Model for Determining the Protection Level of a Complex System

Tetiana Babenko, Hryhorii Hnatiienko and Andrii Bigdan

Taras Shevchenko National University of Kyiv 64/13, Volodymyrska Street, Kyiv, 01601, Ukraine

Abstract

This paper presents a model for assessing the protection level of information systems. The main purpose of the model is to provide comprehensive support for information security specialists and auditors in assessing information security and systems security levels, evaluating security policies implementation, and compliance with security standards. The paper considers approaches to quantifying the system security indicator. The problem statement is offered and approaches for developing the mathematical model of complex protection are considered.

Keywords [1]

Security measures, information security, information technologies, information security management systems, information security risks, risk assessment, integrated quality assessment models.

1. Introduction

Due to developing society and technology, increased attention is paid to the reliability, safety, and sustainability of complex systems. The main goal of creating an integrated security system is to build a security model that will achieve maximum protection of information resources and ensure maximum security. The cost of inspection and validation for critical systems is extremely high and can be as much as half of the total cost of the system.

The organization ensures the corporate security of the following objects: management technologies, human resources, financial resources, material assets, production technologies, business processes, information resources, etc. One of the essential features of information systems is the a priori presence of subjectivity both in the building of such systems and at all stages of their operation. Ensuring the reliable operation of the information security system is an important and urgent task for any organization. In the context of increasing rivalry at all levels from competition in business within market conditions to the confrontation between states. The problem of reliability of the integrated security system requires the development of new models and the generation of new methods to ensure its reliable security [1]. Issues of reliability of complex security require special attention, for example, in the design of decision-making systems and the development of technology to ensure the reliable and sustainable operation of such systems.

2. Capability assessment models overview

2.1. Maturity models

Maturity models describe and define the state of accomplishment or completeness (maturity) of certain capabilities. This concept has no limitations to be applicable to any area. Maturity progress can be viewed either as a specific development path (life cycle perspective) or as potential or desired

Information Technology and Implementation (IT&I-2021), December 01–03, 2021, Kyiv, Ukraine
EMAIL: babenkot@ua.fm (A. 1); g.gna5@ukr.net (A. 2); abigdan@gmail.com (A. 3)
ORCID: 0000-0003-1184-9483 (A. 1); 0000-0002-0465-5018 (A. 2); 0000-0002-2940-6085 (A. 3)


improvements (potential performance perspective). Consequently, maturity models define simplified stages or levels of maturity that measure the completeness of the analyzed objects using various sets of (multidimensional) criteria [2].

Models of cybersecurity capability maturity are usually based on a process model. A process model is a structured set of practices that describe the features of effective processes. A process model is a structured set of practices that describe the characteristics of effective processes, in turn, practices include methods that have been proven to be effective from experience [3]. Based on the results of the methodical review [4], the most relevant models of cybersecurity capability maturity are SSE-CMM (Systems Security Engineering Capability Maturity Model) [5, 6], C2M2 (Cybersecurity Capability Maturity Model) [7], CCSMM (Community Cyber Security Maturity Model) [8], and NICE (National Initiative for Cybersecurity Education–Capability Maturity Model) [9].

There is a classification for five levels of the capability maturity model [10]: initial, ad hoc, defined, managed, and optimized. This classification highlights the architecture of the enterprise and ignores the threats that each one poses.

According to [11], a company's capabilities are determined by technological maturity and risk. The acceptability of each solution is determined by the available data. Regardless, this report ignores the security framework to assess an organization's requirements and mitigate threats.

In [12], the authors drew out key concepts and best practices called master data maturity assessment. This assessment uses a maturity matrix covering 13 areas, identifies 65 capabilities, and evaluates them. In addition, the authors developed an assessment questionnaire to assess the maturity of master data management. Several security frameworks implement security controls for organizations such as NIST [13] and ISO (27001, 27002) [14, 15].

At the same time, leveraging the approach to assessing the maturity of processes for ensuring the security of information processing in information systems does not allow us to avoid the necessity to solve the problem of processing the results of assessing the implementation level of security processes [16] and, accordingly, assessing the protection of information systems based on the obtained expert data.

