New method for assessing the risk of automated information systems information security based on fuzzy-multiple approach

Olexander Shmatko
Doctor of Philosophy in Technical Science, Associate Professor
Department of Software Engineering and Management Information Technologies
National Technical University "Kharkiv Polytechnic Institute"
ORCID https://orcid.org/0000-0002-2426-900X

Natalya Romaschenko
Master Student
Department of Software Engineering and Management Information Technologies
National Technical University "Kharkiv Polytechnic Institute"
ORCID https://orcid.org/0000-0002-4500-4481

Abstract. *The subject of the study is the process of assessing the level of information security risk that is being implemented with the help of the fuzzy logic apparatus. The purpose of this work 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. The methodology is based on the use of fuzzy logic and fuzzy sets. Which implies the introduction of the term sets for each of the system characteristics and the linguistic assessment of the indicators. The tasks to be solved are to analyze existing information security risk assessment methodologies for identifying their strengths and weaknesses. On the basis of the conducted analysis, a new method for assessing the risk of automated information systems information security is proposed. The following results were obtained: the advantages and disadvantages of qualitative and quantitative methodologies for assessing the risk degree of automated systems information security were identified; the main stages of the proposed methodology were described; the degree of information security risk is calculated in comparison to the FAIR methodology. Conclusion: 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.*

Keywords: *information security, risk assessment, information security risk assessment methodology, fuzzy sets, linguistic form*

Introduction

The accession of humanity to the era of high-end technology has accelerated the development of Internet technologies and computing, which has encouraged the booming development of automated information systems (AIS), which are gaining popularity. AIS is the information base of various services that deal with technical, economic and other tasks. Accordingly, existing threats have also been modified and acquired hybridity signs. Currently they combine the influence of all components of security: information security (InfoSec), cyber security (CyberSec), and security of information (SI). Threats have gained signs of hybridization. The main object of which is the economic sector of the country. There is a need for crosscutting (hybrid) technology to counteract the dangers that play a significant role in business processes. That is why, during the design and development of reliable AIS, it is necessary to provide a set of measures aimed at ensuring their protection against deliberate or accidental influences that may lead to a system failure. Among the security threats to the AIS, which directly affect the system, the personnel and its clients are internal and external threats, show synergy in crosscutting application with social engineering. Both the first and the second, depending on the target and nature of the influence on the activity of certain subjects and objects, can be divided into economic, physical and intellectual [1–3].

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. The remaining problem is to improve the existing methods for assessing InfoSec risk in connection with the emergence of new types of hazards. The task of improving the existing methods for assessing the security risk in the AIS remains currently topical due to the emergence of new types of hybrid cyber threats.

Analysis of Recent Studies and Publications

In the modern scientific community there is a significant number of researchers whose subject matter is to assess the risk of systems InfoSec. For example, [4] classifies existing risk analysis of IS, describes the sequence of risk analysis processes, compares software tools for SI risk management. Another example of research in this subject area is the work [5; 6], which describes the methods of assessment and risk management.

The article [7] proposes a mathematical formulation of risk using the SI main concepts of such risk management methodologies as MEHARI, EBIOS, CRAMM and SP 800–30 (NIST).

Basics for risk assessment, in particular in the context of assessing the risks of access control systems that decide on authorization, are presented in [8].

In the article [9] approaches and program solutions for assessing and controlling information risks as a fundamental organizational stage in the development of information security systems of computerized systems are considered.

In the article [10] an advanced methodology of information risk assessment in an automated system was proposed and analyzed. The necessary normative-legal documents of information security are mentioned. The performance of the prototype expert system is considered, which allows to assess the level of information risk for a certain automated system and to determine the need for additional information security measures [11].

The article [12] analyzes the process of the most common models of information security risk assessment in information and telecommunication systems. The main approaches to information security risk assessment are revealed.

The analysis of threats to information security and a detailed description of the intended sources, classification and the reasons for their occurrence is given in [13].

Main materials of the study

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.

