Algorithm of information security risk assessment based on fuzzy-multiple approach

UDC 004.056.53 Serhii Yevseiev[1], Olexander Shmatko[2], Nataliia Romashchenko[3]

[1] Simon Kuznets Kharkiv National University of Economics, [1]serhii.yevseiev@hneu.net
[2,3] National Technical University "Kharkiv Polytechnic Institute",[2]asu.spios@gmail.com, [3]ronatavit@gmail.com

The accession of humanity to the era of high-end technology has accelerated the development of Internet technologies, which has encouraged the booming development of automated information systems (AIS), which are gaining popularity. Currently threats combine the influence of all components of security. Threats have gained signs of hybridization. Providing information security is part of the information system management as a whole. In this case, one of the most important components of the InfoSec management system is the risk assessment, which is intended to determine the effectiveness of the applicable protection mechanisms based on the corresponding metrics.

After analyzing the existing scientific literature from the specified subject area, two main groups of methodology for assessing information security risks are possible to determine: quantitative and qualitative. The combination of quantitative and qualitative methods represents a mixed set of advantages and disadvantages of the above mentioned methods. Hybrid types of risk assessment have the most practical interest.

Despite the high efficiency of the above-mentioned methodologies, they still have a significant common flaw – they require a significant amount of resources to assess the risk of InfoSec, that is, it is necessary to process a large volume of information that takes a lot of time and effort. There is a need to improve the existing methods for assessing the risk of InfoSec. Accordingly, the *purpose* of the article is to develop a methodology for assessing the degree of information security risk, which would avoid the uncertainty factor, that occurs when some parts of information about the analyzed automated information system are absent.

Apply the proposed methodology to compare its effectiveness with the FAIR method. The initial data for the calculation are in Table 1.

Table 1

A set of indicators X

Characteristic	Current value
X_1	*1.2*
X_2	*0.7*
X_3	*0.025*
X_4	*0.004*

Summarize to each indicator the level of its significance for the analysis of r_i.

$$r_i = \frac{1}{N} = \frac{1}{4} = 0.25 \quad (1)$$

Construct a classification of the current value *g* of the risk factor *G* as a criterion for dividing this set into a subset:

Table 2

Value of indicator *g*

Interval *G*	Set names
$0.8 < g < 1$	G_1 – subset of "marginal threat risk to InfoSec";
$0.6 < g < 0.8$	G_2 – subset of "high threat risk to InfoSec";
$0.4 < g < 0.6$	G_3 – subset of "average threat risk to InfoSec";
$0.2 < g < 0.4$	G_4 – subset of "low threat risk to InfoSec";
$0 < g < 0.2$	G_5 – subset of " insignificant risk threat to InfoSec".

Construct a classification of the current values *x* of the *X* indicators as a criterion for breaking up the complete set of their values into a subset of type *B.*

Table 3

Value Subset Partition

Indicator name	Criteria of subset partition				
	B_{i1}	B_{i2}	B_{i3}	B_{i4}	B_{i5}
X_1	$x_1<0.02$	$0,02<x_1<0,16$	$0,16<x_1<0,84$	$0,84<x_1<1$	$1<x_1$
X_2	$x_2<0.02$	$0,02<x_2<0,16$	$0,16<x_2<0,84$	$0,84<x_2<1$	$1\ x_2$
X_3	$x_3<0.02$	$0,02<x_3<0,16$	$0,16<x_3<0,84$	$0,84<x_3<1$	$1<x_3$
X_4	$x_4<0.02$	$0,02\ x_4<0,16$	$0,16<x_4<0,84$	$0,84<x_4<1$	$1<x_4$

Classify the current values of *x* according to the criterion of Table 3. $\lambda_{ij} = 1$, if $b_{i(j-1)}<x_i<b_{ij}$, and $\lambda_{ij} = 0$, when the value does not fall into the selected range of classification. Carry out arithmetical steps to assess the degree of bankruptcy risk of *g*:

$$G = \sum_{j=1}^{5} g_j \sum_{i=1}^{N} r_i \lambda_{ij}, \quad (2)$$

where $g_j = 0.9 - 0.2(j-1)$.

$$G = 0.25 * 0.1 + 0.25 * 0.3 + 0.25 * 0.5 + 0.25 * 0.7 + 0.25 * 0.9 = 0.45$$

The value of *G* corresponds to subset of "average threat risk to InfoSec".

The calculations of the system information security level in comparison to the calculations using the FAIR methodology are given in the work. It is possible to state that the proposed methodology does not yield to its efficiency. Indeed, under the same input conditions, identical values of the indicators in the linguistic form of evaluation were obtained. The methodology provides an opportunity to translate the obtained results of risk assessment from a mathematical language into a linguistic form that is more comprehensible to the decision-maker. This increases the effectiveness of the management of automated information systems protection mechanisms.