2.2. Security level analysis methods

Achieving a certain protection level of an information system is a dynamic and controlled process. The target function of managing the process of ensuring protection is the implementation of the maximum possible protection level of a person and the environment of his life (social, economic, ecological, and other systems) from hazards under these conditions. This feature is often referred to as security management, but this is not entirely true. Strictly speaking, you can control processes and objects. Management of features, properties, state of an object does not have a semantic basis. Therefore, the expression “security management” should be understood as control actions, measures aimed at ensuring the safety of the protected object from possible negative factors.

Security as a category is assessed from various positions. We have already noted that security is defined as a property, a state, and the absence of unacceptable risk. The intuitive assessment of security by different people (non-experts in the field of risk assessment) also, as a rule, is not the same and is not equal to the hazards themselves, but this assessment underlies the perception of danger, and therefore security and risk.

The measure of the demand for security by each person in the presence of real dangers and threats can be determined by various factors [17]. Some of these factors are based on objective assessments by individuals and are adequate to the current situation. Others are subjective in nature, which may be caused by the peculiarities of the perception of hazards and risks, personal attitude to security, insufficient educational level, special knowledge, or other reasons [18, 19].

The many positions from which security is assessed do not change the common and unique case of its goal – to ensure an acceptable (necessary) level of protection [20].

Security is defined as an acceptable hazard. The security level is determined by the security indicators. Security indicators can be the scale of damage to security objects, the probability of causing harm, the risk as to the product of the probability and the loss attributed to a certain point in time. The most widely used security feature is a risk. All risk analysis methods can be divided into expert and calculated.

2.2.1. Expert methods

Expert methods are methods of determining the relative characteristics of risk (low, medium, and high-risk level) by a group of specialists.

Expert methods are most widely used. This is due to their greater simplicity, which makes it possible to involve practitioners in security analysis who do not have special training in the field of probability theory and mathematical statistics. In addition, the use of a number of expert methods is dictated by international standards in the field of management systems.

The method for determining the level of security is associated with expert assessments based on the determination of indicators of various parameters that affect the state of security. The variety of factors affecting the protection level of objects also depends on various indicators [21]:

- The human factor depends on the skill level of employees and their psychological state.
- The technical condition of the facility is determined by the quality of the equipment used and its depleted capacity.
- Technological processes depend on the set parameters and regulatory documents.
- Control over the safe operation of an enterprise depends on the quality of the measures taken during supervision and production control.
- External influences are characterized by natural and weather phenomena.

To determine the level of impact of a particular indicator, weighting factors were introduced for each criterion. The percentage of the causes of accidents, obtained after the analysis of the negative manifestations that occurred, can be used as a basis for determining such coefficients.

2.2.2. Calculation methods

Calculation methods are methods of calculating risk in the characteristics of the probability of causing harm to a particular species [22]. Quantitative risk analysis is another way to determine the protection level of information systems. The expediency of applying this criterion lies in its ability to characterize not only more accurately the possibility of an emergency, but also to assess the likely consequences. However, it is difficult to obtain a sufficiently detailed and reliable result of an accident risk assessment. This is due to the lack of information on incidents, accidents, and failures.In practice, the data of reference books, process modeling, intuitive features of the analyst, and his reasoning can be involved. It turns out that the data obtained is just a guideline for real value. The estimation of the available error is made by some uncertainty. The resulting uncertainty in the risk analysis is a characteristic of the work performed. If the uncertainty is in large enough intervals, then the practical value of the implemented measures is small. For this reason, available risk calculation techniques include guidelines for quantifying uncertainty.

