Modeling of the Integrated Quality Assessment System of the Information Security Management System

Tatiana Babenko, Hryhorii Hnatiienko, Vira Vialkova

Taras Shevchenko National University of Kyiv, 24 Bogdana Gavrylishina Str,04116, Kyiv, Ukraine

Abstract

The paper presents approaches to determining the necessary and sufficient level of implementation of security measures presented in the "best practices" at a certain level acceptable for the organization that meets the real existing threats. The model presented in the work allows an automated integrated assessment of the impact of controls presented in the "best practices" on the functional resistance of the protection system. The model presented in the work can be adapted to the needs of a particular organization, as well as in other subject areas. The article proposes a mathematical model of the problem of implementing a control system. The concept of criticality of controls, as well as various aspects of functional stability and its relationship with reliability, survivability, fault tolerance are considered. Significant attention is paid to taking into account the subjective component in the tasks of determining the quality of implementation of controls and evaluation of the integrated indicator of information system security. Attention is paid to the consideration of granularity in the construction of the function belonging to a fuzzy set. The problem of assessing the integrated quality of the implementation of controls and solving the optimization problem of improving the quality level is considered information system security.

Keywords [1]

Vulnerabilities, threats, security measures, information security, information technologies, information security management systems, information security risks, risk assessment, ISMS integrated quality assessment models.

1. Introduction

Due to the advancement of technology, a violation of today's information ensitive data, sustain fundamental operations, and protect national infrastructure can influence hundreds of thousands, if not millions of individual consumers and even more personal data, all from a single attack on a company.As it is known [1-3], the creation of a completely reliable system of the protection of information, which is processed using information and communication systems (ICS), is fundamentally impossible. In these circumstances, the measures and methods of information protection are used to reduce the likelihood of negative consequences of violation of the basic properties of information or damage from them, but not to avoid them completely. In this context, it makes sense to consider the process of information security at some acceptable level for the organization, which corresponds to the real threats. Under threat (risk) in this context we understand a potentially possible event in the field of information security, which may lead to losses. Currently, there are different approaches to ensure the security of information processed in the ICS of the enterprise, but special attention of experts in this field is focused on ensuring the adaptive security of ICS, which includes the use of one of two technologies: security assessment and intrusion detection.

IT&I-2020 Information Technology and Interactions, December 02–03, 2020, KNU Taras Shevchenko, Kyiv, Ukraine

EMAIL: babenkot@ua.fm (T. Babenko); g.gna5@ukr.net (H. Hnatiienko); veravialkova@mail.com (V. Vialkova)
ORCID: 0000-0003-1184-9483 (T. Babenko); 0000-0002-0465-5018 (H. Hnatiienko); 0000-0001-9109-0280 (V. Vialkova)

At the same time, implementing the "best practice" CMMI, NIST, COBIT, ISO2700, etc., in the process of building and managing information systems (IS), which allows to implement some accepted level of security information.

ISO/IEC 27001:2005, CobiT and ITIL are the three most important best-practice IT-related frameworks. ISO/IEC 27001 is the international Code of Best Practice for Information Security from the International Standards Organization in Geneva. CobiT is Control Objectives for Information and Related Technology, from the IT Governance Institute, in the United States and ITIL is the IT Infrastructure Library, created by the United Kingdom's Office of Government Commerce. ISO 17799, COBIT, and ITIL are all best-practice IT approaches to regulatory and corporate governance compliance. Typically, "best practices" include requirements for assessing and developing information security risks that are connected with the needs of the organization [1]. Implement the"best practice" CMMI, NIST, COBIT, ISO2700, etc provide a well-managed and flexible IT environment in an organization.

Also, the requirements, which are stated in one or another "best practice", are common and can be implemented for all organizations, regardless of their type, size and nature. At that time, the requirements for correspondence to the information security management system (ISMS) of one or another "best practice" do not allow the removal of any of the requirements introduced in it [1].

2. Critical controls

Some of the controls are critical for providing an acceptable level of system’s service, for other parts a reduced level of implementation of controls is acceptable, and for some situations the absence some controls without significant danger to the level of functional stability of ISMS is even possible.

