural series from 1 to λ'.

The search process ends in two cases:

– if the fact of incompatibility of the system of restrictions (9) is detected, as evidenced with equality $\lambda'=0$;

– if a vector of values of the searched variables is found that gives the criterion function (8) a value that is not the least among the possible ones:

$$f(z^*) \geq \max\{\xi(G_k), \quad k=\overline{1,\lambda'}\}.$$

It is advisable to start the solution with an analysis of the full set of options G. In certain cases, this allows us to establish a priori the fact of incompatibility of the system of restrictions (10) or to cut off a subset of options that does not contain acceptable plans.

5 Conclusions

The modern concept of cybersecurity management involves its consideration as a process of performing a set of cyberprotection activities organized into projects. This approach makes it possible to use the mathematical apparatus for making managerial decisions developed in the theory of cybernetic systems and project management.

Based on this concept, a mathematical model is built that allows you to create a calendar plan for cyberprotection measures aimed at maximizing the profit of a company in conditions of limited resources.

It is shown that in the above statement, the task of planning the process for implementing cyberprotection measures may be transformed into the canonical form of combinatorial optimization problems with a linear structure related to the NP-class. For its solution, it is proposed to use an algorithm based on the improved method that implements the idea of directional search of variants.

Despite the completeness of the proposed algorithm, the solutions that are developed on the basis of the above models are approximate in nature due to the artificial transition from continuous to discrete time. However, one has to put up with this, since a constructive formalization of a given problem in continuous time, which could make it possible to find its exact optimal solution taking into account all the real limitations, is not possible.

A further development of the described approach to cyberprotection activities planning can be the transition to stochastic models in which all financial and time indicators that relate to the implementation of cyberprotection measures are presented with random variables with predetermined distribution laws.

The optimization focus of the proposed method can provide increased competitiveness, efficiency and financial performance of companies in the context of contemporary cyber threats.

References

1. Kerzner, Harold. Project Management: A Systems Approach to Planning, Scheduling, and Controlling. 12th edn. Wiley, New-York, 2017, 848 p.
2. Lapygin Yu. Project management: from planning to efficiency estimation, Omega-L, Moscow, 2008, 252 p.
3. Bogdanov V., Project management: corporate system – step by step, Mann, Ivanov and Ferber, Moscow, 2012, 248 p.
4. Archibald, R.D.: Managing High-Technology Programs and Projects. Wiley, New-York, 2008, 396 p.
5. Dvira, D., Razb, T., Shenharc, A. J.: An empirical analysis of the relationship between project planning and project success. Int. J. of Project Management, 21 (2), 2003, p. 89-95.
6. Timmons, F.R.: Project Management for the Security Professional. In: Security Supervision and Management, 4th ed., Butterworth-Heinemann, 2015, pp. 301-308.
7. Yevseyeva, I., Basto-Fernandes, V., Emmerich, M., van Moorsela, A.: Selecting Optimal Subset of Security Controls. In: Cruz-Cunha M., Varajao J., et al. (eds.) The CENTERIS/ProjMAN/HCist Conference 2015, October 7-9, vol. 64, pp. 1035-1042 (2015). DOI: 10.1016/j.procs.2015.08.625.
8. Fielder, A., Panaousis, E., Malacaria, P., Hankin, C., Smeraldi, F.: Decision support approaches for cyber security investment. Decision Support Systems, vol. 86, pp.13-23 (June 2016). DOI: 10.1016/j.dss.2016.02.012.
9. Litvinenko A. Method for directed search in control and diagnostic systems, Scientific publishing center NBUV, Kyiv, 2007, 328 p.
10. Gnatyuk S., Polishchuk Yu., Sydorenko V., Sotnichenko Yu. Determining the level of importance for critical information infrastructure objects, Proceedings of 2019 IEEE International Scientific-Practical Conference: Problems of Infocommunications Science and Technology, PIC S and T 2019, Kyiv, Ukraine, October 8-11, 2019, pp. 829-834.
11. Oksiiuk O., Chaikovska V., Fesenko A. Security technique for authentication process in the cloud environment, Proceedings of 2019 IEEE International Scientific-Practical Conference: Problems of Infocommunications Science and Technology, PIC S and T 2019, pp. 379-382, 2019.
12. Zahran B., Al-Azzeh J., Gizun A., Griga V., Bystrova B. Developing an expert system for assessment of information-psychological influence, Indonesian Journal of Electrical Engineering and Computer Science, 15(3), pp. 1571-1577, 2019.