Table 1. – Advantages and disadvantages of qualitative and quantitative methodologies of InfoSec risk degree assessment

+/-	Quantitative	Qualitative
Advantages	- Risks are the financial consequences priority; - assets are the financial values priority; - obtaining simplified risk management results and investment returns into providing security; - results can be expressed in specific management terminology (for example, monetary value and probability is expressed as a certain percentage); - accuracy tends to increase over time as the business constantly records data.	- Provides clarity and understanding of risk classification; - the opportunity to reach consensus; - there is no need to determine the financial value of assets; - it is easier to involve people who are not experts in the field of computer security.
Disadvantages	- Importance influence attributed to risks on the basis of judgmental opinions of participants; - the process for achieving reliable results and consensus takes a lot of time; - calculation might be complex and time-consuming; - the results are presented only in monetary terms and they are difficult to interpret for "non-techies"; - the process requires special knowledge, so it is difficult to train staff.	- Insufficient distinction between among significant risks; - it is difficult to justify investments in control of implementation, because there are no grounds for the analysis of costs and benefits; - the results depend on the quality of the created risk management team

Quantitative methods use measurable, objective data to determine the value of assets, likelihood of loss and associated risks. The goal is to calculate the numerical values for each of the components collected during the risk assessment and analysis of costs and benefits [14].

Qualitative methods use a relative risk or asset value based on rating or categorization, such as low, medium, high, not important, important, very important, on a scale from 1 to 10. A qualitative model evaluates the actions and probabilities of identified risks at a rapid rate and in a cost-effective way. Risk sets are written and analyzed in a qualitative risk assessment, and can serve as a basis for a targeted quantitative assessment. Quantitative and qualitative information security risk assessment methods have both advantages and disadvantages (Table 1).

Accordingly, the combination of quantitative and qualitative methods represents a mixed set of advantages and disadvantages of the above mentioned methods. At present, hybrid types of risk assessment have the most practical interest.

The relation between methods of detecting attacks and risk assessment methods is presented in Figure 1.

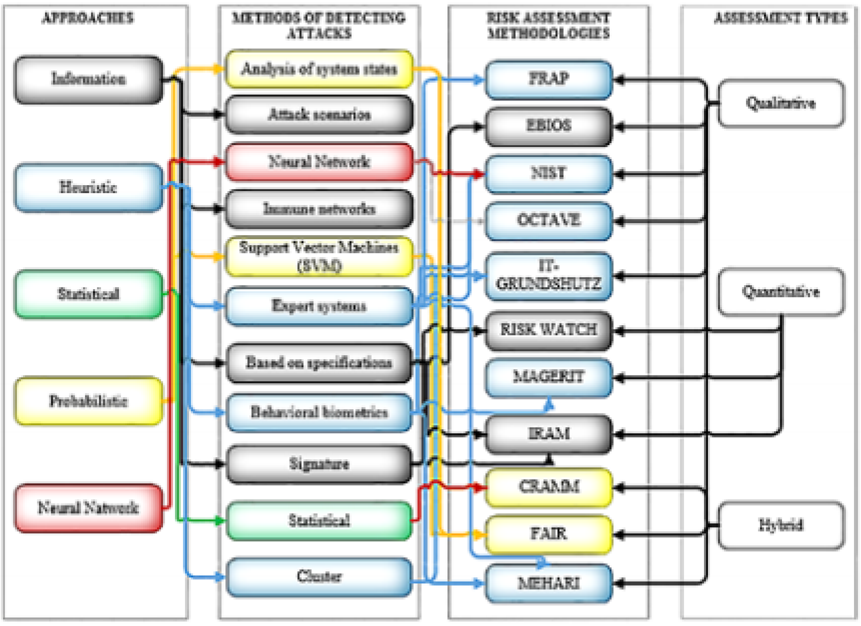


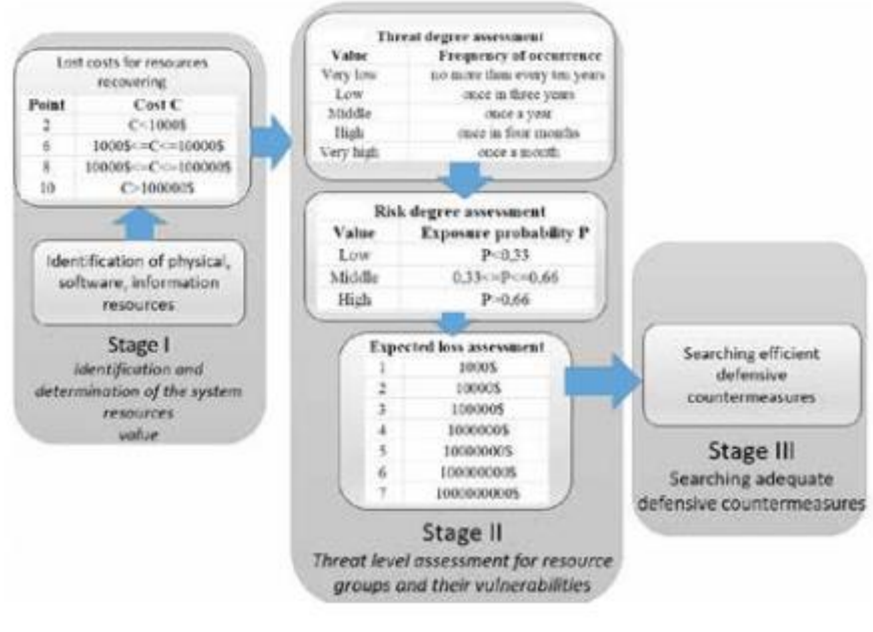
Figure 1. – The relation between methods of detecting attacks and risk assessment