The process of risk management, including IS risks, should be continuous. It is also important to determine the external and internal circumstances of risk assessment and treatment in accordance with the risk treatment plan and the implementation of recommendations and decisions [4]. A qualitative or quantitative approach can be used to analyse the identified IS risks. At the same time, a quantitative approach may be more attractive in some practical situations, which theoretically allows to compare the security of different information processing systems, but its implementation in practice is complicated by the following factors:

- lack of reliable statistics;
- the difficulty of assessing losses in the case of intangible assets;
- the difficulty of assessing indirect losses from the implementation of threats;
- impairment of long-term quantitative risk assessment results due to IS modification and reconfiguration.

Due to the limitations described above, a qualitative approach based on the ranking of threats and related IS risks according to the degree of their danger is usually used for the analysis of IS risks. The results of the risk assessment, to some extent, make it possible to prioritize risks according to their importance or other criteria. For example, according to [5], risk assessment consists of the following actions: risk identification, risk analysis, risk comparison.

Risk assessment allows to determine the value of ISMS information resources and allows to identify possible threats and vulnerabilities and, accordingly, to identify potential consequences. It should be added that solving the problems of risk assessment or cost estimation of IS threats is complicated by the fact that modern information and communication systems are usually geographically distributed and require synchronization in event management, including IS.

ISO 31000 defines a high-level approach to risk management [6, 7]. In the field of information security management first, the circumstances are determined, a risk assessment is performed. Typically, this procedure is performed in two or more stages. The first stage is usually performed to identify potentially high risks that require further assessment, then, in case of incomplete information, other methods may be used. If the risk assessment provides sufficient information to effectively determine the actions to be taken to modify the risks to an acceptable level, there is a transition to IS risk processing, which should result in an acceptable level of residual risks for a particular enterprise. At the same time, risk-taking actions should guarantee the fact that residual risks are actually accepted by the organization. As noted in [5], this fact is especially important in situations where the implementation of any of the security measures was abandoned or postponed, including the situation, when it was made due to cost. There are several options for processing the identified risks, including: recognizing the acceptability of the risk of a particular threat, partial transfer of responsibility for IT security incidents to other organizations, a set of measures to reduce or avoid the risk. As part of solving the problem of IS risk management, all security measures that need to be implemented for the selected risk management options should be identified. In this case, the organization should compare the security measures with those, listed in the relevant "best practice", to determine the fact, that there was no withdrawal of the necessary measures to ensure IS.

Based on the above, the process of identification of IS risk assessment and processing is quite subjective and significantly depends on a significant number of factors, including the chosen risk assessment methodology, completeness of available data on IS status and level, level of training of ISMS implementation and support specialists, performing internal or external IS audit. Existing tools for assessing the level of implementation of a "best practice" and, accordingly, IS measures in the implementation of risk-based model are based on assessing the level of maturity of relevant programs, in particular IS programs. Typically, assessment tools use the maturity assessment system ISO 21827: 2008, which ranges from 0 to 5, with 5 being the highest level of maturity [8]:

0. Not performed
1. Performed informally
2. Planned
3. Well defined
4. Quantitatively controlled
5. Continuous improvement

However, determining the level of maturity of the respective IS or IS program does not allow to draw adequate conclusions wether residual risks of IS are really acceptable and accepted by the organization and how in a limited budget allocated to provide IS to perform simulations of IS threats need to be implemented in order to reduce the likelihood of a particular IS threat or group of threats.

Risk-oriented approach to assessing the need for costs to ensure IS can be supplemented by methods of assessing the feasibility of costs, and in many cases quite difficult and even impossible to apply these methods, because the method, which is used, should: provide a quantitative estimate of costs based on qualitative indicators for assessing the probability of occurrence of IS events and their consequences; be universal; provide an opportunity to model the situation of application of countermeasures aimed at preventing threats that have different levels of impact on IS assets.

