X International Conference of Students, PhD-Students and Young Scientists "Engineer of XXI Century"
11 December 2020 - University of Bielsko-Biała

MODELING OF INFORMATION SECURITY SYSTEM AND AUTOMATED EXPERT ASSESSMENT OF INTEGRAL QUALITY OF SYSTEM FUNCTIONAL STABILITY

Hryhorii HNATIIENKO, Vira VIALKOVA
Supervisor: **Tetiana BABENKO**
Taras Shevchenko National University of Kyiv

Summary: "Best practices" implementation of CMMI, NIST, COBIT, ISO2700, etc., in the process of building and managing information systems (IS), allows to implement some acceptable level of information security, which should be adequate to the actual threats (risks). Respectively, the level of the set of controls implementation, identified in the accepted "best practice", is an important characteristic of the maturity of IS, information security management system (ISMS) and the subject of a large number of specialists' attention.
Keywords: information security, information security risk assessment.

Introduction

The controls, which need to be implemented, during the process of building an information security management system or information systems, are described, in particular.

Some of the controls are critical for the system to provide an acceptable level of services, for other part of them a reduced level of control is acceptable, and in some situations the lack of some controls without significant danger to the level of functional stability of the ISMS system is even possible.

The main part

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 $0 \le b_i \le 1, \forall i \in I$.

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 $0 \le v_{ij} \le 1, \forall i, j \in I$.

The task is to model the characteristics of the information security management system and determine an integrated assessment of the level of information security and, accordingly, to ensure the functional stability of the ISMS.

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.

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.

Normative quality of the control system

While building a control system in full accordance with the standard, 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.

Assessment of the integrated level of control

At the first stage, high-level experts build a model of an ideal control system, that corresponds the standard 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 etc. can be taken into account.

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, 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, which reflects the distribution of quality controls by quality levels and creates a membership function, based on the frequency of values.

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.

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

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.

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.