When assessing uncertainty, two aspects should be given in meaning: qualitative and quantitative. In the first case, we are talking about the completeness and relevance of the disclosed information about the object of study. When performing risk analysis, there is a tendency to conclude on a quantitative expression of uncertainty. Uncertainty, in fact, is the interval of the result [23]. The dependence of uncertainty on the model is due to incomplete information about the factors; application of a model that goes beyond its scope; the use of simplifications and admissibility of errors. The implementation of work in the field of risk analysis and assessment continues to evolve. However, without the necessary attention to quantifying uncertainty, significant results are unlikely to be achieved. It is necessary to understand that only methods for determining the protection level based on mathematical calculations, using statistics and even scientific approaches of the theory of probability, make this work meaningful and effective, and not formal.

3. Problem statement

In general, the auditor needs to assess the security of a specific information system. To simplify and scale the assessment process, questionnaires with discrete “Yes” or “No” answers have been prepared. That is, the auditor must fill in all the answers, and then, based on his results, the protection

level of the information system must be calculated, where each answer should be treated as a parameter with a value of 0 ("No") or 1 ("Yes").

So, let P be considered as a weakly structured system of complex security for an information system, and we are going to determine its integrated protection level. Each information system is characterized by n parameters (1):

$$P = (p_i), \qquad i = 1, \dots, n, \tag{1}$$

It could be known which subsystems the information system consists of. These can be subsystems of information technical protection, cryptographic protection systems, organizational measures for protecting information, a system of complex information protection, etc. We consider two options for assessing the protection level of a complex system:

- Case C1. Individual subsystems are not distinguished at all. In this case (1) is applicable.
- Case C2. There are k subsystems within this information system (2):

$$P = P^1 \cup P^2 \cup \dots \cup P^k, \tag{2}$$

Each subsystem $P^i,\ i \in I = \{1, \dots, k\}$ is defined by a set of parameters (3)

$$P^i = \left(p_1^i, \dots, p_n^i\right), \qquad i \in I, \qquad n = \sum_{i \in I} n_i, \tag{3}$$

The sets of parameters do not intersect $P^i \cap P^j = \emptyset$ for $\forall i \neq j,\ i, j \in I$.

In addition, the set of parameters is unstructured, only their list is known. That is, functional dependencies do not exist or have not been investigated, and the level of connectivity between subsystems has not been identified and/or evaluated.

The parameters that characterize the system in case C1 or the selected subsystems of the information system in case C2 are measured dichotomously (4):

$$p_j^i \in \{0,1\}, \qquad j \in 1, \dots, n, \qquad i \in I = \{1, \dots, k\}, \tag{4}$$

That is, each specific parameter either affects the activity or the quality of the system operation or does not affect it.

To determine the protection level of a complex system, an examination is performed and each of the subsystem parameters is inspected, i.e., we obtain the values of vectors of the form (3) for the protection system of a particular information system.

The task is to build indicators that define the protection level of each of the subsystems $P^i,\ i \in I$, and the integrated protection level of the information system P in general.

4. Approaches review

4.1. General approach

All the information that a person uses in his life and in the decision-making process can be divided into three categories: formalized, partially formalized, and non-formalized [24]. Depending on the level of formalization the types of systems, tasks, problems, and types of solutions are determined: structured, partially structured, and unstructured. Structured problems are repetitive and known algorithms provide solutions. Unstructured problems are original and unusual, there are no solution algorithms for them: each is unique, and it is often impossible to check how effective the solution of an unstructured problem has been and whether there are more successful solution algorithms. Partially (poorly, poorly, semi-) structured problems lie between structured and unstructured.

Such partially structured problems are characterized by the following features:

- lack of a formalized purpose of functioning;
- impossibility to build an analytical model;
- significant influence of non-factors: incompleteness, inaccuracy, ambiguity, uncertainty, unreliability, etc.;
- lack of standards;
- constant changing data and knowledge;
- solutions uniqueness;

- the influence of the human factor;
- large dimension of the decision space, etc.

To date, the mathematical support for the study of many practical problems is traditionally comprised of methods of mathematical statistics, and in some cases, methods of operations research (mathematical programming) are used. But at the same time, it is known that this mathematical apparatus is mostly acceptable for structured problems. As it is known, one of the mathematical tools for studying partially structured problems is the methods of decision theory in a sense it is a logical continuation of mathematical programming (operations research).