This is especially true when it comes to intangible assets or indirect costs. As the categories of costs related to the security of information processed in ICS include organizational costs for the formation and maintenance of the ISMS unit, costs for controlling the level of resource protection, internal and external costs for eliminating the consequences of information security policy violations, ISMS maintenance costs. The above list of costs for providing a highly effective information security system shows the high cost of computer security to create and maintain ISMS or other security systems. At the same time, the introduction of unnecessary security measures, with the exception of the economic component, leads to inconvenience and dissatisfaction of staff. Thus, it is necessary to find sufficient level of protection at which the ratio of the cost of security measures and the amount of possible damage had an acceptable level for the organization.

This study attempts to develop a model that would allow, based on a general list of security measures listed in the "best practices", to determine the necessary and sufficient measures to ensure an acceptable level of security of information processed in the ICS of the enterprise.

3. Functional stability

One of the essential indicators of the level of safe operation of the system is the functional stability [9-11]. Functional stability is the ability of a system to perform its functions during a given time interval under the influence of the flow of operational failures, intentional damage, interference in the exchange and processing of information, as well as in case of errors of service personnel [12, 13]. The main properties of poorly structured complex systems that characterize their functional stability are reliability, survivability, fault tolerance.

With some caveats, functional stability to some extent combines all of these characteristics. The problem considered in this paper can best be described by applying the concept of functional stability, the implementation of which is achieved through the use of different types of redundancy, by reallocating resources to compensate for the consequences of emergency situations [9].

In this paper we will pay attention to the study of the situation of sustainable operation and reliable information protection of a complex poorly structured organizational system. To quickly assess the quality of functioning of such systems, it is necessary to build a model for determining the integrated indicator of the quality of functioning of the information protection system.

This integrated quality indicator must reasonably and adequately reflect changes in the structure of the system and quality indicators of the functioning of its elements. At the same time, it is promising to use the methodology of introspective analysis of subjective components of the system and expert decision-making technologies to solve the described problem [14]. The purpose of the study can be considered achieved when an integrated indicator is defined, which adequately characterizes the state of functional stability of the system and sensitively responds to changes in the composition of the system and the structure of the relationships of its elements. To achieve this goal, it is necessary to develop a mathematical model to ensure a sufficient level of functional stability of a complex poorly structured system based on information about the presence of damage to its elements and subsystems.

It is also necessary to provide options for duplication of functions, operational interchangeability of subsystems, to solve the problem of integrated assessment of the quality of the system and the choice of its optimal configuration to increase functional stability.

This will be facilitated by models for determining the state of execution of functions by elements and subsystems, the choice of options for interaction between elements and subsystems in order to maximize the integrated quality of execution of functions by the whole system. In addition, it is necessary to build a model that will reflect the reaction of the system to different types of environmental influences and changes in the state of the elements of the system.

4. Accounting subjective component

Determining the quality of the implementation of controls significantly depends on the objectivity of the experts involved, as well as on the procedures of analysis of expert data used in the evaluation process. Therefore, the problem of developing methodological and mathematical support for personnel management tasks based on the subjective component to improve the quality of decision-making problems in decision-making in complex poorly structured systems should be given much attention. The development of theoretical and technological bases of expert decision support, which would allow the most effective operation of expert information and decision-making considering the subjective component, the need for prompt and adequate response to modern challenges determine the relevance of this work. The methodology of considering the subjective component is used at all stages of the control evaluation procedure and ensures the receipt of reliable information from all participants in the PR. At the stage of obtaining expert information, decision-makers should be able to set their preferences in a form convenient for them in ordinary or cardinal scales in terms of the subject area. Modern complex systems are characterized by rapid change and the need for rapid response to subjective factors in a variety of manifestations. The world around us is becoming more complex, the pace of change is accelerating, the amount of information is increasing and the uncertainty of the relationships between the elements of the systems is increasing.

It can be argued with some conventionality that the problems of humanity are largely based on incorrectly defined and poorly placed priorities, as well as the inability or unwillingness to adequately carry out the procedure of relative evaluation.

In the tasks of implementing information security systems, the weak structure of subject areas, the complexity and fundamental informality of the relationships between the factors influencing the decision, necessitate the involvement of the subjective component at all stages of implementation and application of controls. In many poorly structured subject areas, the use of expert technologies is often an unalterable way to obtain and justify the choice of acceptable solutions [15, 16].