Given the different nature of the threats to the profiles of the computer system, consider some of the methods of risk assessment [3]. The heuristic approach is implemented in the evaluation methods of NIST, IT-Grundshutz, OCTAVE, MEHARI and MAGERIT. Their common advantages include the flexibility – it allows to conduct an analysis for organizations of different sizes; a detailed description and analysis of the information assets of the research object. In most cases, the above methods give the investigator a qualitative assessment. The disadvantages are the lack of automation of some functions and the human factor's impact on the end result.

CRAMM and FAIR methodologies refer to the probabilistic assessment approach. Their advantage is to provide a comprehensive risk assessment for InfoSec, a detailed description of existing risks and high efficiency of use. Also, the methodologies allow to evaluate the effectiveness of countermeasures. Disadvantages include the ability to work only with existing information assets.

The information approach is represented by the IRAM, EBIOS, and RISK WATCH methodologies.

The conducted analysis showed that the considered methodologies do not allow to conduct an assessment of functional efficiency, based on both technical and economic indicators. To obtain estimates of the risk level of equivalent cash capital and the immediate display of its security, it is proposed to use methodologies based on an integrated approach to risk assessment that combines quantitative and qualitative methods of analysis, including CRAMM and FAIR methodologies, structural schemes are presented in the Figure 2, 3 respectively[14].



Lost costs for resources recovering

Point	Cost C
2	C<1000$
6	1000$<=C<=10000$
8	10000$<=C<=100000$
10	C>100000$

Identification of physical, software, information resources

Stage I

identification and determination of the system resources value

Threat degree assessment

Value	Frequency of occurrence
Very low	no more than every ten years
Low	once in three years
Middle	once a year
High	once in four months
Very high	once a month