Most of the tasks of determining the protection level of the information system are poorly (partially, weakly) formalized. This is because any management task involves a person or a group of people in the decision-making loop, which automatically generates subjectivity, multidimensionality, uncertainty, ambiguity in its formulation, modeling, solution, application, and interpretation. In addition, a significant part of management tasks cannot be solved without the involvement of expert information. Therefore, it is advisable to solve management tasks by methods of decision-making theory with the use of expert technologies.

Based on the expert analysis of the protection levels of the information system, let the values of a vector of the form (1) are obtained, and its elements are given in the dichotomous scale: $p_i \in \{0,1\},\ i = 1, \dots n$. Since in such situation subsystems are not distinguished, we will conventionally call such a system unstructured and consider some problems that arise in this case.

Heuristic E1. All parameters of an information system of case C1 and case C2 are commensurate in value, that is, they cannot significantly differ in their impact on the state of the system.

Considering the heuristic E1, we can assume that the statistical analysis can indicate the state of the system's security. It can show how many parameters of the vector (1) received the value $p_i = 1,\ i = 1, \dots n$, which reflects the presence of system protection for the i-th parameter. But this way of determining the protection level of the information system is not very informative and can only conditionally indicate the security of the system.

4.2. Static approach

Ensuring a reliable level of integrated security requires the creation of an adequate model for relevant and sustainable assessment of the protection level of the informational system in numerical terms.

Along with the security parameters, additional information on the evaluation parameters can be specified by the developers for the inspection model of the system protection level.

To obtain an integrated assessment of the protection level of the information system, additional parameters specific to a particular system can be added to the main assessment parameters.

All systems that are inspected to determine the protection level can be considered interdependent in some way. Since all systems are included as subsystems in a higher-level system – at the state level. In addition, the protection level is a relative value and is determined by comparison with other systems at the national level.

Heuristic E2. The number of positive responses to the total set is an indicator of the level of the subsystem implementation.

Heuristic E3. The existing system security according to parameter $p_i \in \{0,1\},\ i = 1, \dots, n$ indicates its high quality if most of the inspected systems are also protected by this parameter.

At the same time, the opposite reasoning may take place, expressed in the following heuristic.

Heuristic E4. The existing system security by parameter $p_i \in \{0,1\},\ i = 1, \dots, n$ indicates its high quality if the system security is unique, that is, only some of the inspected systems are also protected by this parameter.

Heuristic E3 and heuristic E4 characterize different decision-making strategies and cannot be simultaneously applied to the same parameter. However, applying both heuristics to different parameters in the same system is acceptable, and in some cases useful and even necessary.

Based on the application of these heuristics, the values $q_i \in \{0,1\},\ i = 1, \dots, n$ of some functions are determined, considering the influence of heuristic E3 or heuristic E4, and not dichotomous indicators of the protection level for each parameter.

For each parameter, additional signs can be specified that indicate the feasibility of using the E3 or E4 heuristics. Some signs (classes) of the importance of parameters can be set, which can be considered in subsequent calculations. That is, at the stage of implementing a system security model, a classification of the parameters importance can be specified: when each parameter is assigned to one of the specified 3-5 security classes and is described by means of a vector $\varepsilon_i \in \{0,1\},\ i = 1, \dots, n$.

4.3. Dynamic approach

At the earlier stages of implementing the determination system of protection level, a dynamic approach can be applied. With this approach, the vector $p_i \in \{0,1\}, i = 1, \dots, n$ changes as the database is filled.

In this case, a methodological question arises: enumerate the values obtained at the initial stages of the automated system for determining the protection level or leave them obtained at the beginning of the calculations.

Note that the resulting protection level can be determined on different scales. The representation of the protection level of the information system can be given by a fixed number, in the form of an interval, in the form of a membership function for a fuzzy set. In turn, these types of integrated protection levels can be measured in various specified ranges.