Improving the quality of management of complex systems and ensuring reliable controls requires high-quality involvement of subjective factors in the management loop. To solve modern problems in poorly structured subject areas, it is necessary to effectively involve specialists in subject areas, mathematical modelling and decision-making. Since such a symbiosis is not always possible, there is a need to develop mathematical methods that would adequately model the practical problems of information security.

An important attribute of the process of functioning of complex systems is the presence of internal contradictions caused by lack of knowledge about their functioning. Identification of such knowledge is carried out by turning the intuitive conclusions of experts into formalized. Formalization of decision-making processes largely determines the prospects for the development of automated information systems, increasing the level of their intellectualization and efficiency.

At the same time, it is known that people have natural limitations of their psychophysical capabilities. Therefore, experts are not always able to adequately record their advantages - a direct assessment of various aspects of the practical decision-making situation is rather an exception [17, 18]. The main advantages of the methodology developed by the authors and, in particular, indirect methods of determining the "weight" of objects, over other expert methods are the ability to determine the preferences of experts on features that people cannot assess or mistakenly believe them.

5. Formulation of the problem

Let an information security management system or other organizational system be built. For this object a control system has been defined and implemented in accordance with “best practice”. We will denote the set of control indices as $i \in I = \{1,...,n\}$. Each control is characterized by the level of implementation $a_i, i \in I$ and quality $b_i, i \in I$. Without reducing the generality, we will assume that $0 \le a_i \le 1, \forall i \in I$ and $0 \le b_i \le 1, \forall i \in I$ or measure the level of implementation of controls and their quality on a 100 percent scale.

Remark. Note that the voluntary, insufficiently justified assignment of interest in assessing the quality of control has a negative impact on the calculation of the results of solving the problem as a whole. Therefore, it is logical, without losing information, to consider several levels of quality control and perform calculations in the ordinal (rank) scale. And to clarify the definition of the quality of controls in the 100 percent scale, special procedures for digitization and arithmetic of the digitization scale should be developed and applied. The correlations between controls are also known. They are evaluated or expertly determined $v_{ij}, i, j \in I$. These correlations characterize control level $a_i, i \in I$ into control $a_j, j \in I$. Without reducing the generality, we will also assume that $0 \le v_{ij} \le 1, \forall i, j \in I$ or measure correlations as a percentage. The task is to model the characteristics of the information security management system, arithmetic (digitization) of quality control and determine an integrated assessment of the level of information security and, accordingly, to ensure the functional stability of the ISMS.

6. Mathematical model

We will model the set of controls and correlations between them with graphs or matrices of contiguity or incidence. The level of control implementation can be characterized by some discrete values: scores, verbal expressions, clustered indicators, etc. And the quality of control is functionally dependent on the level of its implementation and is expressed by some given or empirically defined function in analytical or tabular expression $b_i = f(a_i), i \in I$.

In this paper, we will consider the control system separately for each of the protection areas... It is logical to assume that each of the areas forms a relatively autonomous subset, within which the controls are more closely interconnected than the controls included in other subsets. At the same time, the subsets, formed by the directions of protection, are not isolated and this fact can be effectively illustrated by models of graph theory.

By analysing the controls, a polyhedral oriented graph can be constructed. The vertices of the graph are controls with multiple indices $i \in I$, each of which is characterized by the level of implementation $a_i, i \in I$, and quality of functioning $b_i, i \in I$.

The correlations between the controls are arcs $v_{ij}, i, j \in I$. If the arc is absent $\exists : v_{ij} = 0, i, j \in I$, the impact of control with the index $i, i \in I$ and control with index $j, j \in I$ are absent.

The level of influence between controls is expressed in the feedback: positive and negative. We will assume that at the initial stage of modelling and evaluation of ISMS it is determined that the level of implementation of controls in the system is $a_i^0, i \in I$, and the quality of functioning of each of them is defined or measured as $b_i^0, i \in I$.