Risk degree assessment

Value	Exposure probability P
Low	P<0,33
Middle	0,33<=P<=0,66
High	P>0,66

Expected loss assessment

1	1000$
2	10000$
3	100000$
4	1000000$
5	10000000$
6	100000000$
7	1000000000$

Stage II

Threat level assessment for resource groups and their vulnerabilities

Searching efficient defensive countermeasures

Stage III

Searching adequate defensive countermeasures

Figure 2. – CRAMM Methodology – crosscutting approach to risk assessment

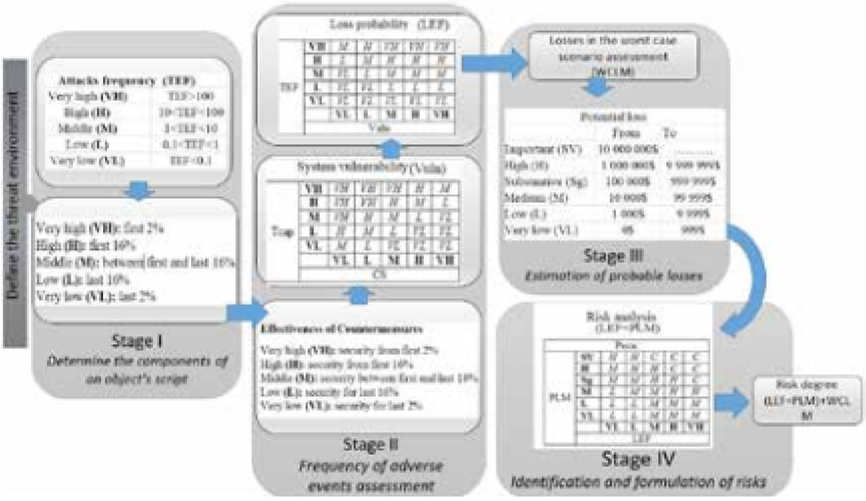

Define the threat environment
Attacks frequency (TEF)
Very high (VH) TEF>100
High (H) 10<TEF<100
Middle (M) 1<TEF<10
Low (L) 0.1<TEF<1
Very low (VL) TEF<0.1
Very high (VH): first 2%
High (H): first 16%
Middle (M): between first and last 16%
Low (L): last 16%
Very low (VL): last 2%
Stage I
Determine the components of an object's script
Loss probability (LEF)
TEF
Vuln
System vulnerability (Vuln)
Tcap
CS
Effectiveness of Countermeasures
Very high (VH): security from first 2%
High (H): security from first 16%
Middle (M): security between first and last 16%
Low (L): security for last 16%
Very low (VL): security for last 2%
Stage II
Frequency of adverse events assessment
Losses in the worst case scenario assessment (WCLM)
Potential loss
From To
Important (SV) 10 000 000$
High (H) 1 000 000$ 9 999 999$
Substantive (Sg) 100 000$ 999 999$
Medium (M) 10 000$ 99 999$
Low (L) 1 000$ 9 999$
Very low (VL) 0$ 999$
Stage III
Estimation of probable losses
Risk analysis (LEF+PLM)
Risk
PLM
LEF
Risk degree (LEF+PLM)+WCL M
Stage IV
Identification and formulation of risks

Figure 3. – FAIR risk assessment methodology

The methodologies of the crosscutting approach to risk assessment, as a rule, use the following stages (steps) [15; 16]:

At the first stage, everything is analyzed regarding the identification and determination of the value of system resources: the definition of the boundaries of the system under investigation: information about the configuration of the system, information about responsible individuals for physical and software resources, determining the number of users of the system, their privileges. Identification of physical, software and informational resources within the boundaries of the system is carried out. A model of the information system is being built from the standpoint of the InfoSec.

The second stage identifies threats and assesses the level of threats to resource groups and their vulnerabilities, assesses the dependence of user-defined services on specific resource groups and the existing level of threats and vulnerabilities, calculates risk levels and analyzes the results. At the end of the stage, the customer receives identified and assessed levels of risk to his system.

The third stage of the study is to find adequate countermeasures – the search for a security solution that best suits the requirements of the customer. At this stage, it generates several variants of countermeasures that are adequate to the identified risks and their levels.

The combination of two qualitative and quantitative approaches will combine the benefits of each of them, provided by them separately, and will open the possibility of obtaining the necessary characteristics for the effective organization of security systems.

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, which would simplify the estimation process and would allow to gain the end results in a linguistic form that is comprehensible to the decision maker. Accordingly, the purpose of the article is to develop a risk assessment methodology for InfoSec based on a fuzzy-multiple approach.

Proposed method

Security risks of information systems are very closely related to uncertainty. Two cases of uncertainty can be determined: identification of the current and future state of the systems.

When solving tasks related to security risk assessment, the question about the qualitative interpretation of certain levels of parameters often arises. The linguistic assessment of the security level is clearer and best describes the state of IT infrastructure security, which in turn encourages the manager to take one or another decision.

In order to fulfill the linguistic assessment, two things are required:

First, you need to define a linguistic scale for evaluation. Most often pentascale is used (five-level classifier) "Very low (VL) – Low (L) – Average (A) – High (H) – Very high (VH)".

Secondly, it is necessary to collect all available information to define linguistic assessment: quantitative data collected in a group of similar objects of observation.

For example, for a qualitative assessment of the level of information security, it is necessary to collect statistical information on similar information systems for a relatively short period of monitoring. This is necessary to maintain the condition of statistical homogeneity. At the same time, it is necessary to take into account the laws that are inherent to the objects of information security.

It should be noted that there are no general universal rules for accurate and rapid assessment of AIS information security. A set of problems may also arise with the collection of initial data for linguistic analysis.

There is a question connected to the additional data analysis, which is related to different time segments of observations. There may be a question about replacing the missing data in one-time period with the data from another similar one, and the parameters of this law will be given according to special rules in order to satisfy the necessary authenticity of the identification of the monitoring law.

The presence of quasistatistics makes it possible to make qualitative conclusions about the behavior of a particular parameter of the investigated IS, makes it possible to conduct a linguistic analysis of input data.

Basic steps of the linguistic classification:

1. The studies of the source data set and its verification as a quasi-statistic are conducted. There is evidence that some data distribution law is hidden in these data, for example, the "gray" Pospelov scale.