5. Unstructured systems

When considering situations in which the structure of the information system and the relationships between its subsystems are known, it is advisable to additionally determine the degree of influence of the subsystems on the protection level of the information system in general.

In the case where an inspection is carried out on a system that is weakly structured, there is more information to assess the protection level. For example, when it is known the structure of the system, the list of its subsystems, and the list of parameters that characterize the operation of these subsystems. Relationships between subsystems, their relative importance to the system in general, mutual influence, priority, etc. can also be known. In this case, we will interpret the problem of considering the features of a structured system in terms of the weighting coefficients of the subsystems.

Based on the analysis of the protection levels of each subsystem, let them be filled with the values of all vectors of subsystems (4), and its elements have dichotomous values.

At the first stage, to conclude about the integrated protection level of the information system in general the interrelations between the importance of subsystems are determined, expressed by normalized weights.

At the second stage, an examination is carried out, that is, an inspection of the protection quality of each subsystem and the system in general [25].

At the third stage, heuristics are applied to calculate the protection level.

At each stage, both an individual expert assessment and group evaluation can be used. We will consider the tasks that arise in different decision-making situations.

5.1. Methods for determining the interrelations between the importance of subsystems

It is difficult for a person to determine the weight of objects through indirect methods. Therefore, indirect methods are often used, or information is considered based on the complex application of several methods. Such approaches have proven themselves well in many areas of human life [26] and have become standard in many studies. Therefore, the task of execution becomes the subject of manipulation of solutions and requires further research [26].

By applying the methods of processing expert information, the weighting factors of the importance of the expertise areas are determined:

$$0 < \rho_i < 1, \qquad \sum_{i=1}^{k} \rho_i = 1, \tag{5}$$

The problem of determining the protection level of the information system in the most general form can be formalized in the class of problems for calculating weight coefficients. Today, there are several common ways to represent the values of weight coefficients:

- Arbitrary real or natural numbers:
  $\infty < \rho_i < \infty, \qquad i \in I.$
- Real numbers subject to restrictions (one-sided or two-sided):
  $\rho_i > 0, i \in I, \qquad -5 \le \rho_i \le 5, i \in I, \qquad 0 < \rho_i < 1, \ \ i \in I.$
- Real or natural numbers, considering the condition of centeredness:
  $\sum_{i \in I} \rho_i = 0, \qquad -\infty < \rho_i < \infty, \qquad i \in I.$
- Real numbers considering the condition of normalization:
  $\sum_{i \in I} \rho_i = 1, \qquad \rho_i > 0, \qquad i \in I.$
- Idealized weights:
  $\max_{i \in I} \rho_i = 1, \qquad \rho_i > 0, \qquad i \in I.$

Peculiarity the use of the interval form for weight coefficients (6) were investigated in [26]:

$$\rho_i \in \left[\rho_i^H, \rho_i^B\right], \qquad 0 < \rho_i^H < \rho_i^B, \qquad i \in I, \tag{6}$$

Weighting factors are often fuzzy because they reflect the real characteristics of poorly structured subject areas. Therefore, in such cases, the weighting factors are appropriate and convenient to represent in the form of fuzzy values. It is proposed to apply weight coefficients in practical problems utilizing a membership function [26], the essence and basic properties of membership functions also were described there.

5.2. A method for indirect determining weights by the incomplete matrix of pairwise comparisons

Consider a method for determining the weight coefficients of objects, based on the analysis of pairwise comparison of objects. This method is focused on finding the weight coefficients of objects in the form of membership functions of a fuzzy set [27]. Moreover, the number of compared areas should be small – 10-15 objects of comparison.

When solving multicriteria optimization problems, the problem of determining the Pareto domain is strictly objective and can be solved without using any heuristics. Narrowing the area of effective objects requires the use of additional information from experts since the effective sets of parameters are not formally comparable with each other. As a rule, three heuristics are used to determine a single solution to a multicriteria problem.

Firstly, to convert all values of object parameters into a dimensionless form in each range of values one of the admissible transformations is used.