The modelling of possible states of the system is that hypothetically or practically changes the initial levels of implementation of some controls and, according to the introduced heuristics, determines how these changes will affect the quality of interconnected controls and ISMS as a whole.

The level of influence between controls is expressed in feedback: this correlation can be positive or negative. It is clear, that the level of influence between controls and the direction of relationships between them are heuristics, which are determined in the initial stages of modelling by experts who have high competences in the field being modelled.

The positive feedback $v_{ij}^{+}, i, j \in I$ is that, when the vertex $i \in I$ of the graph is reached, even in the absence of control $a_i = 0, i \in I$, the system provides a certain level of quality at this vertex, i.e. $b_i > 0, i \in I$. When the level of control decreases, the level of negative feedback $v_{ij}^{-}, i, j \in I$, entails a decrease in the quality of control $a_i^t < a_i^{t-1}, i \in I$ not only of this vertex $b_i^t < b_i^{t-1}, i \in I$, but also of the associated vertices of the graph: $b_j^t < b_j^{t-1}, \forall j : v_{ij} > 0, i, j \in I$, where $t -$ is the rate of system quality assessment: $t = 0,1,2,...$.

In the same way the interaction between the sections of the graph is carried out and modeled through the bridges between the sections.

We will also assume that in the case of a discontinuity of the graph, the modeling of each connectivity component can be performed autonomously, by analogy with the approach described in this work.

7. Regulatory quality of the control system

While building a control system in full accordance with the standard [19], the quality of all controls is one hundred percent and their set is equal to the set of all possible control indices.

Thus, such a situation is ideal and the distance from it to the actual existing control system, which is audited, can serve as quality criteria of the built control system.

It is known that in many practical problems, measurements should be made indirectly, considering the relationship between objects, and not only evaluate the parameters or integral characteristics of objects. In addition, great care should be taken in the choice of measurement scales.

But these aspects of the study of the quality of controls and their interdependence will be considered in the next work.

8. Grain size of the universal set

To define the concept of safety, the whole set of states S is divided into subsets Sc - serviceable states, when there are no failures, Sr - operational states, when there are one or more failures that do not change (deteriorate) the system parameters due to redundancy) Sz - protective states and Sn - dangerous states. Based on this, safety is the property of the system to continuously maintain a serviceable, operational or protective condition for some time or operation [20].

All organizational complex systems seek to develop their staff, technology, information protection, but most practical situations do not lead to the strategic compliance of their intangible assets. The key to creating such a match is "graininess", or detailing, ie operating with non-general formulations.

For example, "develop our staff" or "preserve our core values", and focus on specific specific factors needed for critical internal strategic processes. The strategic map of a balanced scorecard allows managers to highlight the specific human, informational and organizational resources needed to implement the strategy. One approach to classifying tasks or functions performed by a system is the average execution time of a task or function. When assessing the functionality of the elements of the system, comparing the tasks performed by the elements, determining the relationship between them, the difference in the complexity or duration of the function is approximately an order of magnitude.

To adequately model the problem of analysis of the quality of implementation and operation of controls, we introduce the following heuristics. Heuristics. We will consider that at construction of model of system it was possible to distribute all functionality of its elements on such functions which are the constant units commensurate with each other. That is, the complexity, complexity and quality of all functions can be considered as values of the same order. It should be borne in mind that the functions performed by the system, implemented in the control system, of course, are different in priority, importance, weight, impact on other functions, labour effort to implement them, and so on.

An important feature that affects the complexity, complexity, accuracy, adequacy of the model is the choice of grain size. To build an integrated quality function, the ATS system determines discreteness or granularity: it is a heuristic that is accepted depending on the desired level of detail, which suits the decision maker, corresponds to the desired accuracy of the problem, the features of the formulas used and acceptable accuracy of calculations. decision making by rounding.