2. Next, define the main nodes. In the absence of expert evaluation, nodal points can be determined by the simple rule: node point – left end of media interval, nodal

point – right end of media interval, middle point – corresponds to the maximum histogram or median histogram.

3. The interval between the two nodal points standing next is divided into three zones, the middle one is the zone of expert uncertainty in the classification. Thus, the primary linguistic interpretation of the histogram is complete.

After the classificatory definition it is possible to make a correction of pestascale. To do this, you can modify nodal classification points, bringing them closer together and narrowing the uncertainty zone. You can also replace the nodal point with an absolute confidence interval and try to expand it on both sides of the nodal point. All clarifications must be made on the basis of an agreed expert evaluation.

Apply the proposed methodology to compare its effectiveness with the FAIR method. The initial data for the calculation are taken from [14].

Stage 1. In the first stage, term sets are introduced to describe the basic sets of the IS state and the subset of states, described in the natural language:

The complete set of information security status assessment E of IS is broken down into five subsets of the form:

E_1 – subset of states "extremely unsuccessful state of IS InfoSec";

E_2 – subset of states "unsuccessful state of IS InfoSec";

E_3 – subset of states of "average quality of the IS InfoSec state";

E_4 – subset of states "relatively safe state of IS InfoSec";

E_5 – subset of states "the maximum safe state of the IS InfoSec".

The corresponding set E of a full risk set of IS InfoSec threats G is divided into 5 subsets:

G_1 – subset of "marginal threat risk of InfoSec";

G_2 – subset of "high threat risk to InfoSec";

G_3 – subset of "average threat risk to InfoSec";

G_4 – subset of "low threat risk to InfoSec";

G_5 – subset of " insignificant risk threat to InfoSec".

Assume that G takes the value from zero to one by definition.

For an arbitrary separate indicator of the InfoSec assessment X_i, the complete set of its values of B_i is divided into five subsets:

B_{i1} – subset "very low level of indicator X_i";

B_{i2} – subset of "low level of indicator X_i";

B_{i3} – subset of "average level of indicator X_i";

B_{i4} – subset of "high level of indicator X_i";

B_{i5} – subset of "very high level of indicator X_i".

An additional condition for matching the sets B, E and G of the following form is performed: if all the indicators in the analysis have, according to the classification, the level of the subset B_{ij}, then the state of the InfoSec is qualified as E_j, and the degree of InfoSec threat risk is qualified as G_j. Fulfilment of this condition affects the correct quantitative classification of the levels of indicators and the correct determination of the level of significance of the indicator in the evaluation system.

Stage 2. Construct a set of indicators $X = \{X_i\}$ in the number $N = 4$, which, according to expert-analyst, on the one hand, affect the assessment InfoSec threat risk, and, on the other hand, evaluate the different sides of IS InfoSec (Table 2).

Table 2. – A set of indicators X

Characteristic	Current value
X_1	1.2
X_2	0.7
X_3	0.025
X_4	0.004

Stage 3. Summarize to each indicator the level of its significance for the analysis of r_i. To estimate this level, you need to position all the values in descending order of magnitude so that the rule is complied with:

$$r_1 \geq r_2 \geq \ldots \geq r_n \tag{1}$$

If the system of indicators is put in descending order of their significance, then the significance of the i-th index should be determined by the Fishburn's rule [17]:

$$r_i = \frac{1}{N} = \frac{1}{4} = 0.25 \tag{2}$$

The Fishburn's Rule reflects the fact that nothing is known about the level of significance of the indicators (1). Then the estimate (2) corresponds to the maximum entropy of the existing information uncertainty about the object of the study.

Stage 4. Construct a classification of the current value g of the risk factor G as a criterion for dividing this set into a subset (Table 3):

Table 3. – 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".

Stage 5. 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 4):

Table 4. – 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

Stage 6. Evaluate the current level of indicators and reduce the results (Table 5):

Table 5. – Indicator's Level Evaluation

Indicator name	**Current value**
Very high (VH)	$X_1 > 1$
High (H)	0.1< X_2 <1
Medium (M)	0.01< X_3 <0.1
Low (L)	0.001< X_4 <0.01
Very low (VL)	<0.001

Stage 7. Classify the current values of x according to the criterion of Table 4. The result of the classification is (Table 6).

$\lambda_{ij} = 1$, if, and $\lambda_{ij} = 0$, when the value does not fall into the selected range of classification.