Secondly, the vector of the relative importance of the criteria is determined.

Thirdly, it is assumed that the solution of a multicriteria problem is the point of intersection of the ray of normalized weight coefficients of the relative importance of the criteria and the area of effective alternatives of the problem.

It is known that creating the structure of advantages in a formalized form is a difficult task for a person. Research in the field of peer review tasks and the practice of developing decision support systems show that experts and decision-makers do not always have a clear idea of the structure of advantages across a set of objects. In most cases, a person cannot adequately determine the weight

coefficients, as well as he or she cannot highlight explicitly heuristics that he or she leverages in a decision-making situation [28]. One of the methods for solving the problem of determining the weight of objects from an incomplete metricized multiplicative matrix of paired comparisons (7) is described and investigated in [26]:

$$M = (\mu_{ij}), \qquad i, j \in I, \tag{7}$$

At the first stage of this method, a rectangular matrix of size $(n \times N), N = \frac{n(n-1)}{2}$ is created from the matrix of the form (7) with elements (8):

$$P = (\pi_{ij}), \qquad i \in H = \{1, \dots, N\}, \qquad j \in I, \tag{8}$$

where

$$\pi_{ij} = \begin{cases} 1, \text{ if } i = (2-n) + \sum_{l=1}^{s} (n-l), \qquad s = 1, \dots, n-1 \\ \mu_{ij}, \text{ if } j = s + i \text{ for } i = 1, .., n-1, \qquad j = s + i - \sum_{l=1}^{s} (n-l) \text{ for } i \geq l \text{ or } s \geq 2 \\ 0 - \text{in all other cases} \end{cases}$$

From the matrix (8) all possible combinations from the $(n-1)$ row are selected in turn and supplemented with a row of length n, which consists of unit elements. The resulting matrix is denoted by $A^{(l)}$, $l \in \Lambda$ and a system of linear algebraic equations (9) is formed:

$$\begin{cases} A^{(l)}\rho = e \\ \rho_i > 0, \quad i \in I' \end{cases} \tag{9}$$

where Λ – the set of indices of systems of the form (9) for which the matrix $A^{(l)}$, $l \in \Lambda$ is nondegenerate; e – a vector of length n with elements $(0, \dots, 0, 1)^T$, where T – a transposition sign.

It should be noted that systems of linear equations of the form (9) have a special structure that can be used for speeding up the calculating procedure of all possible values of the weight coefficients of objects. First, the matrices $A^{(l)}$, $l \in \Lambda$ in these systems are very sparse, so special methods can be applied to them to simplify the calculations when solving the problem.

Second, the number of compatible systems of the form (6) is n^{n-2} according to Kelly's theorem on the number of undirected trees in a graph, as a result, with a large number of objects many systems of equations are incompatible, so it's not needed to solve them.

For example, for $n = 10$ the number of compatible systems is almost 3.6% of the total number of systems of the form (9), and for $n = 12$ this number is only 0.8% of all possible systems of the form (9). Third, the sequence of calculating systems of the form (9) can be organized in such a way that each successive matrix of the form $A^{(l)}$, $l \in \Lambda$ differs from the previous one by only one row.

5.3. Resulting membership function

We came to determining the membership functions of weights by the matrix of pairwise comparisons to the problem of determining the interrelation between the importance of subsystems to obtain the protection level of a complex system. Applying the method for indirect determining weights by the incomplete matrix of pairwise comparisons sets of weights values (10) are generated:

$$\rho_i \in \{\rho_i^1, \dots, \rho_i^L\}, \qquad i \in I, \tag{10}$$

where $L = |\Lambda|$ – the number of indices of systems of the form (6) of the set Λ.

Based on the obtained values of the weight coefficients (10), which are involved in solving the systems of the form (9), the membership functions of the weight values of the fuzzy set (0,1) are determined. That is, each weighting factor because of applying the described procedure will be characterized by its own membership function of the fuzzy set.