For example, when comparing the quality of implementation of each of the controls, it can be selected grains in the form of intervals of 1%, 3%, 5%, 10% and others. The choice of interval depends on the need to detail the task. It is important that the intervals are the same - for ease of calculation and sufficient intuitive validity. The membership functions of a fuzzy set of type 2 and above will be called blurred membership functions. The blurred membership function is interpreted as an area of insensitivity (inaccuracy, uncertainty) of the expert in determining the functions of belonging of objects x, $x \in X$, to the set A.. Formally, this uncertainty can be determined using "grain size", which reflects the degree of inaccuracy of the measured parameter in relation to the value of "grain". "Grain" is an indivisible (of course inaccurate) unit of measurement of this parameter. In our case, such a parameter is the membership function itself, which is determined on the interval [0,1], the smallest unit of which determines the limiting grain size of the scale. The size of the grain is determined or assigned on the basis of the "limits of distinction" of the grain for the expert.

Depending on the conditions of the problem of integrated evaluation of the quality control system, methods of determining values and other aspects, there are several ways to specify blurred information. But consideration of such methods is not the subject of this work.

9. Assessment of the integrated level of control

Responding to external influences and threats to the information security of the system requires immediate decision-making according to the situation. In addition, a person's ability to simultaneously analyse multiple indicators is limited. Therefore, the task of adequate determination of the integrated indicator of the quality of the system is relevant and its solution contributes to the rapid increase of the functional stability of the system. After making decisions about the redistribution of functions between system elements or their replacement, new values of resources for system tasks and quality levels of their operation are calculated. Based on the obtained values, the function of belonging of the quality levels of the system functioning to the fuzzy set (0,1) is determined. That is, the quality of the system as a result of the application of the described procedure will be characterized by the function of belonging to a fuzzy set. To assess the information security system, we will use the procedures of fuzzy expert assessment of system elements, which can also be used in the future to improve the model of assessing the level of information security of the system.

Today there is a group of indicators that are used to determine the general condition of systems. One of the common tasks of expert evaluation is the choice in a pre-fixed class of relations of some resulting (group, collective, compromise) relationship. At the same time, on the basis of several contradictory indicators, the aggregation (aggregation, generalization, etc.) of indicators into a single integrated indicator is carried out. To construct a convolution (generalized, aggregating, integral, integrative criterion of quality of object) means to supplement a partial order on set of objects. This can be done in many ways and necessarily includes an element of subjectivity.

At the first stage, high-level experts build a model of an ideal control system, that corresponds the standard [19] in the form of a graph with normative vertices and arcs, the model of which is described above. In the second stage, an expert or group of experts are auditing the real control system and are establishing or assessing the presence of controls, the level of their implementation in the system and fill in the column, that models the real ISMS. The coefficients of relative competence of experts [14] etc. can be considered.

On the basis of expertly determined or calculated by another method levels of controls $a_i, i \in I$ and considering the system, that meets the standard [19], the levels of control functioning quality, depending on this information: $b_i, i \in I$ are determined.

At the third stage, the quality levels of the ISMS are clustered in order to build an integrated membership function [21], which reflects the distribution of quality controls by quality levels and creates a membership function, based on the frequency of values [22]. The integral value of the level of implementation quality of the control system, which indicates the degree of functional stability of the system, can be calculated, for example, by the method described by authors. To determine the integrated assessment, we build a matrix of frequencies of different levels of quality of performance of each function $V = (v_{ij}), \; i = 1,...,100, \; j < n.$ Each row of this matrix displays the estimated level of function quality from 0% to 100%, and the column shows the number of functions with the specified level of performance. To determine the integrated level of quality of functioning of a complex system at the first stage, we classify the functions by the level of quality and completeness of their implementation.

Integral quality requires the use of heuristics. An integrated assessment of the quality of the information security system will be determined using an additive criterion. In this case, we use a number of heuristics that allow to justify the adequacy of the calculation of a single integral value of the criterion. Determining the integrated level of quality of functioning of a complex poorly structured system based on the analysis of interchangeability of its subsystems and determining the best options for improving the quality of functions requires the creation of an appropriate mathematical model. The quality of the information security system largely depends on the quality of the system elements.

10. Optimization of the system protection integrated quality.

To increase the overall (resulting, integrated, aggregate, integrative) level of control system implementation quality, an expert or group of experts suggests options to improve the system quality by increasing the level of implementation of some controls and estimating the cost of implementing higher levels of individual controls [23, 24].