Table 6. – Classification Result

Indicator name	Significance	The result of classification by subsets				
		B_{i1}	B_{i2}	B_{i3}	B_{i4}	B_{i5}
X_1	0.25	0	0	0	0	1
X_2	0.25	0	0	1	0	0
X_3	0.25	0	1	0	0	0
X_4	0.25	1	0	0	0	0

Stage 8. Carry out arithmetical steps to assess the degree of bankruptcy risk of g :

$$G = \sum_{j=1}^{5} g_i \sum_{i=1}^{N} r_i \lambda_{ij}$$

where: $g_i = 0.9 - 0.2(j-1)$

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

$G = 0.25 \cdot 0.1 + 0.25 \cdot 0.3 + 0.25 \cdot 0.5 + 0.25 \cdot 0.9 = 0.45$

The obtained result of the InfoSec risk degree corresponds to the research result in [14].

Conclusions

Information is one of the most important resources in modern ISs, therefore, it is necessary to estimate the risk degree of asset exposure to anomalies and attacks. Existing methods for InfoSec risk assessment such as FAIR, MAGERIT, NIST, CRAMM are often used for this purpose. In this case, the above methodologies do not take into account the fact that IS security risks are closely related to the uncertainty that needs to be addressed. The proposed methodology of risk assessment of the InfoSec can solve this problem – it overcomes the uncertainty and allows the researcher to assess the risk degree in a linguistic form. 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. In the case of using the methodology, the researcher gets the opportunity to formulate conclusions about the level of the system security, and to develop recommendations for the implementation of the necessary security mechanisms.

References:

1. Judin O.K. Information security. Regulatory support. – Kyiv : NAU. 2011.
2. Lenkov S. V., Peregudov D. A. & Horoshko V.A. Methods and means of information protection. – Kyiv: Arij. 2008.
3. Jevsejev S. P. Methodology for building security systems for banking information resources. UDC004.056:336.71. 2018.
4. Baranova E. K. Information security risk analysis and assessment techniques. Educational resources and technologies, 1(9), 2015.– P. 73–79.
5. Anikina I.V., Emaletdinova L. Ju. & Kirpichnikova A. P. Methods for assessing and managing information security risks in corporate information networks. Bulletin of the University of Technology, 18(6), 2015. – P. 195–197.
6. Puzyrenko O.G., Ivko S. O. & Lavrut O. O. Analysis of the process of information security risk management in providing information and telecommunication systems. Systems of information processing, 8(124), 2014. – P. 128–134.
7. Ghazouani M., Faris S., Medromi H. & Sayouti A. Information security risk assessment – a practical approach with a mathematical formulation of risk. International Journal of Computer Application, 103(8), 2014.– P. 36–42.
8. Khambhammettu H., Logrippo L., Boulares S & Adi K. A Framework for Risk Assessment in Access Control Systems. Computers & Security, 2013. – 38 p.
9. Chunarova A.V., Parhomenko I. I. & Sashhuk I. I. Analysis of approaches and software solutions for the assessment and control of information risks in the computerized. Bulletin of the Engineering Academy of Ukraine, 2. 2014.– P. 138–142.

10. Buchyk S. S. Methodology for assessing information risks in an automated system. Knowledge-based technologies, 3 (35), 2017. – 224 p.
11. Buchyk S. S. & Shalaev V. A. Analysis of instrumental methods for determining information security risk information and telecommunication systems. Knowledge-based technologies, 3(35), 2017. – P. 215–225.
12. Puzyrenko O. G., Ivko S. O., Lavrut O. O. & Klymovych O. K. Application of information security risk assessment models in information and telecommunication systems. Systems of information processing, 3(128), 2015. – P. 75–79.
13. Gonchar S. Analysis of probability of realization of threats of information protection in automated control systems of technological process. Information protection, 16(1), 2014. – P. 40–46.
14. Korol' O. G. Estimation of the quality of global network services based on Ethernet technologies using a complex indicator. Systems of information processing, 2(148), 2017. – P. 100–110.
15. Kuznecov O. O., Evseev S. P. & Kavun S. V. Information protection and economic security of the enterprise. – Kharkiv: HNEU. 2008. – 360 p.
16. Smirnov O. A., Evseev S. P., Zhukarev, V. Ju., Korol' O. G., Sorokin V. Je. & Meleshko Je. V. D. Technologies and standards of computer networks. – Donetsk: DonIZT, 2012. – 453 p.
17. Cirlov V. L. Basics of Information Security. – Rostov n/D: Feniks 2008.