Thus, the membership functions of the weight coefficients determined on the basis of the application of the described method will have the form:

$$A = \bigcup_{i \in I} A^i, \tag{11}$$

where

$A^i = \{\rho_i, \mu_{A^i}(\rho_i)\},\ i \in I,$

$\rho_i \in \lfloor \rho_i^H, \rho_i^B \rfloor,\ i \in I$, where the boundaries of the intervals are determined by formulas:

$$\rho_i^H = \min_{j=1,\dots,L} \rho_i^j,\ i \in I \qquad (12)$$

$$\rho_i^B = \max_{j=1,\dots,L} \rho_i^j,\ i \in I'$$

As mentioned above, the dynamic approach consists in assessing the protection level of the information system in general and its subsystems as the database becomes full.

For a partly structured system, all subsystems are assessed autonomously, and then the obtained indicators are aggregated. If all or most of the expertise results for the systems being inspected are already known, a static approach can be applied. Based on the implementation of the integral criterion, we determine the protection level of the system in general. In this case, different types of convolutions can be used, depending on the level of criticality of the situation:

$$I^A = \sum_{i=1}^{k} \rho_i \cdot K^i, \quad I^M = \min_{i=1,\dots,k} \rho_i \cdot K^i, \quad I^K = \sqrt{\sum_{i=1}^{k} (\rho_i \cdot K^i)^2}.$$

That is, we can take any of the values calculated in the example above as the protection level of the system or use all of them to obtain a comprehensive characteristic of the protection level. Determining the type of convolution to calculate the values of the integral criterion is the prerogative of the decision-maker. This is done in collaboration with a team of researchers. Research and determination of the most acceptable type of integrated criterion is an important independent task and requires additional research, which is not the subject of this work. The integrated indicator may look like this:

- Consists of three numbers

  $I^S = (I^A, I^M, I^K).$

- Chosen by experts some function f of these values

  $I^S = f(I^A, I^M, I^K).$

6. Conclusion

The assessment of the adequacy of leveraging the proposed approach was carried out by comparing with the results obtained after processing the data on the protection level of information systems by experts. The research sample was presented by 100 expert opinions and standard parameters for assessing the security of the studied systems. Based on the analysis of the obtained results, it was concluded that the proposed approach allows assessing the protection level of the information system with the accuracy of 97% according to the parameters of the information system supplied by auditors and can be used for automation and increasing efficiency and objectivity of auditors' activities.

7. References

[1] Andrew S. Tanenbaum, Maarten Van Steen Distributed Systems: Principles and Paradigms, Prentice Hall of India; 2nd edition (January 1, 2007).

[2] RoyWendler. The maturity of maturity model research: A systematic mapping study / Information and Software Technology. Volume 54, Issue 12, December 2012, Pages 1317-1339.

[3] Select Business Solutions Inc. What is the Capability Maturity Model? (CMM). http://www.selectbs.com/process-maturity/what-is-the-capability-maturity-model

[4] Angel Marcelo Rea-Guaman, Tomás San Feliu, Jose A. Calvo-Manzano, and Isaac Daniel Sanchez-Garcia. Comparative Study of Cybersecurity Capability Maturity Models / International Conference on Software Process Improvement and Capability Determination. – September 2017. DOI: 10.1007/978-3-319-67383-7_8