It is connected with the limited resources, which the organization can allocate to improve the quality of the information security management system.

Defining directions and choosing options for optimizing the integrated level of information security of the organizational system is a multi-criteria task. In addition to ensuring the desired level of implementation of controls, almost every organization should take into account, in particular, its financial capabilities [25].

Therefore, the task of choosing a compromise option to ensure quality control is a multifaceted problem and can be formalized in the classroom of multi-criteria optimization or by applying the idea of system optimization [26-28].

Due to the computational complexity of the problem of control system optimization options direct search, experts can suggest about ten options to improve the quality.

On the basis of the options for increasing the level of separate additional controls implementation, offered by experts, recalculation of new states of system is carried out. Thus, the optimization two-criterion problem to improve the integrated quality of the protection system and minimize the cost of improving the condition of individual controls is solved [29, 30].\

11. Conclusions

A model for assessing the integrated quality of the information security management system based on "best practices" and ways to purposefully improve the quality of its operation is proposed. This model can be adapted to the needs of a particular organization, as well as applied in other subject areas. The model is open to improvement and can easily be focused on dealing with fuzzy data. The integral indicator of the quality will be described in our future papers.

12. References

[1] Bondarev VV Security analysis and monitoring of computer networks. Methods and tools. /V.V. Bondarev. - Moscow: MSTU Publishing House. N.E. Bauman, 2017 – P.225.

[2] Diogenes Y., Ozkaya E. D44 Cybersecurity: attack and defense strategies / trans. with English DA Belikova. – M .: DMK Press, 2020. - 326 p.

[3] Building a HIPAA-Compliant Cybersecurity Program: Using NIST 800-30 and CSF to Secure Protected Health Information https://doi.org/10.1007/978-1-4842-3060-2

[4] International Standards ISO / IEC 27002: 2015 Information technologies. Methods of protection. Code of Practice for Information Security Measures (ISO / IEC 27002: 2013; Cor 1: 2014; IDT).

[5] International Standards ISO/IEC 27006:2015

[6] ISO/IEC 31000:2018 Risk management – Guidelines

[7] IEC 31010: 2019. Risk management – Risk assessment techniques

[8] ISO/IEC 21827:2008 Information technology – Security techniques – Systems Security Engineering – Capability Maturity Model® (SSE-CMM®)

[9] Kravchenko YU.V. Current state and ways of development of the theory of functional stability / YU. V. Kravchenko, S. A. Mykus′ // Modeling and information technology: collection of scientific papers′ IPME im. H.YE. Pukhova. – 2013. – Vyp. 68. P. 60-68.

[10] Norkin, V.I., Gaivoronski, A.A., Zaslavsky, V.A., Knopov, P.S. Models of the Optimal Resource Allocation for the Critical Infrastructure Protection // Cybernetics and Systems Analysis, 54(5), pp. 696-706. (2018)

[11] Y. Kravchenko, O. Leshchenko, N. Dakhno, O. Trush, O. Makhovych “Evaluating the effectiveness of cloud services”, IEEE International Conference on Advanced Trends in Information Theory, ATIT`2019, Proceedings, pp.120–124.

[12] Artyushyn L.M., Mashkov O.A. Optimization of digital automatic systems resistant to failures., Kyiv: KVVAYU, 1991, 88 p.

[13] Barabash O. V., Kravchenko Y. V. Functional stability is a property of complex technical systems. collection of scientific papers. NAOU. Byul. № 40. - K .: NAOU, 2002. – P. 225-222.

[14] Hnatiienko H., Snytyuk V. A posteriori determination of expert competence under uncertainty / Selected Papers of the XIX International Scientific and Practical Conference "Information Technologies and Security" (ITS 2019), pp. 82–99 (2019).

[15] Tsyganok V.V., Kadenko S.V., Andriichuk O.V. Considering Importance of Information Sources during Aggregation of Alternative Rankings / CEUR Workshop Proceedings, Vol. 2067. Selected Papers of the XVII International Scientific and Practical Conference on Information Technologies and Security (ITS 2017); Kyiv, Ukraine, November 30, 2017. P.132-141.

[16] Bozóki Sándor & Tsyganok Vitaliy The (logarithmic) least squares optimality of the arithmetic (geometric) mean of weight vectors calculated from all spanning trees for incomplete additive (multiplicative) pairwise comparison matrices International Journal of General Systems. 2019. vol.48, No.4. P.362-381.

[17] Samokhvalov, Y. Construction of the Job Duration Distribution in Network Models for a Set of Fuzzy Expert Estimates / Advances in Intelligent Systems and Computing, 1020, pp. 110-121. (2020).

[18] Samokhvalov, Y.Y. Development of the Prediction Graph Method Under Incomplete and Inaccurate Expert Estimates / Cybernetics and Systems Analysis, 54(1), pp. 75-82. (2018).

[19] ДСТУ ISO/IEC 27001:2015.

[20] Zaslavskyi, V., Pasichna, M. Type variety principle and the algorithm of strategic planning of diversified portfolio of electricity generation sources / Advances in Intelligent Systems and Computing 582, pp. 474-485. (2018).

[21] N. Kiktev, V. Osypenko, N. Shkurpela, A. Balaniuk. Input Data Clustering for the Efficient Operation of Renewable Energy Sources in a Distributed Information System. 2020 IEEE 15th International Conference on Computer Sciences and Information Technologies (CSIT). 23-26 Sept. 2020, Zbarazh, Ukraine. pp. 9-12. DOI: 10.1109/CSIT49958.2020.9321940

[22] Hnatiienko H. Choice Manipulation in Multicriteria Optimization Problems / Selected Papers of the XIX International Scientific and Practical Conference "Information Technologies and Security" (ITS 2019), pp. 234–245 (2019).

[23] Mulesa, O. Designing fuzzy expert methods of numeric evaluation of an object for the problems of forecasting / Oksana Mulesa, Fedir Geche // *Eastern-European Journal of Enterprise Technologies*. –2016. – Vol. 3, N 4(81). – P. 37-43. – Way of Access : DOI : 10.15587/1729-4061.2016.70515. http://dspace.uzhnu.edu.ua/jspui/handle/lib/8849

[24] Mulesa, O., Snytyuk, V., and Myronyuk, I. (2019). Optimal alternative selection models in a multi-stage decision-making process. *EUREKA: Physics and Engineering*, (6), 43-50.

[25] Kraevsky, V., Kostenko, O., Kalivoshko, O., Kiktev, N., Lyutyy, I. Financial infrastructure of telecommunication space: Accounting information attributive of syntalytical submission / IEEE International Scientific-Practical Conference: Problems of Infocommunications Science and Technology, PIC S and T 2019 – Proceedings, 2019, pp. 873-876, 9061494. (2019).

[26] Hlushkov V.M. Fundamentals of paperless computer science. M.: Nauka. The main edition of physical and mathematical literature, 1982. – 552 p.

[27] Toliupa, S., Nakonechnyi, V., Tereikovskyi, I., Tereikovska, L., & Korystin, O. One-periodic template marks model of normal behavior of the safety parameters of information systems networking resources. In 2019 IEEE International Scientific-Practical Conference: Problems of Infocommunications Science and Technology, PIC S and T 2019 – Proceedings (pp.764-768).

[28] Toliupa, S., Parkhomenko, I., & Shvedova, H. Security and regulatory aspects of the critical infrastructure objects functioning and cyberpower level assesment. In 2019 3rd International Conference on Advanced Information and Communications Technologies, AICT 2019 – Proceedings (pp. 463–468).

[29] M. Beshley, S. Toliupa, V. Pashkevych and R. Kolodiy. Development of Software System for Network Traffic Analysis and Intrusion Detection. 2018 International Conference on Information and Telecommunication Technologies and Radio Electronics (UkrMiCo), Odessa, Ukraine, 2018, pp. 1-6.

[30] Toliupa, S., Babenko, T., & Trush, A. The building of a security strategy based on the model of game management. In 2017 4th International Scientific-Practical Conference Problems of Infocommunications Science and Technology, PIC S and T 2017 – Proceedings. pp. 57–60.