[5] SSE Project Team: System Security Engineering Capability Maturity Model (SSE-CMM): Model Description Document Version 3.0. Technical report, SSE-CMM (2003)
[6] ISO/IEC 21827:2008 Information technology – Security techniques – Systems Security Engineering – Capability Maturity Model® (SSE-CMM)
[7] Department of Energy: Cybersecurity Capability Maturity Model (C2M2): Version 1.1. Technical report, Department of Homeland Security (2014)
[8] White, G.B.: The community cyber security maturity model. In: IEEE International Conference on Technologies for Homeland Security, pp. 173–178. IEEE Press, Wakefield (2011)
[9] US Department of Homeland Security: Cybersecurity Capability Maturity Model: Version1.0. White paper, Department of Homeland Security (2014)
[10] Lankhorst M. Beyond enterprise architecture. In Enterprise Architecture at Work. Springer; 2013. pp. 303–308.
[11] J.K.D. Sc, C. Eng, A. Massie. A framework for a systems engineering body of knowledge / 11th International Symposium of the INCOSE Melbourne, Australia (2000), pp. 1-7.
[12] M. Spruit, K. Pietzka. Md3m: the master data management maturity model / Comput. Human Behav., 51 (2015), pp. 1068-1076
[13] K. Stouffer, K. Stouffer, T. Zimmerman, C. Tang, J. Lubell, J. Cichonski, J. McCarthy. Cybersecurity framework manufacturing profile / US Department of Commerce, National Institute of Standards and Technology (2017)
[14] ISO. ISO/IEC 27001:2013 Information technology – Security techniques – Information security management systems – Requirements; 2013. URL: https://www.iso.org/standard/54534.html
[15] ISO. ISO/IEC 27002:2013 Information technology – Security techniques – code of practice for information security controls; 2013. URL: https://www.iso.org/standard/54533.html
[16] Palko, D., Hnatienko, H., Babenko, T., Bigdan, A. Determining key risks for modern distributed information systems / CEUR Workshop Proceedings, 2021, 3018, pp. 81–100.
[17] Palko, D., Myrutenko, L., Babenko, T., Bigdan, A. Model of Information Security Critical Incident Risk Assessment / 2020 IEEE International Conference on Problems of Infocommunications Science and Technology, PIC S and T 2020, 2021, pp. 157–161, 9468107.
[18] Kravchenko, Y., Vialkova, V. The problem of providing functional stability properties of information security systems // Modern Problems of Radio Engineering, Telecommunications and Computer Science, Proceedings of the 13th International Conference on TCSET 2016, pp. 526–530.
[19] Hrechko Viktoriia; Hrygorii Hnatienko; Tetiana Babenko. An intelligent model to assess information systems security level // 2021 Fifth World Conference on Smart Trends in Systems Security and Sustainability (WorldS4), London, United Kingdom, 29-30 July 2021/ Date Added to IEEE *Xplore*: 19 August 2021, Pp 128–133, DOI: 10.1109/WorldS451998.2021.9514019.
[20] Henry K. Risk management and analysis / Kevin Henry // Information Security Management Handbook / Edited by Harold F. Tipton, Micki Krauze. - 6th edition. - Boca Raton: Auerbach Publications, 2017. - Part 1, Section 1.4, Ch. 28. - P. 321-329.
[21] Edinyj Standart. Metody ocenki urovnya promyshlennoj bezopasnosti na opasnyx proizvodstvennyx obektax, 2015. URL: https://1cert.ru/stati/metody-otsenki-urovnya-promyshlennoy-bezopasnosti-na-opasnykh-proizvodstvennykh-obektakh
[22] IEC 31010:2019 Risk management – Risk assessment techniques, 2019. URL: https://www.iso.org/standard/72140.html
[23] Hnatiienko, H., Snytyuk, V. A posteriori determination of expert competence under uncertainty / CEUR Workshop Proceedings, 2019, 2577, pp. 82–99.
[24] Makarov IM, Vinogradskaya TM, Rubchinskiy AA, Sokolov VV Theory of choice and decision making. Moscow: Nauka, 1982. 330 p.
[25] Babenko, T., Hnatiienko, H., Vialkova, V. Modeling of the integrated quality assessment system of the information security management system / CEUR Workshop Proceedings, 2021, 2845, pp. 75–84.
[26] Saaty, T.L. Decision making with the analytic hierarchy process, International Journal of Services Sciences 1 (1) (2008): 83-98. doi: 10.1504/IJSSCI.2008.017590.\
[27] 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.
[28] Kraevsky, V., Kostenko, O., Kalivoshko, O., Kiktev, N., Lyutyy, I. 2019 IEEE International Scientific-Practical Conference Problems of Infocommunications, Science and Technology (PIC S&T). DOI: 10.1109/PICST47496.2019.9061494.